

Appendices

Table of Appendices

Appendix A: E-Authentication Partnership Trust Framework

Attachment 1: Final Trust Framework	2
Attachment 2: EAP Snap-In Contracts Issues Brief	94
Attachment 2: EAP Accreditation, Certification and Assessment Models	112

Appendix B: E-Authentication Federation

Attachment 1: Draft Legal Document Suite, November 23, 2004	149
Attachment 2: Draft Legal Document Suite, October 14, 2005	171

Appendix C: Certification Authority Ratings and Trust Guidelines

Attachment 1: Final CARAT Guidelines	264
Attachment 2: Background Materials on the CARAT Guidelines	390
Attachment 3: IETF RFC 3627 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	394

Appendix D: NACHA Electronic Benefits Transfer

Attachment 1: QUEST® Operating Rules	584
Attachment 2: Amendments & Variances	674

Appendix E: Nationwide Health Information Network

Attachment 1: DURSA Overview	676
Attachment 2: Data Use and Reciprocal Support Agreement (DURSA)	682
Attachment 3: NwHIN Onboarding Process	721

Appendix F: Multi-State E-Mall™ Operating Rules

Attachment 1: Version 1 Operating Rules	798
---	-----

Attachment 2: Version 2 Operating Rules	817
Attachment 3: Version 3 Operating Rules	842
Attachment 4: Technology Hypothesis and Analysis	846
Attachment 5: Legal/Business Hypothesis and Analysis	854
<hr/>	
Appendix G: InCommon® Federation	
Attachment 1: By Laws of the InCommon LLC	873
Attachment 2: Operating Agreement	880
Attachment 3: Federation Operating Policies and Practices	896
Attachment 4: Federation Participation Agreement	906
Attachment 5: Federation Participant Operational Practices	918
Attachment 6: Identity Assurance Assessment Framework	929
Attachment 7: Identity Assurance Profiles Bronze and Silver	952
Attachment 8: Federation SAML 2.0 Profiles	970
Attachment 9: Certification Practices Statement for Client Certificates	979
<hr/>	
Appendix H. Federation for Identity and Cross-Credentialing Systems, Inc.®	
Attachment 1: FiXs® Bylaws	1010
Attachment 2: FiXs Operating Rules	1029
Attachment 3: FiXs Policy Document	1126
Attachment 4: FiXs Trust Model	1162
Attachment 5: FiXs Implementation Guidelines	1175
Attachment 6: FiXs Security Guidelines	1220
Attachment 7: FiXs Trusted Broker (FTB) Gateway	1249
Attachment 8: FiXs Configuration Control Board Procedures	1272
Attachment 9: FiXs Certification and Accreditation Process	1284

Appendix A: E-Authentication Partnership Trust Framework

Attachment 1: Final Trust Framework

Attachment 2: EAP Snap-In Contracts Issues Brief

Attachment 2: EAP Accreditation, Certification and Assessment Models



Electronic Authentication Partnership

Trust Framework

Version 1.0
January 6, 2005

Electronic Authentication Partnership Trust Framework

Contents

1	Business Rules.....	1
1.1	Scope.....	1
1.2	Participation and Voluntary Termination	1
1.3	Roles and Obligations	2
1.4	Enforcement and Recourse.....	6
1.5	General Terms.....	8
1.6	Interpretation.....	8
2	Assurance Levels.....	9
2.1	Assurance Level Policy Overview	9
2.2	Description of the Four Assurance Levels.....	9
3	Service Assessment Criteria.....	13
3.1	Context and Scope	13
3.2	Readership	13
3.3	Terminology	13
3.4	Criteria Descriptions	14
3.5	Common Organizational Service Assessment Criteria	14
3.6	Identity Proofing Service Assessment Criteria	35
3.7	Credential Management Service Assessment Criteria.....	48
4	Accreditation and Certification Rules.....	77
4.1	Assessor Accreditation :	77
4.2	Certification of Credential Service Provider Offerings.....	78
4.3	Process for Handing Non-Compliance	81
4.4	Acceptable Public Statements Regarding EAP Accreditation and Certification.....	82
5	EAP Glossary.....	83
6	Publication Acknowledgements.....	88

1 BUSINESS RULES

1.1 Scope

Signatories to these business rules agree that these rules govern the use and validation of Electronic Authentication Partnership (EAP) certified credentials, the certification of such credentials and the accreditation of those who assess issuers of such credentials. These business rules are intended to cover use of credentials for purposes of authentication and not specifically for the application of a legal signature, which may be subject to other rules depending upon the parties and transactions involved.

The EAP is responsible for the EAP certification of credentials issued by a credential service provider (CSP). The EAP is responsible for the accreditation of assessors who evaluate CSPs for purposes of EAP certification of credentials. An EAP certified credential issued by any EAP CSP may be used by any EAP-relying party that is a signatory to these business rules and that chooses to accept or otherwise rely upon the credential by agreement with the issuing CSP.

The foregoing does not prohibit use of an EAP credential under a different brand, certification, or set of rules, provided that the credential is clearly being used as a non-EAP credential.

Claimants are not direct signatories to these business rules. Claimants must have contracts with each CSP issuing an EAP credential to the claimant. The claimant can be a person, the electronic agent of a person, or any legal entity, including a corporation.

1.2 Participation and Voluntary Termination

Each relying party and CSP must agree to be bound by these business rules as a precondition to participation in the EAP System. By contractually agreeing to be bound by these business rules, a party becomes a signatory to these rules. Before becoming eligible to become a signatory to these rules, a CSP must successfully complete an assessment by an EAP-accredited assessor, be awarded EAP certification for one or more lines of credentials issued by that CSP and sign a CSP participation agreement. A relying party becomes a signatory to these business rules by contracting with one or more EAP CSPs and assenting to the relying party participation agreement. A person need not be a member of the EAP non-profit corporation in order to become a signatory to these business rules. Execution of the participation agreement must be performed by a person legally authorized to bind the respective relying party or CSP for that purpose. The execution of the relying party or CSP participation agreement may be accomplished by any method of contracting approved for this purpose by the EAP Board of Directors.

A party that has become a signatory to these business rules may terminate signatory status at any time by providing the EAP with written notice of termination that includes the effective date of termination. Such notice must be provided no less than 30 days prior to the effective date of termination. Any signatory that objects to an amendment under Section 3.1.1 may give notice of termination less than 30 days prior to the effective date if necessary to avoid becoming bound to the amendment to which the signatory objects. Termination of signatory status terminates any EAP trademark license and any CSP participation agreement and/or relying party agreement to which the signatory is a party.

1.3 Roles and Obligations

1.3.1 EAP

1.3.1.1 Promulgation and Amendment of Business Rules and Other Documents

The EAP shall formalize and may periodically amend these business rules. The EAP shall also formalize and may periodically amend a set of documents governing the accreditation of assessors of EAP CSPs and the certification of EAP credentials. The EAP reserves the right, at its discretion, to formalize and periodically amend such other materials, including policies or guidelines, participation agreements, handbooks or other documents relevant to the EAP. Notice of all amendments shall be given by EAP by electronic mail to the contact person(s) identified by each signatory for such purpose and by posting to the EAP web site. All amendments shall be effective as of the date specified in such notice. If a signatory objects in writing to an amendment within 30 days after notice of the amendment is given by EAP, such objection shall be deemed to be a notice of termination of such signatory's participation in EAP under Section 1.2.

1.3.1.2 Relying Party, CSP and Assessor Approval

The EAP is responsible for approving participation in the EAP System by relying parties, CSPs and assessors. The EAP shall formalize and may periodically amend requirements for certification of credentials issued by a CSP and the accreditation of assessors of CSPs. The EAP shall formalize, maintain and update as needed an EAP-approved CSP list (EAP CSP list) of certified signatory CSPs. This EAP CSP list shall include, at a minimum, the names of each CSP, the level of assurance for which credentials issued by the CSP have been certified and a URL and other contact information for the CSP.

1.3.1.3 Contact Information

Current contact information for the EAP can be found at <http://www.eapartnership.org>.

1.3.2 CSP OBLIGATIONS

1.3.2.1 CSP Certification

A CSP is obliged to achieve certification of one or more lines of credentials and be added to the EAP CSP list as a prerequisite to being approved by the EAP for participation in the EAP System.

1.3.2.2 CSP Participation Agreement

A CSP is obliged to execute a CSP participation agreement as a prerequisite to being approved by the EAP for participation in the EAP System.

1.3.2.3 Continued Compliance with Certification Requirements

Each approved and certified CSP must comply with all certification requirements during the period of time for which credentials issued by the CSP are certified.

1.3.2.4 Use of EAP Trademark

A CSP may not use or display the EAP trademark in association with the issuance, validation or other servicing of an EAP credential or otherwise use or display the EAP trademark on or associated with any service, product, literature or other information unless such use has been approved by the EAP and the trademark is used in accordance with the applicable agreement with the EAP.

1.3.2.5 Records of EAP Related Disputes

A CSP is required to investigate any complaint raised to the CSP from a relying party regarding an EAP credential. The CSP is also required to keep auditable records of its investigation and decisions regarding any complaint.

1.3.2.6 Validation

Each CSP must make available a method of validation for each EAP credential it issues or is otherwise responsible for validating. Such method must be accessible and reliable.

1.3.2.7 Privacy Practices

Each CSP must be able to verify that it is complying with applicable privacy practices, as stated in Section 1.3.4.8 of these business rules.

1.3.2.8 Relying Party Agreement With CSP

Each approved CSP shall have in place a contract governing the rights and obligations between it and any relying party using, validating or otherwise relying upon EAP-certified credentials issued by that CSP. The parties to the contract, levels of assurance involved, applicable band of monetary recourse (identified in Section 1.4.2), and effective dates must be reported to the EAP in a timely fashion. At a minimum, such contracts shall inform the relying party that it must agree to abide by these business rules and agree to terms and conditions of use of the EAP System contained in a relying party agreement. Such agreement may contain such additional terms as the parties may agree to.

1.3.3 RELYING PARTY OBLIGATIONS

1.3.3.1 Relying Party Participation Agreement

A relying party is obliged to execute a relying party participation agreement as a prerequisite to (a) approval for participation in the EAP System and (b) seeking to validate and rely upon a credential issued under these rules.

1.3.3.2 Reasonable Reliance and Level of Assurance

A relying party is obliged to determine for itself the appropriate level of assurance of the EAP credential needed for a particular application, transaction or other session. A relying party is obliged to establish that a credential is in fact issued by a listed EAP-approved and accredited CSP in order for the relying party's reliance upon the asserted identity of the claimant to be deemed reasonable under these business rules. A relying party is obliged to successfully validate an EAP credential in order for its reliance upon the asserted identity of the claimant to be deemed reasonable under these business rules. Any use by or validation of an EAP credential by a party that has not entered into a relying party agreement with the CSP that issued the credential shall be at the sole risk of that party, for which the CSP shall have no liability whatsoever.

1.3.3.3 Use of EAP Trademark

A relying party may not use or display the EAP trademark in association with the acceptance, validation or other use of an EAP credential or otherwise use or display the EAP trademark on or associated with any service, product, literature or other information unless such use has been approved by the EAP and the trademark is used in accordance with the applicable agreement with the EAP.

1.3.4 ASSESSOR OBLIGATIONS

1.3.4.1 CSP Accreditation

An assessor is not eligible for approval by the EAP to conduct an assessment for purposes of EAP certification of a CSP or otherwise participate as an assessor in the EAP System unless that assessor has been and remains accredited by the EAP.

1.3.4.2 CSP Participation Agreement

An assessor is obliged to execute an EAP assessor agreement as a prerequisite to being approved by the EAP.

1.3.4.3 Continued Compliance with Accreditation Requirements

In accordance with the requirements of the EAP accreditation and certification rules and any applicable service assessment criteria, approved and accredited assessors must remain in compliance with all accreditation requirements for the period of time for which they are accredited.

1.3.4.4 Use of EAP Trademark

An assessor may not use or display the EAP trademark in association with an assessment or otherwise use or display the EAP trademark on or associated with any service, product, literature or other information unless such use has been approved by the EAP and the trademark is used in accordance with the applicable agreement with the EAP.

1.3.5 GENERAL OBLIGATIONS

1.3.4.5 Record Keeping

Every signatory wishing to avail itself of EAP resolution of disputes under the terms of these business rules is obliged to keep records sufficient to preserve evidence of the facts related to a particular dispute.

1.3.4.6 System Security and Reliability

Every signatory agrees to safeguard the security and reliability of the EAP System. Specifically, every signatory agrees that the EAP reserves the right to suspend use of the EAP System, in whole or in part, and the participation of any party or parties to the system without notice and at the sole discretion of the EAP to protect the integrity and efficacy of the EAP System or the rights or property of any party. Agreement to access, use or rely upon the EAP System is subject to such terms and conditions as the EAP may provide in these business rules, related participation agreements or otherwise.

1.3.4.7 Third Party Processors

Any CSP or relying party that is a signatory to these rules and uses a third-party processor to perform any processing, transactions or other obligations related to participation in the EAP System either must take full responsibility for assuring that actions of the third-party processor are in compliance with all applicable terms of these business rules or assure that the third party itself becomes a direct signatory of these business rules.

1.3.4.8 Claimant Privacy

Every signatory to these business rules must assure that each claimant for which the signatory collects or otherwise uses personally identifiable information has granted informed consent with regard to the sharing of any personally identifiable information about the claimant by the signatory with any other party, whether such information is contained in a credential, other identity assertion or otherwise. The informed consent of the individual must be obtained before personally identifiable information is used for enrollment, authentication or any subsequent uses. Claimants must be provided with a clear statement about the collection and use of personally identifiable information upon which to make informed decisions. Signatories must collect only the information necessary to complete the intended authentication function.

Informed consent, for the purposes of this section, is an agreement made by a claimant with the legal capacity to do so who is so situated as to be able to exercise free power of choice without the intervention of any element of force, fraud, deceit, duress, over-reaching, or other form of constraint or coercion and who is given sufficient information about the subject matter and elements of the transaction involved as to enable him or her to make an informed and enlightened decision.

Nothing in these business rules shall be construed to authorize or permit the sharing of any personally identifiable information about an end user other than the information contained in a certificate or other identity assertion. Such information can be shared only with an approved relying party to whom the end user has presented credentials or attempted to access services with an identity assertion operating under the EAP. If any other personally identifiable information about a claimant is shared with any party operating within the EAP System or any other party, the required consent terms listed in this section of these business rules must be affirmatively assented to by the claimant.

1.4 Enforcement and Recourse

1.4.1 BREACH OF ACCREDITATION OR CERTIFICATION REQUIREMENTS

1.4.1.1 Compliance Determination

Upon receipt by the EAP of credible information that an assessor or CSP is not in compliance with the requirements for accreditation or certification, the EAP Board or staff or a committee at Board discretion shall make a determination on whether the assessor or CSP is in fact in material non-compliance with EAP requirements and shall communicate the determination to the affected parties. The Board of Directors shall establish further criteria, as needed, detailing conduct or circumstances constituting material non-compliance with EAP rules or standards.

1.4.1.2 Period to Cure

An assessor or CSP found to be in material non-compliance shall be afforded an opportunity and period of time to remedy that material non-compliance, provided such period does not unduly jeopardize the integrity of the EAP System or the rights or property of another party.

1.4.2 MONETARY REOURSE

A CSP may be liable solely under the terms of an applicable relying-party agreement with an EAP-approved relying party for losses suffered by such EAP-approved relying party where the cause is attributable to conduct by the CSP that was carried out in material non-compliance with these business rules or with certification requirements.

A CSP may offer credentials at a band of monetary recourse set independently from levels of assurance. A CSP shall disclose the monetary recourse it will or will not make available with respect to EAP credentials and any applicable terms or limitations governing the recourse according to

Table 1-1:

Table 1-1. Bands and Amounts of Monetary Recourse	
Band	Amount
1. No recourse	Zero monetary recourse
2. By agreement	By agreement of the parties

1.4.2.1 Safe Harbors

1.4.2.1.1 *Losses Arising From Authorization or Unreasonable Reliance*

In no event shall liability or other recourse specified herein be triggered by unreasonable reliance on a credential by a relying party or by losses resulting from authorization errors that have not been caused by errors in authentication of identity of a `claimant by means of an EAP credential.

1.4.2.1.2 *Conduct in Accordance with Business Rules*

Under these business rules, an approved CSP is not liable for losses suffered by an approved relying party where the cause is attributable to conduct by the CSP that was carried out in accordance with these business rules.

1.4.2.2 Request for Monetary Recourse

If a relying party is eligible to request monetary recourse under these rules, then it may do so by submitting to the relevant CSP an event summary, including at least the following information: The account, the date(s) of incorrect authentication validation(s), the cost of repair and the amount of recourse requested, as constrained by the applicable floor and ceiling at the band of recourse for the EAP credential in question. A relying party may request \$0, even if costs are significant.

1.4.2.3 Reporting to the EAP

All requests for monetary recourse and the dispositions of all requests must be reported to the EAP by each relying party and CSP involved.

1.4.3 ADMINISTRATIVE RE COURSE

Based on review of all available data and in light of all relevant circumstances, the EAP Board of Directors may take administrative recourse against any signatory determined to be in material non-compliance with these business rules, to include, as needed, any of the following remedies.

1.4.3.1 Warning

The non-complying party may be given a warning. The warning may be confidential or may be publicized within the EAP or publicized more broadly, at the discretion of the EAP Board of Directors.

1.4.3.2 Credential Revocation

The non-complying party may be required to revoke one or more EAP credentials.

1.4.3.3 Non-compliance Fees

The non-complying party may be subject to a schedule of fees, to be specified by the EAP Board of Directors. The fees may increase according to the length of time before the party comes back into compliance.

1.4.3.4 Suspension

The non-complying party may have its participation in the EAP System suspended, including the suspension of accreditation or certification, pending coming back into compliance.

1.4.3.5 Termination

The non-complying party may have its participation in the EAP System terminated, including the termination of accreditation or certification.

1.5 General Terms

1.5.1 GOVERNING LAW

These business rules and any related materials governing the EAP shall be construed and adjudicated according to the laws of the state of Delaware.

1.5.2 DISCLAIMER

No signatory may disclaim the warranty of merchantability and fitness for a particular purpose with respect to the provision of any service or product to any other signatory under these business rules.

1.5.3 ASSIGNMENT AND SUCCESSION

No signatory may sell, rent, lease, sublicense, assign, grant a security interest in or otherwise transfer any right and/or obligation contained in these business rules or the participation agreement executed by that signatory without the express written consent of the EAP.

1.5.4 HOLD HARMLESS

All signatories to these business rules agree to hold the EAP harmless for any losses or other liability arising out of or in relation to the issuance, use, acceptance, validation, or other reliance upon an EAP credential or otherwise arising out of or in relation to participation in the EAP System or other conduct subject to these business rules.

1.5.5 SEVERABILITY

If any provision, set of provisions or part of a provision of these business rules is held to be unenforceable or otherwise invalid in whole or in part, the remaining provisions shall remain in full force and effect and shall be construed to the maximum extent practicable as a consistent and reasonable entire agreement.

1.6 Interpretation

The terms of these business rules shall be interpreted by the EAP so as to avoid conflict or inconsistencies between the various provisions and between these business rules, applicable participation agreements and other relevant EAP materials.

2 ASSURANCE LEVELS

2.1 Assurance Level Policy Overview

An assurance level (AL) describes the degree to which a relying party in an electronic business transaction can be confident that the credential being presented actually represents the entity named in it and that it is the represented entity who is actually engaging in the electronic transaction. ALs are based on two factors:

- The extent to which the identity presented in an electronic credential can be trusted to actually belong to the entity represented. This factor is generally handled by identity proofing.
- The extent to which the electronic credential can be trusted to be a proxy for the entity named in it and not someone else (known as identity binding). This factor is directly related to the trustworthiness of the credential technology, the processes by which the credential is secured to a token, the trustworthiness of the system that manages the credential and token, and the system available to validate the credential, including the reliability of the credential service provider responsible for this service.

Managing risk in electronic transactions requires authentication processes that provide an appropriate level of assurance. Because different levels of risk are associated with different electronic transactions, EAP has adopted a multi-level approach to ALs. Each level describes a different degree of certainty in the identity of the claimant.

The EAP defines four levels of assurance. The four EAP ALs are based on the four levels of assurance posited by the U.S. Federal Government and described in OMB M-04-04 and NIST Special Publication 800-63 for use by Federal agencies. The EAP ALs enable subscribers and relying parties to select appropriate electronic trust services. EAP uses the ALs to define the service assessment criteria to be applied to electronic trust service providers when they are demonstrating compliance through the EAP assessment process. Relying parties should use the levels to map risk and determine the type of credential issuing and authentication services they require. Credential service providers (CSPs) should use the levels to determine what types of credentialing electronic trust services to offer.

2.2 Description of the Four Assurance Levels

The four ALs describe the degree of certainty associated with an identity. The levels are identified by both a number and a text label. The levels are defined as shown in **Error! Reference source not found.**:

Table 2-1. Four Assurance Levels

Number	Label	Description
1	Minimal	Little or no confidence in the asserted identity's validity
2	Moderate	Some confidence in the asserted identity's validity

3	Substantial	High confidence in the asserted identity's validity
4	High	Very high confidence in the asserted identity's validity

The choice of AL is based on the degree of authentication required to mitigate risk and the level of authentication provided by the credentialing process. The degree of authentication required is determined by the relying party through risk assessment processes covering the electronic transaction system. By mapping impact levels to ALs, relying parties can then determine what level of authentication they require. (Further information on assessing risk is provided below.)

The level of authentication provided is measured by the strength and rigor of the identity-proofing process, the credential's strength and the management processes the service provider applies to it. The EAP has established service assessment criteria at each AL for electronic trust services providing credential management services. These criteria are described in Section 3.

CSPs can determine the AL at which their services might qualify by evaluating their overall business processes and technical mechanisms against the EAP service assessment criteria. Services can be developed to qualify for a particular AL. The service assessment criteria within each AL are the basis for assessing and approving electronic trust services.

Potential Impact of Authentication Errors	Assurance Level*			
	1	2	3	4
Inconvenience, distress or damage to standing or reputation	Min	Mod	Sub	High
Financial loss or agency liability	Min	Mod	Sub	High
Harm to agency programs or public interests	N/A	Min	Mod	High
Unauthorized release of sensitive information	N/A	Min	Sub	High
Personal safety	N/A	N/A	Min	Sub High
Civil or criminal violations	N/A	Min	Sub	High

*Min=Minimum; Mod=Moderate; Sub=Substantial; High=High

2.2.1 ASSURANCE LEVEL 1 (MINIMAL)

At AL1, there is minimal confidence in the asserted identity. Use of this level is appropriate when no negative consequences result from erroneous authentication and the authentication mechanism used provides some assurance. A wide range of available technologies and any of the token methods associated with higher ALs, including PINS, can satisfy the authentication requirement. This level does not require use of cryptographic methods.

The electronic submission of forms by individuals can be Level 1 transactions when all information flows to the organization from the individual, there is no release of information in return and the criteria for higher assurance levels are not triggered. For example, when an individual uses a web site to pay a parking ticket or tax payment, the transaction can

be treated as a Level 1 transaction. Other examples of Level 1 transactions include transactions in which a claimant presents a self-registered user ID or password to a merchant's web page to create a customized page, or transactions involving web sites that require registration for access to materials and documentation such as news or product documentation.

2.2.2 ASSURANCE LEVEL 2 (MODERATE)

At AL2 there is confidence that an asserted identity is accurate. Moderate risk is associated with erroneous authentication. Single-factor remote network authentication is appropriate. Successful authentication requires that the claimant prove control of the token through a secure authentication protocol. Eavesdropper, replay and online guessing attacks are prevented. Although the identity proofing requirements are similar to those for AL1, the authentication mechanisms must be more secure.

For example, a transaction in which a beneficiary changes an address of record through an insurance provider's web site can be a Level 2 transaction. The site needs some authentication to ensure that the address being changed is the entitled person's address. However, this transaction involves a low risk of inconvenience. Since official notices regarding payment amounts, account status and records of changes are sent to the beneficiary's address of record, the transaction entails moderate risk of unauthorized release of personally sensitive data.

2.2.3 ASSURANCE LEVEL 3 (SUBSTANTIAL)

AL3 is appropriate for transactions requiring high confidence in an asserted identity. Substantial risk is associated with erroneous authentication. This level requires multi-factor remote network authentication. Identity proofing procedures require verification of identifying materials and information. Authentication must be based on proof of possession of a key or password through a cryptographic protocol. Tokens can be "soft," "hard," or "one-time password" device tokens. Note that both identity proofing and authentication mechanism requirements are more substantial.

For example, a transaction in which a patent attorney electronically submits confidential patent information to the U.S. Patent and Trademark Office can be a Level 3 transaction. Improper disclosure would give competitors a competitive advantage. Other Level 3 transaction examples include online access to a brokerage account that allows the claimant to trade stock, or use by a contractor of a remote system to access potentially sensitive personal client information.

2.2.4 ASSURANCE LEVEL 4 (HIGH)

AL4 is appropriate for transactions requiring very high confidence in an asserted identity. This level provides the best practical remote-network authentication assurance, based on proof of possession of a key through a cryptographic protocol. Level 4 is similar to Level 3 except that only "hard" cryptographic tokens are allowed. High levels of cryptographic assurance are required for all elements of credential and token management. All sensitive data transfers are cryptographically authenticated using keys bound to the authentication process.

For example, access by a law enforcement official to a law enforcement database containing criminal records requires Level 4 protection. Unauth-

orized access could raise privacy issues and/or compromise investigations. Dispensation by a pharmacist of a controlled drug also requires Level 4 protection. The pharmacist needs full assurance that a qualified doctor prescribed the drug, and the pharmacist is criminally liable for any failure to validate the prescription and dispense the correct drug in the prescribed amount. Finally, approval by an executive of a transfer of funds in excess of \$1 million out of an organization's bank accounts would be a Level 4 transaction.

3 SERVICE ASSESSMENT CRITERIA

3.1 Context and Scope

The EAP Service Assessment Criteria (SAC) are prepared and maintained by the Electronic Authentication Partnership (EAP) as part of its Trust Framework. These criteria set out the requirements for services and their providers at all assurance levels within the Framework. These criteria focus on the specific requirements for EAP assessment at each assurance level (AL) for the following:

- The general business and organizational conformity of services and their providers,
- The functional conformity of identity proofing services, and
- The functional conformity of credential management services and their providers.

These criteria (at the applicable level) must be complied with by all services that are assessed for certification under the EAP Trust Framework.

These criteria have been approved under the EAP's governance rules as being suitable for use by EAP-recognized assessors in the performance of their assessments of trust services whose providers are seeking approval by EAP.

In the context of the EAP Trust Framework, the status of this document is normative. An applicant provider's trust service **shall** comply with all applicable criteria within this SAC at their nominated AL.

This document describes the specific criteria that must be met to achieve each of the four ALs supported by the EAP. To be certified under the EAP System, services must comply with all criteria at the appropriate level.

3.2 Readership

This description of Service Assessment Criteria is required reading for all EAP-recognized assessors, since it sets out the requirements with which service functions must comply to obtain EAP approval.

The description of criteria in sections 3.5, 3.6 and 3.7 is required reading for all providers of services that include identity-proofing functions, since providers must be fully aware of the criteria with which their service must comply. It is also recommended reading for those involved in the governance and day-to-day administration of the EAP Trust Framework.

Identity proofing criteria included in section 3.6 is required reading for all Electronic Trust Service Providers whose services include identity-proofing functions, since providers must be fully aware of the criteria with which their service must comply.

This document will also be of interest to those wishing to have a detailed understanding of the operation of the EAP's Trust Framework but who are not actively involved in its operations or in services that may fall within the scope of the Framework.

3.3 Terminology

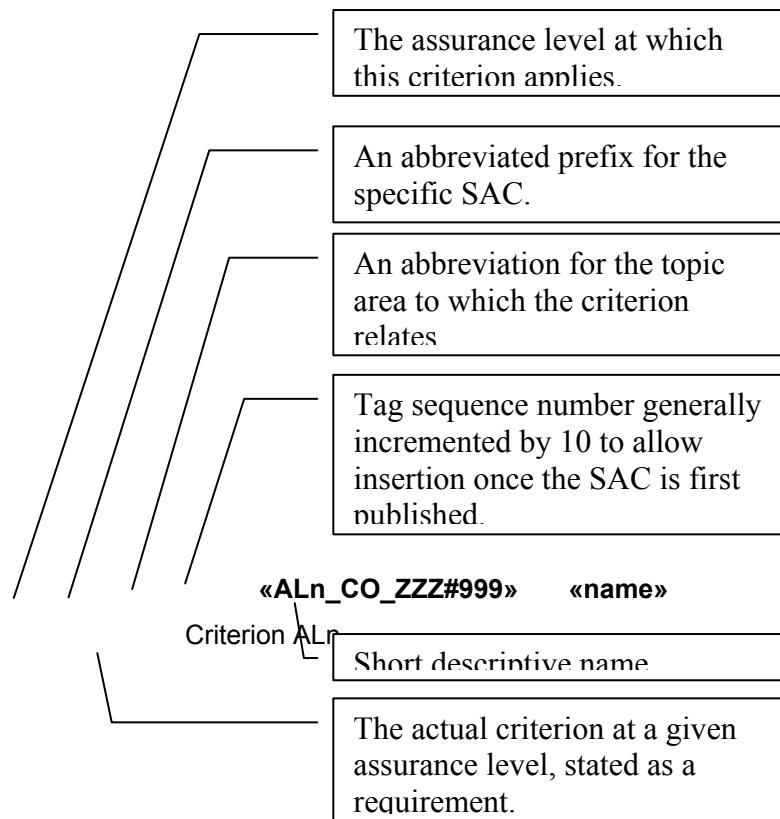
All special terms used in this description are defined in the EAP Glossary.

3.4 Criteria Descriptions

The Service Assessment Criteria are organized by AL. Subsections within each level describe the criteria that apply to specific functions. The subsections are parallel. Subsections describing the requirements for the same function at different levels of assurance have the same title.

Each criterion consists of three components: a unique alphanumeric tag, a short name, and the criterion (or criteria) associated with the tag. The tag provides a unique reference for each criterion that assessors and service providers can use to refer to that criterion. The name identifies the intended scope or purpose of the criterion.

The criteria are described as follows:



3.5 Common Organizational Service Assessment Criteria

The Service Assessment Criteria in this section establish the general business and organizational requirements for conformity of services and service providers at all ALs defined in Section 2. These criteria are generally referred to elsewhere within EAP documentation as CO-SAC.

These criteria may only be used in an assessment in combination with one or more other SACs that address the technical functionality of specific service offerings.

3.5.1 ASSURANCE LEVEL 1 (MINIMAL)

3.5.1.1 Enterprise and Service Maturity

These criteria apply to the establishment of the enterprise offering the service and its basic standing as a legal and operational business entity.

An enterprise and its specified service must:

AL1_CO_ESM#010 Established enterprise

Be a valid legal entity and a person with legal authority to commit the enterprise must submit the assessment package.

AL1_CO_ESM#020 Established service

Be described in the assessment package as it stands at the time of submission for assessment and must be assessed strictly against that description.

AL1_CO_ESM#040 Legal compliance

Set out and demonstrate that it understands and complies with any legal requirements incumbent on it in connection with operation and delivery of the specified service, accounting for all jurisdictions within which its services may be used.

3.5.1.2

Notices & User information

These criteria address the publication of information describing the service and the manner of and any limitations upon its provision.

An enterprise and its specified service must:

AL1_CO_NUI#010 General Service Definition

Make available to the intended user community a Service Definition for its specified service that includes all applicable Terms, Conditions, Fees and Privacy Policy for the service, including any limitations of its usage.

AL1_CO_NUI#020 Due notification

Have in place and follow appropriate policy and procedures to ensure that it notifies subscribers in a timely and reliable fashion of any changes to the Service Definition and any applicable Terms, Conditions and Privacy Policy for the specified service.

AL2_CO_NUI#035 User Agreement

Through a user agreement:

- a) require the Subscriber to provide full and correct information as required under the terms of their use of the service.
- b) obtain a record (hard-copy or electronic) of the Subscriber's Agreement to the Terms and Conditions of service.

3.5.1.3

Information Security Management

No stipulation.

3.5.1.4

Secure Communications

AL1_CO_SCO#020 Protection of secrets

Ensure that:

- a) access to shared secrets shall be subject to discretionary controls which permit access to those roles/applications which need such access.

- b) stored shared secrets are not held in their plaintext form.
- c) any plaintext passwords or secrets are not transmitted across any public or unsecured network.

3.5.2 ASSURANCE LEVEL 2 (MODERATE)

Criteria in this section address the establishment of the enterprise offering the service and its basic standing as a legal and operational business entity.

3.5.2.1 Enterprise and Service Maturity

These criteria apply to the establishment of the enterprise offering the service and its basic standing as a legal and operational business entity.

An enterprise and its specified service must:

AL2_CO_ESM#010 Established enterprise

Be a valid legal entity and a person with legal authority to commit the enterprise must submit the assessment package.

AL2_CO_ESM#020 Established service

Be described in the assessment package as it stands at the time of submission for assessment and must be assessed strictly against that description.

AL2_CO_ESM#040 Legal compliance

Set out and demonstrate that it understands and complies with any legal requirements incumbent on it in connection with operation and delivery of the specified service, accounting for all jurisdictions within which its services may be offered.

AL2_CO_ESM#050 Financial Provisions

Demonstrate that it has adequate financial resources for the continued operation of the service and has in place appropriate provision for the degree of liability exposure being carried.

AL2_CO_ESM#060 Data Retention & Protection

Specifically set out and demonstrate that it understands and complies with those legal and regulatory requirements incumbent upon it concerning the retention of private (personal and business) information (its secure storage and protection against loss and/or destruction) and the protection of private information (against unlawful or unauthorized access unless permitted by the information owner or required by due process).

3.5.2.2 Notices and User Information/Agreements

These criteria apply to the publication of information describing the service and the manner of and any limitations upon its provision, and how users are required to accept those terms.

An enterprise and its specified service must:

AL2_CO_NUI#010 General Service Definition

Make available to the intended user community a Service Definition for its specified service that includes any specific uses or limitations on its use, all applicable Terms, Conditions, Fees and Privacy Policy for the service, including any limitations of its usage and definitions of any terms having specific intention or interpretation. Specific provisions are stated in further criteria in this section.

AL2_CO_NUI#020 Service Definition sections

Publish a Service Definition for the specified service containing clauses that provide the following information:

- a) the legal jurisdiction under which the service is operated.
- b) if different from the above, the legal jurisdiction under which subscriber and any relying party agreements are entered into.
- c) applicable legislation with which the service complies.
- d) obligations incumbent upon the CSP
- e) obligations incumbent upon the subscriber.
- f) notifications and guidance for relying parties, especially in respect of actions they are expected to take should they choose to rely upon the service's product.
- g) statement of warranties.
- h) statement of liabilities.
- i) procedures for notification of changes to terms and conditions.
- j) steps the ETSP will take in the event that it chooses or is obliged to terminate the service.
- k) full contact details for the ETSP (i.e., conventional post, telephone, Internet) including a helpdesk.
- l) availability of the specified service per se and of its help desk facility.
- m) termination of aspects or all of service.

AL2_CO_NUI#030 Due notification

Have in place and follow appropriate policy and procedures to ensure that it notifies subscribers in a timely and reliable fashion of any changes to the Service Definition and any applicable Terms, Conditions, Fees and Privacy Policy for the specified service and provides a clear means by which subscribers may indicate that they wish to accept the new terms or terminate their subscription.

AL2_CO_NUI#034 Subscriber Information

Require the Subscriber to provide full and correct information as required under the terms of their use of the service.

AL2_CO_NUI#036 Subscriber Agreement

Obtain a record (hard-copy or electronic) of the Subscriber's Agreement to the Terms & Conditions of service.

AL2_CO_NUI#038 Change of Subscriber Information

Require and provide the mechanisms for the Subscriber to provide in a timely manner full and correct amendments should any of their recorded information change, as required under the terms of their use of the service, and only after the subscriber's identity has been authenticated.

AL2_CO_NUI#040 Helpdesk facility

Ensure that its helpdesk is available for any queries related to the specified service during the regular business hours of its primary operational location, minimally from 9 AM to 5 PM, Monday through Friday, excepting Federal holidays.

3.5.2.3 Information Security Management

These criteria apply to the way in which the enterprise manages security for its business, the specified service and information relating to its user community. These criteria focus on the key components of an effective Information Security Management System (ISMS).

An enterprise and its specified service must:

AL2_CO_ISM#010 Documented policies and procedures

Have documented all security-relevant administrative, management and technical policies and procedures. The enterprise must ensure that these are based upon recognized standards or published references, are adequate for the specified service and are applied in the manner intended.

AL2_CO_ISM#020 Policy Management & Responsibility

Have a clearly defined managerial role, at a senior level, in which full responsibility for the business's security policies is vested and from which promulgation of policy and related procedures is controlled and managed. The policies in place must be properly maintained so as to be effective at all times.

AL2_CO_ISM#030 Risk Management

Demonstrate a risk management methodology that adequately identifies and mitigates risks related to the specified service and its user community.

AL2_CO_ISM#040 Continuity of Operations Plan

Have and shall keep updated a Continuity of Operations Plan that covers disaster recovery and the resilience of the specified service.

AL2_CO_ISM#050 Configuration Management

Demonstrate a Configuration Management system that at least includes:

- a) version control for software system components.
- b) timely identification and installation of all applicable patches for any software used in the provisioning of the specified service.

AL2_CO_ISM#060 Quality Management

Demonstrate a Quality Management system that is appropriate for the specified service.

AL2_CO_ISM#065 System Installation & Operation Controls

Apply controls during system development, procurement installation and operation that protect the security and integrity of the system environment, hardware, software and communications.

AL2_CO_ISM#070 Internal Service Audit

Unless it can show that by reason of its size or for other operational reason it is unreasonable, be regularly audited for effective provision of the specified service by internal audit functions independent of the parts of the enterprise responsible for the Specified Service.

AL2_CO_ISM#080 Independent Audit

Be audited by an independent auditor at least every 24 months to ensure the organization's security-related practices are consistent with the policies and procedures for the specified service and the appointed auditor must have appropriate accreditation or other acceptable experience and qualification.

AL2_CO_ISM#090 Audit Records

Retain full records of all audits, both internal and independent, for a period that, at a minimum, fulfills its legal obligations and otherwise for greater periods either as it may have committed to in its Service Definition or required by any other obligations it has with/to a Subscriber. Such records must be held securely and protected against loss, alteration or destruction.

AL2_CO_ISM#100 Termination provisions

Have in place a clear plan for the protection of subscribers' private and secret information related to their use of the service which must ensure the ongoing secure preservation and protection of legally required records and for the secure destruction and disposal of any such information whose retention is not legally required. Essential details of this plan must be published.

3.5.2.4 Security-relevant Event (Audit) Records

These criteria apply to the need to provide an auditable log of all events that are pertinent to the correct and secure operation of the service.

An enterprise and its specified service must:

AL2_CO_SER#010 Security event logging

Maintain a log of all security-relevant events concerning the operation of the service, together with a precise record of the time at which the event occurred (time-stamp) [AL4 provided by a trusted time-source]and such records must be retained with appropriate protection, accounting for service definition, risk management requirements and applicable legislation.

3.5.2.5 Operational infrastructure

These criteria apply to the infrastructure within which the delivery of the specified service takes place. These criteria emphasize the personnel involved and their selection, training and duties.

An enterprise and its specified service must:

AL2_CO_OPN#010 Technical security

Demonstrate that the technical controls employed will provide the level of security required by the risk assessment plan and the ISMS and that these controls are effectively integrated with the appropriate procedural and physical security measures.

AL2_CO_OPN#020 Defined security roles

Define by means of a job description the roles and responsibilities for every security-relevant task, relating it to specific procedures (which shall be set out in the ISMS) and other job descriptions. Where the role is security critical or where special privileges or shared duties exist, these must be specifically highlighted, including access privileges relating to logical and physical parts of the services operations.

AL2_CO_OPN#030 Personnel recruitment

Demonstrate that it has defined practices for the selection, evaluation and contracting of all personnel, both direct employees and those whose services are provided by third parties.

AL2_CO_OPN#040 Personnel skills

Ensure that employees are sufficiently trained, qualified, experienced and current for the roles they fulfill. Such measures must be accomplished either by recruitment practices or through a specific training program. Where employees are undergoing on-the-job training, they must only do so under the guidance of a mentor with established leadership skills.

AL2_CO_OPN#045 Adequacy of Personnel resources

Have sufficient staff to operate the Specified Service according to its policies and procedures.

AL2_CO_OPN#050 Physical access control

Apply physical access control mechanisms to ensure that access to sensitive areas is restricted to authorized personnel.

AL2_CO_OPN#060 Logical access control

Employ logical access control mechanisms to ensure that access to sensitive system functions and controls is restricted to authorized personnel.

3.5.2.6 External Services and Components

These criteria apply to the relationships and obligations upon contracted parties both to apply the policies and procedures of the

enterprise and also to be available for assessment as critical parts of the overall service provision.

An enterprise and its specified service must:

AL2_CO_ESC#010 Contracted policies and procedures

Where the enterprise uses the services of external suppliers for specific packaged components of the service or for resources that are integrated with its own operations and under its controls, ensure that those parties are engaged through reliable and appropriate contractual arrangements which stipulate critical policies, procedures and practices that the subcontractor is required to fulfill.

AL2_CO_ESC#020 Visibility of contracted parties

Where the enterprise uses the services of external suppliers for specific packaged components of the service or for resources that are integrated with its own operations and under its controls, ensure that contractors' compliance with contractually stipulated policies and procedures, and thus with EAP assessment criteria, can be proven and subsequently monitored.

3.5.2.7 Secure Communications

An enterprise and its specified service must:

AL2_CO_SCO#010 Secure remote communications

If the Specific Service components are located remotely from and communicate over a public or unsecured network with other service components or other CSP(s) it services, the communications must be cryptographically authenticated by an authentication method that meets, at a minimum, the requirements of AL2 and encrypted using a Federal Information Processing Standard (FIPS)-approved encryption method or a mechanism of demonstrably equivalent rigor.

AL2_CO_SCO#020 Protection of secrets

Ensure that:

- a) access to shared secrets shall be subject to discretionary controls that permit access to those roles/applications requiring such access.
- b) stored shared secrets are not held in their plaintext form.
- c) any long-term (i.e., not session) shared secrets are revealed only to the Subscriber and to CSP's direct agents (bearing in mind a, above).

3.5.3 ASSURANCE LEVEL 3 (SUBSTANTIAL)

Achieving AL3 requires meeting all criteria required to achieve AL2. This section includes only requirements additional to those described in Section 3.5.2.

3.5.3.1 Enterprise and Service Maturity

Criteria in this section address the establishment of the enterprise offering the service and its basic standing as a legal and operational business entity.

An enterprise and its specified service must:

AL3_CO_ESM#010 Established enterprise

Be a valid legal entity and a person with legal authority to commit the enterprise must submit the Assessment Package.

AL3_CO_ESM#020 Established service

Be described in the assessment package as it stands at the time of submission for assessment and must be assessed strictly against that description.

AL3_CO_ESM#040 Legal compliance

Set out and demonstrate that it understands and complies with any legal requirements incumbent on it in connection with operation and delivery of the specified service, accounting for all jurisdictions within which its services may be offered.

AL3_CO_ESM#050 Financial Provisions

Demonstrate that it has adequate financial resources for the continued operation of the service and has in place appropriate provision for the degree of liability exposure being carried.

AL3_CO_ESM#060 Data Retention and Protection

Specifically set out and demonstrate that it understands and complies with those legal and regulatory requirements incumbent upon it concerning the retention of private (personal and business) information (its secure storage and protection against loss and/or destruction) and the protection of private information (against unlawful or unauthorized access unless permitted by the information owner or required by due process).

AL3_CO_ESM#070 Ownership

If the enterprise named as the CSP is a part of a larger entity, the nature of the relationship with its parent organization shall be disclosed to the assessors and, on their request, to customers.

AL3_CO_ESM#080 Independent management and operations

Demonstrate that, for the purposes of providing the specified service, its management and operational structures are distinct, autonomous, have discrete legal accountability and function according to separate policies, procedures and controls.

3.5.3.2 Notices and User Information

Criteria in this section address the publication of information describing the service and the manner of and any limitations upon its provision, and how users are required to accept those terms.

An enterprise and its specified service must:

AL3_CO_NUI#010 General Service Definition

Make available to the intended user community a service definition for its specified service which includes any specific uses or limitations on its use, all applicable terms, conditions, fees and privacy policy for the service, including any limitations of its usage and definitions of any terms having specific intention or interpretation. Specific provisions are stated in further criteria in this section.

AL3_CO_NUI#020 Service Definition Sections

Publish a service definition for the specified service containing clauses which provide the following information:

- a) the legal jurisdiction under which the service is operated;
- b) if different to the above, the legal jurisdiction under which subscriber and any relying party agreements are entered into;
- c) applicable legislation with which the service complies;
- d) obligations incumbent upon the ETSP;
- e) obligations incumbent upon the subscriber;
- f) notifications and guidance for relying parties, especially in respect of actions they are expected to take should they choose to rely upon the service's product;
- g) statement of warranties;
- h) statement of liabilities;
- i) procedures for notification of changes to terms and conditions;
- j) steps the ETSP will take in the event that it chooses or is obliged to terminate the service;
- k) full contact details for the ETSP (i.e. conventional post, telephone, internet) including a helpdesk;
- l) availability of the specified service *per se* and of its help desk facility;
- m) termination of aspects or all of service.

AL3_CO_NUI#030 Due notification

Have in place and follow appropriate policy and procedures to ensure that it notifies subscribers in a timely and reliable fashion of any changes to the service definition and any applicable terms, conditions, fees and privacy policy for the specified service and provides a clear means by which subscribers may indicate that they wish to accept the new terms or terminate their subscription.

AL3_CO_NUI#034 Subscriber Information

Require the subscriber to provide full and correct information as required under the terms of their use of the service.

AL3_CO_NUI#036 Subscriber Agreement

Obtain a record (hard-copy or electronic) of the subscriber's agreement to the terms and conditions of service.

AL3_CO_NUI#038 Change of Subscriber Information

Require and provide the mechanisms for the Subscriber to provide in a timely manner full and correct amendments should any of their recorded information change, as required under the terms of their use of the service, and only after the subscriber's identity has been authenticated.

AL3_CO_NUI#040 Helpdesk facility

Ensure that its helpdesk is available for any queries related to the specified service during the regular business hours of its primary operational location, minimally from 9:00 a.m. through 5:00 p.m., Monday to Friday inclusive, excepting Federal holidays.

3.5.3.3

Information Security Management

Criteria in this section address the way in which the enterprise manages the security of its business, the specified service and information it holds relating to its user community. This focuses on the key components which make up a well-established Information Security Management System (ISMS).

An enterprise and its specified service must:

AL3_CO_ISM#010 Documented policies and procedures

Have documented all security relevant administrative management and technical policies and procedures. The enterprise must ensure that these are based upon recognized standards or published references are adequate for the specified service and are applied in the manner intended.

AL3_CO_ISM#020 Policy Management and Responsibility

Have a clearly defined managerial role, at a senior level, where full responsibility for the business' security policies is vested and from which promulgation of policy and related procedures is controlled and managed. The policies in place must be properly maintained so as to be effective at all times.

AL3_CO_ISM#030 Risk Management

Demonstrate a risk management methodology that adequately identifies and mitigates risks related to the specified service and its user community and must show that a risk assessment review is performed at least once every six months.

AL3_CO_ISM#040 Continuity of Operations Plan

Have and shall keep updated a continuity of operations plan that covers disaster recovery and the resilience of the specified service and must show that a review of this plan is performed at least once every six months.

AL3_CO_ISM#050 Configuration Management

Demonstrate a configuration management system that at least includes:

- a) version control for software system components;
- b) timely identification and installation of all applicable patches for any software used in the provisioning of the specified service;
- c) version control and managed distribution for all documentation associated with the specification, management and operation of the system, covering both internal and publicly available materials.

AL3_CO_ISM#060 Quality Management

Demonstrate a quality management system that is appropriate for the specified service.

AL3_CO_ISM#065 System Installation and Operation Controls

Apply controls during system development, procurement, installation and operation that protect the security and integrity of the system environment, hardware, software and communications having particular regard to:

- a) the software and hardware development environments, for customized components.
- b) the procurement process for commercial off-the-shelf (COTS) components.
- c) contracted consultancy/support services.
- d) shipment of system components.
- e) storage of system components.
- f) installation environment security.
- g) system configuration.
- h) transfer to operational status.

AL3_CO_ISM#070 Internal Service Audit

Unless it can show that by reason of its size or for other arguable operational reason it is unreasonable so to perform, be regularly audited for effective provision of the specified service by internal audit functions independent of the parts of the enterprise responsible for the specified service.

AL3_CO_ISM#080 Independent Audit

Be audited by an independent auditor at least every 24 months to ensure the organization's security-related practices are consistent with the policies and procedures for the specified service and the appointed auditor must have appropriate accreditation or other acceptable experience and qualification.

AL3_CO_ISM#090 Audit Records

Retain full records of all audits, both internal and independent, for a period which, as a minimum, fulfils its legal obligations and otherwise for greater periods either as it may have committed to in its service definition or required by any other obligations it has with/to a subscriber. Such records must be held securely and protected against loss, alteration or destruction.

AL3_CO_ISM#100 Termination provisions

Have in place a clear plan for the protection of subscribers' private and secret information related to their use of the service which must ensure the ongoing secure preservation and protection of legally-required records and for the secure destruction and disposal of any such information whose retention is not legally required. Essential details of this plan must be published.

AL3_CO_ISM#110 Best Practice Security Management

Have in place an Information Security Management System (ISMS) that follows best practices as accepted by the information security industry and that applies and is appropriate to the CSP in question. All requirements defined by preceding criteria in this section must fall wholly within the scope of this ISMS.

3.5.3.4

Security-Relevant Event (Audit) Records

The criteria in this section are concerned with the need to provide an auditable log of all events which are pertinent to the correct and secure operation of the service.

An enterprise and its specified service must:

AL3_CO_SER#010 Security Event Logging

Maintain a log of all security-relevant events concerning the operation of the service, together with a precise record of the time at which the event occurred (time-stamp).

3.5.3.5

Operational Infrastructure

The criteria in this section address the infrastructure within which the delivery of the specified service takes place. It puts particular emphasis upon the personnel involved, and their selection, training and duties.

An enterprise and its specified service must:

AL3_CO_OPN#010 Technical security

Demonstrate that the technical controls employed will provide the level of security required by the risk assessment plan and the ISMS, and that these controls are effectively integrated with the appropriate procedural and physical security measures.

AL3_CO_OPN#020 Defined security roles

Define by means of a job description the roles and responsibilities for every security-relevant task, relating it to specific procedures (which shall be set out in the ISMS) and other job descriptions. Where the role is security critical or where special privileges or shared duties exist these must be specifically highlighted, including access privileges relating to logical and physical parts of the services operations.

AL3_CO_OPN#030 Personnel recruitment

Demonstrate that there are defined practices for the selection, vetting and contracting of all personnel, both direct employees and those whose services are provided by third parties. Full records of all searches and supporting evidence of qualifications and past employment must be kept for the duration of the individual's employment plus the longest lifespan of any credential issued under the service policy.

AL3_CO_OPN#040 Personnel skills

Ensure that employees are sufficiently trained, qualified, experienced and current for the roles they fulfill. Such measures must be accomplished either by recruitment practices or through a specific training program. Where employees are undergoing on the job training they must only do so under the guidance of a mentor with established leadership skills.

AL3_CO_OPN#045 Adequacy of Personnel resources

Have sufficient staff to operate the specified service according to its policies and procedures.

AL3_CO_OPN#050 Physical access control

Apply physical access control mechanisms to ensure access to sensitive areas is restricted to authorized personnel.

AL3_CO_OPN#060 Logical access control

Employ logical access control mechanisms to ensure access to sensitive system functions and controls is restricted to authorized personnel.

3.5.3.6 External Services and Components

This section addresses the relationships and obligations upon contracted parties both to apply the policies and procedures of the enterprise and also to be available for assessment as critical parts of the overall service provision.

An enterprise and its specified service must:

AL3_CO_ESC#010 Contracted policies and procedures

Where the enterprise uses the services of external suppliers for specific packaged components of the service or for resources which are integrated with its own operations and under its controls, ensure that those parties are engaged through reliable and appropriate contractual arrangements which stipulate critical policies, procedures and practices that the sub-contractor is required to fulfill.

AL3_CO_ESC#020 Visibility of contracted parties

Where the enterprise uses the services of external suppliers for specific packaged components of the service or for resources which are integrated with its own operations and under its controls, ensure that contractors' compliance with contractually stipulated policies and procedures, and thus with the EAP's assessment criteria, can be proven and subsequently monitored.

3.5.3.7 Secure Communications

An enterprise and its specified service must:

AL3_CO SCO#010 Secure remote communications

If the Specific Service components are located remotely from and communicate over a public or unsecured network with other service components or other CSPs it services, the communications must be cryptographically authenticated by an authentication protocol that meets, at a minimum, the requirements of AL3] and encrypted using an Approved Encryption method.

AL3_CO SCO#020 Protection of secrets

Ensure that:

- a) access to shared secrets shall be subject to discretionary controls that permit access to those roles/applications requiring such access.
- b) stored shared secrets are encrypted such that
 - i the encryption key for the shared secret file is encrypted under a key held in a FIPS 140-2 Level 2 (or higher) validated hardware cryptographic module or any FIPS 140-2 Level 3 or 4 cryptographic module and decrypted only as immediately required for an authentication operation.
 - ii they are protected as a key within the boundary of a FIPS 140-2 Level 2 (or higher) validated hardware cryptographic module or any FIPS 140-2 Level 3 or 4 cryptographic module and are not exported in plaintext from the module.
 - iii they are split by an '*n from m*' cryptographic secret-sharing method.
- c) any long-term (i.e., not session) shared secrets are revealed only to the Subscriber and CSP direct agents (bearing in mind a, above).

3.5.4 ASSURANCE LEVEL 4 (HIGH)

Achieving AL4 requires meeting all criteria required to achieve AL3. This section includes only requirements additional to those described in Section 3.5.3.

3.5.4.1 Enterprise and Service Maturity

Criteria in this section address the establishment of the enterprise offering the service and its basic standing as a legal and operational business entity.

An enterprise and its specified service must:

AL4_CO ESM#010 Established enterprise

Be a valid legal entity and a person with legal authority to commit the enterprise must submit the Assessment Package.

AL4_CO ESM#020 Established service

Be described in the Assessment Package as it stands at the time of submission for assessment and must be assessed strictly against that description.

AL4_CO ESM#040 Legal compliance

Set out and demonstrate that it understands and complies with any legal requirements incumbent on it in connection with

operation and delivery of the specified service, accounting for all jurisdictions within which its services may be offered.

AL4_CO_ESM#050 Financial Provisions

Demonstrate that it has adequate financial resources for the continued operation of the service and has in place appropriate provision for the degree of liability exposure being carried.

AL4_CO_ESM#060 Data Retention and Protection

Specifically set out and demonstrate that it understands and complies with those legal and regulatory requirements incumbent upon it concerning the retention of private (personal and business) information (its secure storage and protection against loss and/or destruction) and the protection of private information (against unlawful or unauthorized access unless permitted by the information owner or required by due process).

AL4_CO_ESM#070 Ownership

If the enterprise named as the ETSP is a part of a larger entity, the nature of the relationship with its parent organization, shall be disclosed to the assessors and, on their request, to customers.

AL4_CO_ESM#080 Independent Management and Operations

Demonstrate that, for the purposes of providing the specified service, its management and operational structures are distinct, autonomous, have discrete legal accountability and function according to separate policies, procedures and controls.

3.5.4.2

Notices and User Information/Agreements

Criteria in this section address the publication of information describing the service and the manner of and any limitations upon its provision, and how users are required to accept those terms.

An enterprise and its specified service must:

AL4_CO_NUI#010 General Service Definition

Make available to the intended user community a Service Definition for its specified service which includes any specific uses or limitations on its use, all applicable Terms, Conditions, Fees and Privacy Policy for the service, including any limitations of its usage and definitions of any terms having specific intention or interpretation. Specific provisions are stated in further criteria in this section.

AL4_CO_NUI#020 Service Definition Sections

Publish a Service Definition for the specified service containing clauses which provide the following information:

- a) the legal jurisdiction under which the service is operated;

- b) if different to the above, the legal jurisdiction under which subscriber and any relying party agreements are entered into;
- c) applicable legislation with which the service complies;
- d) obligations incumbent upon the ETSP;
- e) obligations incumbent upon the subscriber;
- f) notifications and guidance for relying parties, especially in respect of actions they are expected to take should they choose to rely upon the service's product;
- g) statement of warranties;
- h) statement of liabilities;
- i) procedures for notification of changes to terms and conditions;
- j) steps the ETSP will take in the event that it chooses or is obliged to terminate the service;
- k) full contact details for the ETSP (i.e. conventional post, telephone, internet) including a helpdesk;
- l) availability of the specified service *per se* and of its help desk facility;
- m) termination of aspects or all of service.

AL4_CO_NUI#030 Due Notification

Have in place and follow appropriate policy and procedures to ensure that it notifies subscribers in a timely and reliable fashion of any changes to the service definition and any applicable terms, conditions, fees and privacy policy for the specified service and provides a clear means by which subscribers may indicate that they wish to accept the new terms or terminate their subscription.

AL4_CO_NUI#034 Subscriber Information

Require the Subscriber to provide full and correct information as required under the terms of their use of the service.

AL4_CO_NUI#036 Subscriber Agreement

Obtain a record (hard-copy or electronic) of the Subscriber's Agreement to the Terms and Conditions of service.

AL4_CO_NUI#038 Change of Subscriber Information

Require and provide the mechanisms for the Subscriber to provide in a timely manner full and correct amendments should any of their recorded information change, as required under the terms of their use of the service, and only after the subscriber's identity has been authenticated.

AL4_CO_NUI#040 Helpdesk facility

Ensure that its helpdesk is available for any queries related to the specified service during the regular business hours of its primary operational location, minimally from 9:00 a.m. to 5:00 p.m., Monday to Friday inclusive, excepting Federal holidays.

3.5.4.3 Information Security Management

Criteria in this section address the way in which the enterprise manages the security of its business, the specified service and information it holds relating to its user community. This focuses

on the key components which make up a well-established Information Security Management System (ISMS).

An enterprise and its specified service must:

AL4_CO_ISM#010 Documented policies and procedures

Have documented all security-relevant administrative, management and technical policies and procedures. The enterprise must ensure that these are based upon recognized standards or published references, are adequate for the specified service and are applied in the manner intended.

AL4_CO_ISM#020 Policy Management and Responsibility

Have a clearly defined managerial role, at a senior level, where full responsibility for the business' security policies is vested and from which promulgation of policy and related procedures is controlled and managed. The policies in place must be properly maintained so as to be effective at all times.

AL4_CO_ISM#030 Risk Management

Demonstrate a risk management methodology that adequately identifies and mitigates risks related to the specified service and its user community and must show that on-going risk assessment review is conducted as a part of the business' procedures.

AL4_CO_ISM#040 Continuity of Operations Plan

Have and shall keep updated a continuity of operations plan that covers disaster recovery and the resilience of the specified service and must show that on-going review of this plan is conducted as a part of the business' procedures.

AL4_CO_ISM#050 Configuration Management

Demonstrate a Configuration Management system that at least includes:

- a) version control for software system components;
- b) timely identification and installation of all applicable patches for any software used in the provisioning of the specified service;
- c) version control and managed distribution for all documentation associated with the specification, management and operation of the system, covering both internal and publicly available materials.

AL4_CO_ISM#060 Quality Management

Demonstrate a Quality Management system that is appropriate for the specified service.

AL4_CO_ISM#065 System Installation and Operation Controls

Apply controls during system development, procurement installation and operation which protect the security and integrity of the system environment, hardware, software and communications having particular regard to:

- a) the software and hardware development environments, for customized components;

- b) the procurement process for COTS components;
- c) contracted consultancy/support services;
- d) shipment of system components;
- e) storage of system components;
- f) installation environment security;
- g) system configuration;
- h) transfer to operational status.

AL4_CO_ISM#070 Internal Service Audit

Unless it can show that by reason of its size or for other arguable operational reason it is unreasonable so to perform, be regularly audited for effective provision of the specified service by internal audit functions independent of the parts of the enterprise responsible for the Specified Service.

AL4_CO_ISM#080 Independent Audit

Be audited by an independent auditor at least every 24 months to ensure the organization's security-related practices are consistent with the policies and procedures for the specified service and the appointed auditor must have appropriate accreditation or other acceptable experience and qualification.

AL4_CO_ISM#090 Audit Records

Retain full records of all audits, both internal and independent, for a period which, as a minimum, fulfils its legal obligations and otherwise for greater periods either as it may have committed to in its Service Definition or required by any other obligations it has with/to a Subscriber. Such records must be held securely and protected against loss, alteration or destruction.

AL4_CO_ISM#100 Termination provisions

Have in place a clear plan for the protection of subscribers' private and secret information related to their use of the service which must ensure the ongoing secure preservation and protection of legally-required records and for the secure destruction and disposal of any such information whose retention is not legally required. Essential details of this plan must be published.

AL4_CO_ISM#110 Best Practice Security Management

Have in place a certified Information Security Management System (ISMS) which has been assessed and found to be in compliance with the code of practice ISO/IEC 17799 through application of practices defined in BS 7799 Part 2 and which applies and is appropriate to the ETPS in question. All requirements expressed in preceding criteria in this 'ISM' section must *inter alia* fall wholly within the scope of this ISMS.

3.5.4.4 Security-Related (Audit) Records

The criteria in this section are concerned with the need to provide an auditable log of all events which are pertinent to the correct and secure operation of the service.

An enterprise and its specified service must:

AL4_CO_SER#010 Security Event Logging

Maintain a log of all security-relevant events concerning the operation of the service, together with a precise record of the time at which the event occurred (time-stamp) provided by a trusted time-source and such records must be retained with appropriate protection, accounting for service definition, risk management requirements and applicable legislation.

3.5.4.5 Operational Infrastructure

The criteria in this section address the infrastructure within which the delivery of the specified service takes place. It puts particular emphasis upon the personnel involved, and their selection, training and duties.

An enterprise and its specified service must:

AL4_CO_OPN#010 Technical Security

Demonstrate that the technical controls employed will provide the level of security required by the risk assessment plan and the ISMS, and that these controls are effectively integrated with the appropriate procedural and physical security measures.

AL4_CO_OPN#020 Defined Security Roles

Define by means of a job description the roles and responsibilities for every security-relevant task, relating it to specific procedures (which shall be set out in the ISMS) and other job descriptions. Where the role is security critical or where special privileges or shared duties exist these must be specifically highlighted, including access privileges relating to logical and physical parts of the services operations.

AL4_CO_OPN#030 Personnel Recruitment

Demonstrate that there are defined practices for the selection, vetting and contracting of all personnel, both direct employees and those whose services are provided by third parties. Full records of all searches and supporting evidence of qualifications and past employment must be kept for the duration of the individual's employment plus the longest lifespan of any credential issued under the service policy.

AL4_CO_OPN#040 Personnel skills

Ensure that employees are sufficiently trained, qualified, experienced and current for the roles they fulfill. Such measures must be accomplished either by recruitment practices or through a specific training program. Where employees are undergoing on the job training they must only do so under the guidance of a mentor with established leadership skills.

AL4_CO_OPN#045 Adequacy of Personnel resources

Have sufficient staff to operate the Specified Service according to its policies and procedures.

AL4_CO_OPN#050 Physical access control

Apply physical access control mechanisms to ensure access to sensitive areas is restricted to authorized personnel.

AL4_CO_OPN#060 Logical access control

Employ logical access control mechanisms to ensure access to sensitive system functions and controls is restricted to authorized personnel.

3.5.4.6 External Services and Components

This section addresses the relationships and obligations upon contracted parties both to apply the policies and procedures of the enterprise and also to be available for assessment as critical parts of the overall service provision.

An enterprise and its specified service must:

AL4_CO_ESC#010 Contracted Policies and Procedures

Where the enterprise uses the services of external suppliers for specific packaged components of the service or for resources which are integrated with its own operations and under its controls, ensure that those parties are engaged through reliable and appropriate contractual arrangements which stipulate critical policies, procedures and practices that the sub-contractor is required to fulfill.

AL4_CO_ESC#020 Visibility of Contracted Parties

Where the enterprise uses the services of external suppliers for specific packaged components of the service or for resources which are integrated with its own operations and under its controls, ensure that contractors' compliance with contractually stipulated policies and procedures, and thus with the EAP's assessment criteria, can be proven and subsequently monitored.

3.5.4.7 Secure Communications

An enterprise and its specified service must:

AL4_CO_SCO#010 Secure remote communications

If the specific service components are located remotely from and communicate over a public or unsecured network with other service components or other ETSP(s) it services, the communications must be cryptographically authenticated by an authentication protocol that meets, as a minimum, the requirements of AL4 and encrypted using an approved encryption method.

AL4_CO SCO#020 Protection of secrets

Ensure that:

- a) access to shared secrets shall be subject to discretionary controls which permit access to those roles/applications which need such access;
- b) stored shared secrets are encrypted such that:
- c) the encryption key for the shared secret file is encrypted under a key held in a FIPS 140-2¹ Level 2 or higher validated hardware cryptographic module or any FIPS 140-2 Level 3 or 4 cryptographic module and decrypted only as immediately required for an authentication operation;
- d) they are protected as a key within the boundary of a FIPS 140-2 Level 2 or higher validated hardware cryptographic module or any FIPS 140-2 Level 3 or 4 cryptographic module and is not exported in plaintext from the module;
- e) they are split by an '*n from m*' cryptographic secret-sharing method.
- f) any long-term (i.e. not session) shared secrets are revealed only to the Subscriber and the ETSP's direct agents (bearing in mind (a) above).

3.6 Identity Proofing Service Assessment Criteria

The Service Assessment Criteria in this section establish the requirements for the technical conformity of identity-proofing services at all ALs defined in Section 2.

These criteria apply to a particular kind of electronic trust service (ETS) recognized by the EAP and to the related electronic trust service provider (ETSP)—an identity proofing service. (For definitions of terms used in this section, see Section 5).

These criteria are generally referred to elsewhere within EAP documentation as ID-SAC.

These criteria do not address the delivery of a credential to the applicant/subscriber, which is dealt with by the Credential Management SAC (CM-SAC), described in Section 3.7.

These criteria may only be used in an assessment in one of the following circumstances:

- In conjunction with the Common Organizational SAC (CO-SAC), described in Section 3.5, for a standalone identity proofing service.
- In combination with one or more other SACs that must include the CO-SAC and where the identity proofing functions that these criteria address form part of a larger service offering.

3.6.1 ASSURANCE LEVEL 1 (MINIMAL)

3.6.1.1 Policy

An enterprise or specified service must:

¹ FIPS PUB 140-2 Security Requirements for Cryptographic Modules

AL1_ID_POL#010 Unique service identity

Ensure that a unique identity is attributed to the specific service, such that credentials issued by it can be distinguishable from those issued by other services, including services operated by the same enterprise.

AL1_ID_POL#020 Unique subject identity

Ensure that each Applicant's identity is unique within the service's community of subjects and uniquely associable with tokens and/or credentials issued to that identity.

3.6.1.2 Identity Verification

3.6.1.2.1 In-Person Public Verification

An enterprise or specified service must:

AL1_ID_IPV#010 Required evidence

Ensure that the Applicant possesses any one of the following forms of evidence:

- a) one form of Federal or state-issued identity.
- b) one signed bank or credit card.
- c) two utility statements.
- d) any other equivalent form of proof.

AL1_ID_IPV#020 Evidence checks

Ensure that the name on the evidence offered bears the name the Applicant claims and in addition establish, according to the form of evidence provided, any one of the following:

- a) the Applicant appears to be the person named.
- b) the Applicant can reproduce any signatures shown on bank cards.
- c) addresses provided are consistent.
- d) any other checks that establish an equivalent degree of certitude.

3.6.1.2.2 Remote Public Verification

If the specific service offers remote identity proofing to applicants with whom it has no previous relationship, then it must comply with the criteria in this section.

An enterprise or specified service must::

AL1_ID_RPV#010 Required evidence

Require the Applicant to provide a contact telephone number or email address.

AL1_ID_RPV#020 Evidence checks

Verify the provided information by either:

- a) confirming the request by calling the number.
- b) successfully sending a confirmatory email and receiving a positive acknowledgement.

3.6.1.2.3 Secondary Verification

In each of the above cases an enterprise or specified service must:

AL1_ID_SCV#010 Secondary checks

Have in place additional measures (e.g., require additional documentary evidence, delay completion while out-of-band checks are undertaken) to deal with any anomalous circumstances that can be reasonably anticipated (e.g., a legitimate and recent change of address that has yet to be established as the address of record).

3.6.1.3 Verification Records

No criteria.

3.6.2 ASSURANCE LEVEL 2 (MODERATE)

3.6.2.1 Policy

The specific service must show that it applies identity proofing policies and procedures and that it retains appropriate records of identity proofing activities and evidence.

The enterprise or specified service must:

AL2_ID_POL#010 Unique service identity

Ensure that a unique identity is attributed to the specific service, such that credentials issued by it can be distinguishable from those issued by other services, including services operated by the same enterprise.

AL2_ID_POL#020 Unique subject identity

Ensure that each Applicant's identity is unique within the service's community of subjects and uniquely associable with tokens and/or credentials issued to that identity.

AL2_ID_POL#030 Published Proofing Policy

Publish the Identity Proofing Policy under which it verifies the identity of applicants² in form, language and media accessible to the declared community of users.

AL2_ID_POL#040 Adherence to Proofing Policy

Perform all identity proofing strictly in accordance with its published Identity Proofing Policy, through application of the procedures and processes set out in its Identity Proofing Practice Statement.

3.6.2.2 Identity Verification

The specific service must offer at least one of the following classes of identity proofing service and may offer any additional sets it chooses, subject to the nature and the entitlement of the CSP concerned.

² For an identity proofing service that is within the management scope of a credential management service provider, this should be the credential management service's definitive policy; for a stand-alone identity proofing service, the policy may be either that of a client who has defined one through contract, the ID service's own policy or a separate policy that explains how the client's policies will be complied with.

3.6.2.2.1 *In-Person Public Verification*

If the specific service offers in-person identity proofing to applicants with whom it has no previous relationship, then it must comply with the criteria in this section.

The enterprise or specified service must:

AL2_ID_IPV#010 Required evidence

Ensure that the Applicant is in possession of a primary Government Picture ID document that bears a photographic image of the holder.

AL2_ID_IPV#020 Evidence checks

Ensure that the presented document:

- a) appears to be a genuine document properly issued by the claimed issuing authority and valid at the time of application.
- b) bears a photographic image of the holder that matches that of the Applicant;
- c) states an address at which the Applicant can be contacted.

3.6.2.2.2 *Remote Public Verification*

If the specific service offers remote identity proofing to applicants with whom it has no previous relationship, then it must comply with the criteria in this section.

An enterprise or specified service must:

AL2_ID_RPV#010 Required evidence

Ensure that the Applicant submits the references of and attests to current possession of a primary Government Picture ID document, and provides additional verifiable personal information that at a minimum must include:

- a) a name that matches the referenced photo-ID.
- b) date of birth.
- c) current address or personal telephone number.
- d) the issuer, account number and expiration date of a current credit card.

Additional information may be requested so as to ensure a unique identity, and alternative information may be sought where the enterprise can show that it leads to at least the same degree of certitude when verified.

AL2_ID_RPV#020 Evidence checks

Electronically verify by a record check against the provided identity references with the specified issuing authorities/institutions or through similar databases:

- a) the existence of such records with matching name and reference numbers;
- b) corroboration of date of birth, current address of record and other personal information sufficient to ensure a unique identity.

Additional checks may be performed so as to establish the uniqueness of the claimed identity, and alternative checks may be performed where the enterprise can show that they lead to at least the same degree of certitude.

3.6.2.2.3 Current Relationship Verification

If the specific service offers identity proofing to applicants with whom it has a current relationship, then it must comply with the criteria in this section.

The enterprise or specified service must:

AL2_ID_CRV#010 Required evidence

Ensure that it has previously exchanged a shared secret (e.g., a PIN or password) with the applicant.

AL2_ID_CRV#010 Evidence checks

Ensure that it has:

- a) only issued the shared secret after originally establishing the applicant's identity with a degree of rigor equivalent to that required under either the AL2 (or higher) requirements for in-person or remote public verification
- b) an ongoing business relationship sufficient to satisfy the enterprise of the applicant's continued personal possession of the shared secret.

3.6.2.2.4 Affiliation Verification

If the specific service offers identity proofing to applicants on the basis of some form of affiliation, then it must comply with the criteria in this section for the purposes of establishing that affiliation, in addition to the previously stated requirements for the verification of the individual's identity.

The enterprise or specified service must:

AL2_ID_AFV#010 Required evidence

Ensure that the Applicant possesses:

- a) identification from the organization with which it is claiming Affiliation.
- b) agreement from the organization that the Applicant may be issued a credential indicating that an affiliation exists.

AL2_ID_AFV#020 Evidence checks

Ensure that the presented documents:

- a) each appear to be a genuine document properly issued by the claimed issuing authorities and valid at the time of application.
- b) refer to an existing organization, with a contact address.
- c) indicate that the Applicant has some form of recognizable affiliation with the organization.
- d) appear to grant the Applicant an entitlement to obtain a credential indicating its affiliation with the organization.

3.6.2.2.5 Secondary Verification

In each of the above cases the enterprise or specified service must:

AL2_ID_SCV#010 Secondary checks

Have in place additional measures (e.g., require additional documentary evidence, delay completion while out-of-band checks are undertaken) to

deal with any anomalous circumstances that can be reasonably anticipated (e.g., a legitimate and recent change of address that has yet to be established as the address of record).

3.6.2.3 Verification Records

The specific service must retain records of the identity proofing (verification) that it undertakes.

An enterprise or specified service must:

AL2_ID_VRC#010 Verification Records for Personal Applicants

Log, taking account of all applicable legislative and policy obligations, a record of the facts of the verification process. At a minimum, records of identity information must include:

- a) the Applicant's full legal name.
- b) the Applicant's date of birth.
- c) the Applicant's current address of record.
- d) the Subscriber's current telephone or email address of record.
- e) type, issuing authority and reference number(s) of all documents checked in the identity proofing process.
- f) where required, a telephone or email address for related contact and/or delivery of credentials/notifications.
- g) any pseudonym used by the Applicant in lieu of the verified identity.
- h) date and time of verification.

AL2_ID_VRC#020 Verification Records for Affiliated Applicants

In addition to the foregoing, log, taking account of all applicable legislative and policy obligations, a record of the additional facts of the verification process. At a minimum, records of identity information must include:

- a) the Subscriber's full legal name.
- b) the Subscriber's current address of record.
- c) the Subscriber's current telephone or email address of record.
- d) the Subscriber's acknowledgement for issuing the Subject with a credential.
- e) type, issuing authority and reference number(s) of all documents checked in the identity proofing process.

AL2_ID_VRC#040 Record Retention

Either retain securely the record of the verification process for the duration of the subscriber account plus 7.5 years, or submit same record to a client CSP that has undertaken to retain the record for the requisite period or longer.

3.6.3 ASSURANCE LEVEL 3 (SUBSTANTIAL)

3.6.3.1 Policy

The specific service must show that it applies identity-proofing policies and procedures and that it retains appropriate records of identity-proofing activities and evidence.

The enterprise or specified service must:

AL3_ID_POL#010 Unique service identity

Ensure that a unique identity is attributed to the specific service, such that credentials issued by it can be distinguishable from those issued by other services, including services operated by the same enterprise.

AL3_ID_POL#020 Unique subject identity

Ensure that each Applicant's identity is unique within the service's community of subjects and uniquely associable with tokens and/or credentials issued to that identity.

AL3_ID_POL#030 Published Proofing Policy

Publish the Identity Proofing Policy under which it verifies the identity of applicants³ in form, language and media accessible to the declared community of Users.

AL3_ID_POL#040 Adherence to Proofing Policy

Perform all identity proofing strictly in accordance with its published Identity Proofing Policy, applying the procedures and processes set out in its Identity Proofing Practice Statement.

3.6.3.2 Identity Verification

The specific service must offer at least one of the following classes of identity proofing services and may offer any additional services it chooses, subject to the nature and the entitlement of the CSP concerned.

3.6.3.2.1 In-Person Public Verification

A specific service that offers identity proofing to applicants with whom it has no previous relationship must comply with the criteria in this section.

The enterprise or specified service must:

AL3_ID_IPV#010 Required evidence

Ensure that the Applicant is in possession of a primary Government Picture ID document that bears a photographic image of the holder.

AL3_ID_IPV#020 Evidence checks

Ensure that the presented document:

- a) appears to be a genuine document properly issued by the claimed issuing authority and valid at the time of application.
- b) bears a photographic image of the holder that matches that of the Applicant.
- c) states an address at which the Applicant can be contacted.

³ For an identity proofing service that is within the management scope of a Credential Management service provider, this should be the Credential Management service's definitive policy; for a stand-alone identity proofing service, the policy may be either that of a client who has defined one through contract, the ID service's own policy or a separate policy that explains how the client's policies will be complied with.

- d) is electronically verified by a record check with the specified issuing authority or through similar databases that:
 - i) establishes the existence of such records with matching name and reference numbers.
 - ii) corroborates date of birth, current address of record and other personal information sufficient to ensure a unique identity.

3.6.3.2.2 *Remote Public Verification*

A specific service that offers remote identity proofing to applicants with whom it has no previous relationship must comply with the criteria in this section.

The enterprise or specified service must:

AL3_ID_RPV#010 Required evidence

Ensure that the Applicant submits details of and attests to current possession of:

- a) a primary Government Picture ID document, and either
 - i) an account number issued by a regulated financial institution.
 - ii) a source of personal information relating to the applicant.

AL3_ID_RPV#020 Evidence checks

Electronically verify by a record check against the provided identity references with the specified issuing authorities/institutions or through similar databases:

- a) the existence of such records with matching name and reference numbers.
- b) corroboration of date of birth, current address of record or personal telephone number, and other personal information sufficient to ensure a unique identity.
- c) dynamic verification of personal information previously provided by or likely to be known only by the applicant.

3.6.3.2.3 *Affiliation Verification*

A specific service that offers identity proofing to applicants on the basis of some form of affiliation must comply with the criteria in this section to establish that affiliation and with the previously stated requirements to verify the individual's identity.

The enterprise or specified service must:

AL3_ID_AFV#010 Required evidence

Ensure that the Applicant possesses:

- a) identification from the organization with which it is claiming Affiliation.
- b) agreement from the organization that the Applicant may be issued a credential indicating that an affiliation exists.

AL3_ID_AFV#020 Evidence checks

Ensure that the presented documents:

- a) each appear to be a genuine document properly issued by the claimed issuing authorities and valid at the time of application.
- b) refer to an existing organization, with a contact address.

- c) indicate that the Applicant has some form of recognizable affiliation with the organization.
- d) appear to grant the Applicant an entitlement to obtain a credential indicating an affiliation with the organization.

3.6.3.2.4 Secondary Verification

In each of the above cases, the enterprise or specified service must also meet the following criteria:

AL3_ID_SCV#010 Secondary checks

Have in place additional measures (e.g., require additional documentary evidence, delay completion while out-of-band checks are undertaken) to deal with any anomalous circumstance that can reasonably be anticipated (e.g., a legitimate and recent change of address that has yet to be established as the address of record).

3.6.3.3 Verification Records

The specific service must retain records of the identity proofing (verification) that it undertakes.

The enterprise or specified service must:

AL3_ID_VRC#010 Verification Records

Log, taking account of all applicable legislative and policy obligations, a record of the facts of the verification process. At a minimum, records of identity information must include:

- a) the Applicant's full legal name.
- b) the Applicant's date and place of birth (as declared, but not necessarily verified).
- c) the Applicant's current address of record.
- d) the Subscriber's current telephone or email address of record.
- e) type, issuing authority and reference number(s) of all documents checked in the identity proofing process.
- f) any pseudonym used by the Applicant in lieu of the verified identity.
- g) date and time of verification.
- h) where the identity proofing is conducted in person, the signature of the Applicant.
- i) identity of the registrar.
- j) identity of the CSP providing the verification service or the location at which the (in-house) verification was performed.

AL3_ID_VRC#020 Verification Records for Affiliated Applicants

In addition to the foregoing, log, taking account of all applicable legislative and policy obligations, a record of the additional facts of the verification process. At a minimum, records of identity information must include:

- a) the Subscriber's full legal name.
- b) the Subscriber's current address of record.
- c) the Subscriber's current telephone or email address of record.
- d) the Subscriber's acknowledgement of issuing the subject with a credential.
- e) type, issuing authority and reference number(s) of all documents checked in the identity-proofing process.

- f) where required, a telephone or email address for related contact and/or delivery of credentials/notifications.

AL3_ID_VRC#040 Record Retention

Either retain securely the record of the verification/revocation process for the duration of the Subscriber account plus 7.5 years, or submit the same record to a client CSP that has undertaken to retain the record for the requisite period or longer.

3.6.4 ASSURANCE LEVEL 4 (HIGH)

Identity proofing at Assurance Level 4 requires the physical presence of the applicant in front of the registration officer with photo ID or other readily verifiable biometric identity information, as well as the requirements set out by the following criteria.

3.6.4.1 Policy

The specific service must show that it applies identity-proofing policies and procedures and that it retains appropriate records of identity-proofing activities and evidence.

The enterprise or specified service must:

AL4_ID_POL#010 Unique service identity

Ensure that a unique identity is attributed to the specific service, such that credentials issued by it can be distinguishable from those issued by other services, including services operated by the same enterprise.

AL4_ID_POL#020 Unique subject identity

Ensure that each Applicant's identity is unique within the service's community of subjects and uniquely associable with tokens and/or credentials issued to that identity.

AL4_ID_POL#030 Published Proofing Policy

Publish the Identity Proofing Policy under which it verifies the identity of applicants⁴ in form, language and media accessible to the declared community of users.

AL4_ID_POL#040 Adherence to Proofing Policy

Perform all identity proofing strictly in accordance with its published Identity Proofing Policy, applying the procedures and processes set out in its Identity Proofing Practice Statement.

3.6.4.2 Identity Verification

The specific service may offer only face-to-face identity proofing service. Remote verification is not allowed at this level.

⁴ For an identity proofing service that is within the management scope of a credential management service provider, this should be the credential management service's definitive policy; for a stand-alone identity proofing service, the policy may be either that of a client which has defined one through contract, the ID service's own policy or a separate policy that explains how the client's policies will be complied with.

The enterprise or specified service must:

3.6.4.2.1 *In-Person Public Verification*

AL4_ID_IPV#010 Required evidence

Ensure that the Applicant is in possession of:

- a) a primary Government Picture ID document that bears a photographic image of the holder and either
 - i) secondary Government Picture ID or an account number issued by a regulated financial institution.
 - ii) two items confirming name, and address or telephone number, such as: utility bill, professional license or membership, or other evidence of equivalent standing.

AL4_ID_IPV#020 Evidence checks – primary ID

Ensure that the presented document:

- a) appears to be a genuine document properly issued by the claimed issuing authority and valid at the time of application.
- b) bears a photographic image of the holder which matches that of the Applicant.
- c) states an address at which the Applicant can be contacted.
- d) is electronically verified by a record check with the specified issuing authority or through similar databases that:
 - i) establishes the existence of such records with matching name and reference numbers.
 - ii) corroborates date of birth, current address of record and other personal information sufficient to ensure a unique identity.

AL4_ID_IPV#030 Evidence checks – secondary ID

Ensure that the presented document meets the following conditions:

- 1) If it is secondary Government Picture ID,
 - a) appears to be a genuine document properly issued by the claimed issuing authority and valid at the time of application.
 - b) bears a photographic image of the holder which matches that of the applicant.
 - c) states an address at which the Applicant can be contacted.
- 2) If it is a financial institution account number,
 - a) is verified by a record check with the specified issuing authority or through similar databases that :
 - i) establishes the existence of such records with matching name and reference numbers.
 - ii) corroborates date of birth, current address of record and other personal information sufficient to ensure a unique identity.
- 3) If it is two utility bills or equivalent documents,
 - a) each appears to be a genuine document properly issued by the claimed issuing authority.
 - b) corroborates current address of record or telephone number sufficient to ensure a unique identity.

AL4_ID_IPV#050 Applicant knowledge checks

Where the Applicant is unable to satisfy any of the above requirements, that the applicant can provide a Social Security Number (SSN) that matches the claimed identity.

3.6.4.2.2 *Affiliation Verification*

A specific service that offers identity proofing to applicants on the basis of some form of affiliation must comply with the criteria in this section to establish that affiliation, in addition to complying with the previously stated requirements for verifying the individual's identity.

The enterprise or specified service must:

AL4_ID_AFV#010 Required evidence

Ensure that the Applicant possesses:

- a) identification from the organization with which the Applicant is claiming Affiliation.
- b) agreement from the organization that the Applicant may be issued a credential indicating that an affiliation exists.

AL4_ID_AFV#020 Evidence checks

Ensure that the presented documents:

- a) each appear to be a genuine document properly issued by the claimed issuing authorities and valid at the time of application.
- b) refer to an existing organization, with a contact address.
- c) indicate that the Applicant has some form of recognizable affiliation with the organization.
- d) appear to grant the Applicant an entitlement to obtain a credential indicating an affiliation with the organization.

3.6.4.2.3 *Secondary Verification*

In each of the above cases, the enterprise or specified service must also meet the following criteria:

AL4_ID_SCV#010 Secondary checks

Have in place additional measures (e.g., require additional documentary evidence, delay completion while out-of-band checks are undertaken) to deal with any anomalous circumstances that can reasonably be anticipated (e.g., a legitimate and recent change of address that has yet to be established as the address of record).

3.6.4.3 *Verification Records*

The specific service must retain records of the identity proofing (verification) that it undertakes.

The enterprise or specified service must:

AL4_ID_VRC#010 Verification Records

Log, taking account of all applicable legislative and policy obligations, a record of the facts of the verification process. At a minimum, records of identity information must include:

- a) the Applicant's full legal name.
- b) the Applicant's date and place of birth (as declared, but not necessarily verified).
- c) the Applicant's current address of record.
- d) the type, issuing authority and reference number(s) of all documents checked in the identity-proofing process.

- e) a telephone or email address for related contact and/or delivery of credentials/notifications.
- f) any pseudonym used by the Applicant in lieu of the verified identity.
- g) a biometric record of the Applicant (e.g., a photograph, fingerprint, voice recording).
- h) date and time of verification, issued by a trusted time-source.
- i) the signature of the Applicant.
- j) identity of the registrar.
- k) identity of the CSP providing the verification service or the location at which the (in-house) verification was performed.

AL4_ID_VRC#020 Verification Records for Affiliated Applicants

In addition to the foregoing, log, taking account of all applicable legislative and policy obligations, a record of the additional facts of the verification process. At a minimum, records of identity information must include:

- a) the Subscriber's full legal name.
- b) the Subscriber's current address of record.
- c) the Subscriber's current telephone or email address of record.
- d) the Subscriber's authorization for issuing the Subject a credential.
- e) type, issuing authority and reference number(s) of all documents checked in the identity-proofing process.
- f) a biometric record of each required representative of the affiliating organization (e.g., a photograph, fingerprint, voice recording), as determined by that organization's governance rules/charter.

AL4_ID_VRC#040 Record Retention

Either retain securely the record of the verification/revocation process for the duration of the Subscriber account plus 10.5 years, or submit the record to a client CSP that has undertaken to retain the record for the requisite period or longer.

3.6.5 COMPLIANCE TABLES

Use the following tables to correlate criteria for a particular AL and the evidence offered to support compliance.

CSPs preparing for an assessment can use the table appropriate to the level at which they are seeking approval to correlate evidence with criteria or to justify nonapplicability (e.g., "specific service types not offered").

Assessors can use the tables to record assessment steps and their determination of compliance or failure. (

(THESE TABLES, AND OTHER BLANK TABLES IN PART 3, WILL BE COMPLETED PRIOR TO PUBLIC EXPOSURE OF THE FRAMEWORK IN JANUARY 2005.)

Table 3-1. ID-SAC - AL1 Compliance

Clause	Description	Compliance
AL1_ID_POL#010	Unique service identity	
AL1_ID_POL#020	Unique subject identity	
AL1_ID_IPV#010	Required evidence	
AL1_ID_IPV#020	Evidence checks	
AL1_ID_RPV#010	Required evidence	
AL1_ID_RPV#020	Evidence checks	
AL1_ID_SCV#010	Secondary checks	

Table 3-2. ID-SAC - AL2 Compliance

Clause	Description	Compliance

Table 3-3. ID-SAC - AL31 compliance

Clause	Description	Compliance

Table 3-4. ID-SAC - AL4 compliance

Clause	Description	Compliance

3.7 Credential Management Service Assessment Criteria

The Service Assessment Criteria in this section establish requirements for the functional conformity of credential management services and their providers at all ALs defined in Section 2. These criteria are generally referred to elsewhere within EAP documentation as CM-SAC.

The criteria are divided into five parts. Each part deals with a specific functional aspect of the overall credential management process.

This SAC must be used in conjunction with the Common Organizational SAC (CO-SAC), described in Section 3.5, and in addition must either:

- Explicitly include the criteria of the Identity Proofing SAC (ID-SAC) described in Section 3.6, or
- Rely upon the criteria of the ID-SAC being fulfilled by the use of an EAP-approved ID-proofing service.

3.7.1 PART A--CREDENTIAL OPERATING ENVIRONMENT

The criteria in this part deal with the overall operational environment in which the credential life-cycle management is conducted. The credential management service assessment criteria must be used in conjunction with

the common organizational criteria described in Section 3.5. In addition, they must either explicitly include the identify-proofing service assessment criteria described in Section 3.6 or rely upon those criteria being fulfilled by the use of an EAP-approved identity-proofing service.

These criteria describe requirements for the overall operational environment in which credential life-cycle management is conducted. The common organizational criteria describe broad requirements. The criteria in this section describe implementation specifics. Implementation depends on the AL. The procedures and processes required to create a secure environment for management of credentials and the particular technologies that are considered strong enough to meet the assurance requirements differ considerably from level to level.

3.7.1.1 Assurance Level 1 (Minimal)

These criteria apply to PINs and passwords.

3.7.1.1.1 *Credential Policy and Practices*

These criteria apply to the policy and practices under which credentials are managed.

An enterprise and its specified service must:

AL1_CM_CPP#010 Credential Policy and Practice Statement

No stipulation.

3.7.1.1.2 *Security Controls*

An enterprise and its specified service must:

AL1_CM_CTR#010 Secret revelation

No stipulation.

AL1_CM_CTR#020 Protocol threat risk assessment and controls

Account for the following protocol threats and apply appropriate controls:

- a) password guessing.
- b) message replay.

AL1_CM_CTR#030 System threat risk assessment and controls

Account for the following system threats and apply appropriate controls:

- a) the introduction of malicious code.
- b) compromised authentication arising from insider action.
- c) out-of-band attacks by other users and system operators (e.g., shoulder-surfing).
- d) spoofing of system elements/applications.
- e) malfeasance on the part of subscribers and subjects.

3.7.1.1.3 *Storage of Long-term Secrets*

An enterprise and its specified service must:

AL1_CM_STS#010 Stored Secrets

Not store secrets (such as passwords) as plain text and apply discretionary access controls that limit access to administrators and those applications that require access.

3.7.1.1.4 Security-relevant Event (Audit) Records

No stipulation.

3.7.1.1.5 Subject Options

An enterprise and its specified service must:

AL1_CM_OPN#010 Changeable PIN/Password

Permit subjects to change their PINs/passwords.

3.7.1.2 Assurance Level 2 (Moderate)

These criteria apply to passwords.

3.7.1.2.1 Credential Policy & Practices

These criteria apply to the policy and practices under which credentials are managed.

An enterprise and its specified service must:

AL2_CM_CPP#010 Credential Policy and Practice Statement

Include in its Service Definition a description of the Policy against which it issues credentials and the corresponding Practices it applies in their management. At a minimum the Policy and Practice Statement must specify:

- a) if applicable, any OIDs related to the Practice & Policy Statement;
- b) how users may subscribe to the service/apply for credentials and how users' credentials will be delivered to them.
- c) how subscribers acknowledge receipt of tokens and credentials and what obligations they accept in so doing (including whether they consent to publication of their details in credential status directories).
- d) how credentials may be renewed, modified, revoked and suspended, including how requestors are authenticated or their identity re-proven.
- e) what actions a subscriber must take to terminate a subscription.

AL2_CM_CPP#020 Management Authority

Have a nominated management body with authority and responsibility for approving the Credential Policy & Practice Statement and for its implementation.

3.7.1.2.2 Security Controls

An enterprise and its specified service must:

AL2_CM_CTR#010 Secret revelation

Use communication and authentication protocols that minimize the duration of any clear-text disclosure of long-term secrets, even when disclosed to trusted parties.

AL2_CM_CTR#020 Protocol threat risk assessment and controls

Account for the following protocol threats in its risk assessment and apply controls that reduce them to acceptable risk levels:

- a) password guessing.
- b) message replay.
- c) eavesdropping.

AL2_CM_CTR#030 System threat risk assessment and controls

Account for the following system threats in its risk assessment and apply controls that reduce them to acceptable risk levels:

- a) the introduction of malicious code.
- b) compromised authentication arising from insider action.
- c) out-of-band attacks by both users and system operators (e.g., the ubiquitous shoulder-surfing).
- d) spoofing of system elements/applications.
- e) malfeasance on the part of subscribers and subjects.
- f) intrusions leading to information theft.

AL2_CM_CTR#040 Specified Service's Key Management

Specify and observe procedures and processes for the generation, storage and destruction of its own cryptographic keys used for securing the Specific Service's assertions and other publicized information. At a minimum these should address:

- a) the physical security of the environment.
- b) access control procedures limiting access to the minimum number of authorized personnel.
- c) public-key publication mechanisms.
- d) application of controls deemed necessary as a result of the service's risk assessment.
- e) destruction of expired or compromised private keys in a manner that prohibits their retrieval, or their archival in a manner that prohibits their reuse.

3.7.1.2.3 Storage of Long-term Secrets

An enterprise and its specified service must:

AL2_CM_STS#010 Stored Secrets

Not store secrets (such as passwords) as plain text and apply discretionary access controls that limit access to administrators and to those applications requiring access.

3.7.1.2.4 Security-Relevant Event (Audit) Records

These criteria describe the need to provide an auditable log of all events that are pertinent to the correct and secure operation of the service. The common organizational criteria applying to provision of an auditable log of all events pertinent to the correct and secure operation of the service must also be considered carefully. These criteria carry implications for credential management operations.

3.7.1.2.5 Subject Options

An enterprise and its specified service must:

AL2_CM_OPN#010 Changeable PIN/Password

Permit Subjects to change their passwords.

3.7.1.3 Assurance Level 3 (Substantial)

These criteria apply to one-time password devices and soft crypto applications protected by passwords or biometric controls.

3.7.1.3.1 Credential Policy & Practices

These criteria apply to the policy and practices under which credentials are managed.

An enterprise and its specified service must:

AL3_CM_CPP#010 Credential Policy & Practice Statement

Include in its Service Definition a full description of the Policy against which it issues credentials and the corresponding Practices it applies in their issuance. At a minimum the Practice and Policy Statement must specify:

- a) if applicable, any OIDs related to the Practice & Policy Statement.
- b) how users may subscribe to the service/apply for credentials and how the users' credentials will be delivered to them.
- c) how subscribers acknowledge receipt of tokens and credentials and what obligations they accept in so doing (including whether they consent to publication of their details in credential status directories).
- d) how credentials may be renewed, modified, revoked and suspended, including how requestors are authenticated or their identity -proven.
- e) what actions a subscriber must take to terminate a subscription.

AL3_CM_CPP#020 Management Authority

Have a nominated management body with authority and responsibility for approving the Credential Policy & Practice Statement, and for its implementation.

3.7.1.3.2 Security Controls

AL3_CM_CTR#010 Secret revelation

Use communication and authentication protocols that minimize the duration of any clear-text disclosure of long-term secrets, even when disclosed to ostensibly trusted parties.

AL3_CM_CTR#020 Protocol threat risk assessment and controls

Account for the following protocol threats in its risk assessment and apply controls that reduce them to acceptable risk levels:

- a) password guessing.
- b) message replay.
- c) eavesdropping.
- d) relying party (verifier) impersonation.
- e) man-in-the-middle attack.

AL3_CM_CTR#030 System threat risk assessment and controls

Account for the following system threats in its risk assessment and apply controls that reduce them to acceptable risk levels:

- a) the introduction of malicious code.
- b) compromised authentication arising from insider action.
- c) out-of-band attacks by both users and system operators (e.g., the ubiquitous shoulder-surfing).
- d) spoofing of system elements/applications.
- e) malfeasance on the part of subscribers and subjects.
- f) intrusions leading to information theft.

AL3_CM_CTR#040 Specified Service's Key Management

Specify and observe procedures and processes for the generation, storage and destruction of its own cryptographic keys used for securing the Specific Service's assertions and other publicized information. At a minimum, these should address:

- a) the physical security of the environment.
- b) access control procedures limiting access to the minimum number of authorized personnel.
- c) public-key publication mechanisms.
- d) application of controls deemed necessary as a result of the service's risk assessment.
- e) destruction of expired or compromised private keys in a manner that prohibits their retrieval **or** their archival in a manner that prohibits their reuse.

3.7.1.3.3 Storage of Long-term Secrets

An enterprise and its specified service must:

AL3_CM_STS#010 Stored Secrets

Not store secrets (such as passwords) as plain text and apply discretionary access controls that limit access to administrators and to those applications that require access.

AL3_CM_STS#020 Stored Secret Encryption

Encrypt such shared secret files so that:

- a) the encryption key for the shared secret file is encrypted under a key held in a FIPS 140-2 Level 2 or higher validated hardware cryptographic module or any FIPS 140-2 Level 3 or 4 cryptographic module.
- b) the shared secret file is decrypted only as immediately required for an authentication operation.
- c) shared secrets are protected as a key within the boundary of a FIPS 140-2 Level 2 or higher validated hardware cryptographic module or any FIPS 140-2 Level 3 or 4 cryptographic module and are not exported from the module in plain text.
- d) shared secrets are split by an n from m cryptographic secret sharing method.

3.7.1.3.4 Security-relevant Event (Audit) Records

These criteria describe the need to provide an auditable log of all events that are pertinent to the correct and secure operation of the service. The common organizational criteria applying to the recording of all security-related events must also be considered carefully. These criteria carry implications for credential management operations.

In the specific context of a certificate management service, an enterprise and its specified service must:

AL3_CM_SER#010 Security event logging

Ensure that such audit records include:

- a) the identity of the point of Registration (irrespective of whether internal or outsourced).
- b) generation of the subscriber's keys or the evidence that the subscriber was in possession of both parts of their own key-pair.
- c) generation of the subscriber's certificate.
- d) dissemination of the subscriber's certificate.
- e) any revocation or suspension associated with the subscriber's certificate.

3.7.1.3.5 Subject options

An enterprise and its specified service must:

AL3_CM_OPN#010 Changeable PIN/Password

Permit Subjects to change the password used to activate their credentials.

3.7.1.4 Assurance Level 4 (High)

These criteria apply exclusively to cryptographic technology deployed through a Public Key Infrastructure. This technology requires hardware tokens protected by password or biometric controls. No other forms of credential are permitted at AL4.

3.7.1.4.1 Certification Policy and Practices

These criteria apply to the policy and practices under which certificates are managed.

An enterprise and its specified service must:

AL4_CM_CPP#010 Certificate Policy/Certification Practice Statement

Include in its Service Definition its full Certificate Policy and the corresponding Certification Practice Statement. The Certificate Policy and Certification Practice Statement must conform to IETF RFC 3647 (2003-11) in their content and scope or be demonstrably consistent with the content or scope of that RFC. At a minimum, the Certificate Policy must specify:

- a) applicable OIDs for each certificate type issued.
- b) how users may subscribe to the service/apply for certificates, and how certificates will be issued to them.
- c) if users present their own keys, how they will be required to demonstrate possession of the private key:.
- d) if users' keys are generated for them, how the private keys will be delivered to them.
- e) how subscribers acknowledge receipt of tokens and credentials and what obligations they accept in so doing (including whether they consent to publication of their details in certificate status directories).

- f) how certificates may be renewed, re-keyed, modified, revoked and suspended, including how requestors are authenticated or their identity proven.
- g) what actions a subscriber must take to terminate their subscription.

AL4_CM_CPP#020 Management Authority

Have a nominated high-level management body with authority and responsibility for approving the Certificate Policy and Certification Practice Statement, including ultimate responsibility for its proper implementation.

3.7.1.4.2 Security Controls

An enterprise and its specified service must:

AL4_CM_CTR#010 Secret revelation

Use communication and authentication protocols that minimize the duration of any clear-text disclosure of long-term secrets, even when disclosed to ostensibly trusted parties, which must themselves be authenticated prior to being granted access to any sensitive information.

AL4_CM_CTR#020 Protocol threat risk assessment and controls

Account for the following protocol threats in its risk assessment and apply controls that reduce them to acceptable risk levels:

- a) password guessing.
- b) message replay.
- c) eavesdropping.
- d) relying party (verifier) impersonation.
- e) man-in-the-middle attack.
- f) session hijacking.

AL4_CM_CTR#030 System threat risk assessment and controls

Account for the following system threats in its risk assessment and apply controls that reduce them to acceptable risk levels:

- a) the introduction of malicious code.
- b) compromised authentication arising from insider action.
- c) out-of-band attacks by both users and system operators (e.g., the ubiquitous shoulder-surfing).
- d) spoofing of system elements/applications.
- e) malfeasance on the part of subscribers and subjects.
- f) intrusions leading to information theft.

AL4_CM_CTR#040 Specified Service's Key Management

Specify and observe procedures and processes for the generation, storage and destruction of its own cryptographic keys used for securing the Specific Service's assertions and other publicized information. At a minimum, these should address:

- a) the physical security of the environment.
- b) access control procedures limiting access to the minimum number of authorized personnel.
- c) public-key publication mechanisms.
- d) application of controls deemed necessary as a result of the service's risk assessment.

- e) destruction of expired or compromised private keys in a manner that prohibits their retrieval, or their archival in a manner which prohibits their reuse;

3.7.1.4.3 Storage of Long-term Secrets

The enterprise and its specified service must meet the following criteria:

AL4_CM_STS#010 Stored Secrets

Not store secrets (such as passwords) as plain text and must apply discretionary access controls that limit access to administrators and to those applications that require access.

AL4_CM_STS#020 Stored Secret Encryption

Encrypt such shared secret files so that:

- a) the encryption key for the shared secret file is encrypted under a key held in a FIPS 140-2 Level 2 or higher validated hardware cryptographic module or any FIPS 140-2 Level 3 or 4 cryptographic module.
- b) the shared secret file is decrypted only as immediately required for an authentication operation.
- c) shared secrets are protected as a key within the boundary of a FIPS 140-2 Level 2 or higher validated hardware cryptographic module or any FIPS 140-2 Level 3 or 4 cryptographic module and are not exported from the module in plaintext.
- d) shared secrets are split by an *n* from *m* cryptographic secret sharing method.

3.7.1.4.4 Security-relevant Event (Audit) Records

These criteria describe the need to provide an auditable log of all events that are pertinent to the correct and secure operation of the service. The common organizational criteria relating to the recording of all security-related events must also be considered carefully. These criteria carry implications for credential management operations.

An enterprise and its specified service must:

AL4_CM_SER#010 Security event logging

Ensure that such audit records include:

- a) the identity of the point of Registration (whether internal or outsourced).
- b) generation of the subscriber's keys or evidence that the subscriber was in possession of both parts of the key-pair.
- c) generation of the subscriber's certificate.
- d) dissemination of the subscriber's certificate.
- e) any revocation or suspension associated with the subscriber's certificate.

3.7.1.4.5 Subject Options

An enterprise and its specified service must:

AL4_CM_OPN#010 Changeable PIN/Password

Permit Subjects to change the passwords used to activate their credentials.

3.7.2 PART B--CREDENTIAL ISSUING

These criteria apply to the verification of the identity of the subject of a credential and with token strength and credential delivery mechanisms. They address requirements levied by the use of various technologies to achieve the appropriate AL.⁵ These criteria include by reference all applicable criteria in Section 3.6.

3.7.2.1 Assurance Level 1 (Minimal)

3.7.2.1.1 *Identity Proofing*

These criteria determine how the enterprise shows compliance with the criteria for fulfilling identity proofing functions.

The enterprise and its specified service must:

AL1_CM_IDP#010 Self-managed Identity Proofing

If the enterprise assumes direct responsibility for identity-proofing functions, show, by direct inclusion, compliance with all applicable identity-proofing service assessment criteria^{6,7} for AL1 or higher.

AL1_CM_IDP#020 EAP-approved outsourced service

If the enterprise outsources responsibility for identity-proofing functions and uses a service already operating under an EAP Identity-proofing Approval, show that the service in question has been approved at AL1 or higher.

AL1_CM_IDP#030 Non EAP-approved outsourced service

If the enterprise outsources responsibility for identity-proofing functions, ensure that each provider of such a service demonstrates compliance with all applicable identity-proofing service assessment criteria⁴ for AL1 or higher, and that the enterprise itself has in place controls to ensure the continued fulfillment of those criteria by the provider to which the functions have been outsourced.

AL1_CM_IDP#040 Revision to subscriber information

Provide a means for subscribers to amend their stored information after registration.

3.7.2.1.2 *Credential Creation*

These criteria address the requirements for creation of credentials that can only be used at AL1. Any

⁵ Largely driven by the guidance in NIST SP 800-63.

⁶ Formal reference of this document is *EAP CSAC 04011, "ID-SAC"*

⁷ Not all criteria may be applicable – the precise scope (definition) of the identity proofing performed by a particular service may exclude certain functionality and therefore certain criteria.

credentials/tokens that comply with the criteria stipulated for AL2 and higher are acceptable at AL1.

An enterprise and its specified service must:

AL1_CM_CRN_#010 Authenticated Request

Only accept a request to generate a credential and bind it to an identity if the source of the request can be authenticated as being authorized to perform Identity proofing at AL1 or higher.

AL1_CM_CRN_#020 Unique identity

Ensure that the identity (e.g., UserID) to which a credential is to be bound is unique within the Specified Service's intended community.

AL1_CM_CRN_#030 Token uniqueness

Allow the subscriber to select a unique token (e.g., UserID combined with PIN/password) that must be validated to be unique within the Specified Service's intended community and assigned uniquely to a single identity.

3.7.2.2 Assurance Level 2 (Moderate)

3.7.2.2.1 *Identity Proofing*

These criteria determine how the enterprise shows compliance with the criteria for fulfilling identity-proofing functions.

The enterprise and its specified service must:

AL2_CM_IDP#010 Self-managed Identity Proofing

If the enterprise assumes direct responsibility for identity-proofing functions, show, by direct inclusion, compliance with all applicable identity-proofing service assessment criteria for AL2 or higher.

AL2_CM_IDP#020 EAP-approved outsourced service

If the enterprise outsources responsibility for identity-proofing functions and uses a service already operating under an EAP Identity-proofing Approval, show that the service in question has been approved at AL2 or higher and that its approval has at least 6 months of remaining validity.

AL2_CM_IDP#030 Non EAP-approved outsourced service

If the enterprise outsources responsibility for identity-proofing functions, ensure that each provider of such a service demonstrates compliance with all applicable identity-proofing service assessment criteria^{3,4} for AL2 or higher, and that the enterprise itself has in place controls to ensure the continued fulfillment of those criteria by the provider to which the functions have been outsourced.

AL2_CM_IDP#040 Revision to subscriber information

Provide a means for subscribers to securely amend their stored information after registration, either by re-proving their identity as in the

initial registration process or by using their credentials to authenticate their revision.

3.7.2.2.2 *Credential Creation*

These criteria define the requirements for creation of credentials whose highest use is at AL2. Credentials/tokens that comply with the criteria stipulated at AL3 and higher are also acceptable at AL2 and below.

Note, however, that a token and credential created according to these criteria may not necessarily provide that level of assurance for the claimed identity of the subscriber. Authentication can only be provided at the assurance level at which the identity is proven.

An enterprise and its specified service must:

AL2_CM_CRN_#010 Authenticated Request

Only accept a request to generate a credential and bind it to an identity if the source of the request can be authenticated as being authorized to perform Identity proofing at AL2 or higher.

AL2_CM_CRN_#020 Unique identity

Ensure that the identity (e.g., UserID) to which a credential is to be bound is unique within the Specified Service's intended community.

AL2_CM_CRN_#030 Token uniqueness

Allow the subscriber to select a unique token (e.g., UserID combined with PIN/password) that must be validated to be unique within the Specified Service's intended community and assigned uniquely to a single identity.

AL2_CM_CRN_#040 Password strength

Only allow passwords that, over the life of the password, have resistance to an on-line guessing attack against a selected user/password of at least 1 in 2^{14} (16,384), accounting for state-of-the-art attack strategies.

AL2_CM_CRN_#050 One-time password strength

Only allow password tokens that, over the life of the password, have a resistance to guessing of 1 in 2^{14} (16,384), accounting for state-of-the-art attack strategies.

AL2_CM_CRN_#060 Software cryptographic token strength

Refer to Section 3.7.2.3.

AL2_CM_CRN_#070 Hardware token strength

Refer to Section 3.7.2.3.

AL2_CM_CRN_#080 Binding of key

No stipulation.

AL2_CM_CRN #090 Nature of subject

Record the nature of the subject of the credential (which must correspond to the manner of identity proofing performed), i.e., private person, a named person acting on behalf of a corporation or other legal entity, corporation or legal entity, or corporate machine entity, in a manner that can be unequivocally associated with the credential and the identity that it asserts.

3.7.2.2.3 Credential Delivery

The enterprise and its specified service must:

AL2_CM_CRD #010 Confirm subject's details

Confirm the subject's contact details and notify the subject of the credential's issuance by:

- a) sending notice to the address of record confirmed during Identity proofing or
- b) issuing the credential(s) in a manner that confirms the address of record supplied by the applicant during Identity proofing or
- c) issuing the credential(s) in a manner that confirms the ability of the applicant to receive telephone communications at a telephone number or email at an email address supplied by the applicant during Identity proofing.

3.7.2.3 Assurance Level 3 (Substantial)

3.7.2.3.1 Identity Proofing

These criteria in this section determine how the enterprise shows compliance with the criteria for fulfilling identity-proofing functions.

The enterprise and its specified service must:

AL3_CM_IDP#010 Self-managed Identity Proofing

If the enterprise assumes direct responsibility for identity proofing functions, show, by direct inclusion, compliance with all applicable identity-proofing service assessment criteria for AL3 or AL4.

AL3_CM_IDP#020 EAP-approved outsourced service

If the enterprise outsources responsibility for identity-proofing functions and uses a service already operating under an EAP Identity-proofing Approval, show that the service in question has been approved at AL3 or AL4 and that its approval has at least 6 months of remaining validity.

AL3_CM_IDP#030 Non EAP-approved outsourced service

Not use any non-EAP-approved outsourced services for identity proofing.

AL3_CM_IDP#040 Revision to subscriber information

Provide a means for subscribers to securely amend their stored information after registration, either by re-proving their identity as in the initial registration process or by using their credentials to authenticate their revision. Successful revision must, where necessary, instigate the re-issuance of the credential.

3.7.2.3.2 *Credential Creation*

These criteria define the requirements for creation of credentials whose highest use is AL3. Any credentials/tokens that comply with the criteria stipulated at AL4 are also acceptable at AL3 and below.

Note, however, that a token and credential created according to these criteria may not necessarily provide that level of assurance for the claimed identity of the subscriber. Authentication can only be provided at the assurance level at which the identity is proven.

An enterprise and its specified service must:

AL3_CM_CRN_#010 Authenticated Request

Only accept a request to generate a credential and bind it to an identity if the source of the request can be authenticated as being authorized to perform Identity proofing at AL3 or higher.

AL3_CM_CRN_#020 Unique identity

Ensure that the identity (e.g., UserID) to which a credential is to be bound is unique within the Specified Service's intended community, accounting fully for identities previously used and that are now cancelled.

AL3_CM_CRN_#030 Token uniqueness

Allow the subscriber to select a unique token (e.g., UserID combined with PIN/password) that must be validated to be unique within the Specified Service's intended community and assigned uniquely to a single identity.

AL3_CM_CRN_#040 PIN/Password strength

Not use PIN/password tokens.

AL3_CM_CRN_#050 One-time password strength

Only allow one-time password tokens that:

- a) depend on a symmetric key stored on a personal hardware device evaluated against FIPS 140-2 Level 1 or higher.
- b) permit at least 10^6 possible password values.
- c) require password or biometric activation by the subscriber.

AL3_CM_CRN_#060 Software cryptographic token strength

Ensure that software cryptographic keys stored on general-purpose devices:

- a) are protected by a key and cryptographic protocol that are evaluated against FIPS 140-2 Level 2.
- b) require password or biometric activation by the subscriber or employ a password protocol when being used for authentication.

AL3_CM_CRN_#070 Hardware token strength

Ensure that hardware tokens used to store cryptographic keys:

- a) employ a cryptographic module that is evaluated against FIPS 140-2 Level 1 or higher.

- b) require password or biometric activation by the subscriber or also employ a password when being used for authentication.

AL3_CM_CRN_#080 Binding of key

If the Specified Service generates the subject's key pair, that the key generation process securely and uniquely binds that process to the certificate generation and maintains at all times the secrecy of the private key, until it is accepted by the subject.

AL3_CM_CRN_#090 Nature of subject

Record the nature of the subject of the credential (which must correspond to the manner of identity proofing performed), i.e., private person, a named person acting on behalf of a corporation or other legal entity, corporation or legal entity, or corporate machine entity, in a manner that can be unequivocally associated with the credential and the identity that it asserts.

3.7.2.3.3 Subject Key Pair Generation

An enterprise and its specified service must:

AL3_CM_SKP_#010 Key generation by Specified Service

If the Specified Service generates the Subject's keys:

- a) use a FIPS-approved algorithm that is recognized as being fit for the purposes of the service.
- b) only create keys of a key length and for use with a FIPS-approved public key algorithm recognized as being fit for the purposes of the service.
- c) generate and store the keys securely until delivery to and acceptance by the Subject.
- d) deliver the Subject's private key in a manner that ensures that the privacy of the key is not compromised and only the Subject has access to the private key.

AL3_CM_SKP_#020 Key generation by Subject

If the Subject generates and presents its own keys, obtain the Subject's written confirmation that it has:

- a) used a FIPS-approved algorithm that is recognized as being fit for the purposes of the service.
- b) created keys of a key length and for use with a FIPS-approved public key algorithm recognized as being fit for the purposes of the service.

3.7.2.3.4 Credential Delivery

An enterprise and its specified service must:

AL3_CM_CRD_#010 Confirm subject's details

Confirm the subject's contact details and notify the subject of the credential's issuance by:

- a) sending notice to the address of record confirmed during Identity proofing, and either
 - i) issuing the credential(s) in a manner that confirms the address of record supplied by the applicant during Identity proofing; or

- ii) issuing the credential(s) in a manner that confirms the ability of the applicant to receive telephone communications at a phone number supplied by the applicant during Identity proofing while recording the applicant's voice.

AL3_CM_CRD_#020 Subject's acknowledgement

Receive acknowledgement of receipt of the credential before it is activated and its directory status record is published (and thereby the subscription becomes active or re-activated, depending upon the circumstances of issue).

3.7.2.4 Assurance Level 4 (High)

3.7.2.4.1 *Identity Proofing*

These criteria determine how the enterprise shows compliance with the criteria for fulfilling identity-proofing functions.

An enterprise and its specified service must:

AL4_CM_IDP#010 Self-managed Identity Proofing

If the enterprise assumes direct responsibility for identity-proofing functions, show, by direct inclusion, compliance with all applicable identity-proofing service assessment criteria for AL4.

AL4_CM_IDP#020 EAP-approved outsourced service

If the enterprise outsources responsibility for identity-proofing functions and uses a service already operating under an EAP Identity-proofing Approval, show that the service in question has been approved at AL4 and that its approval has at least 12 months of remaining validity.

AL4_CM_IDP#030 Non EAP-approved outsourced service

Not use any non-EAP-approved outsourced services for identity proofing unless they can be demonstrated to have satisfied equivalently rigorous requirements established by another scheme recognized by EAP.

AL4_CM_IDP#040 Revision to subscriber information

Provide a means for subscribers to securely amend their stored information after registration, either by re-proving their identity as in the initial registration process or by using their credentials to authenticate their revision. Successful revision must, where necessary, instigate the re-issuance of the credential.

3.7.2.4.2 *Credential Creation*

These criteria define the requirements for creation of credentials whose highest use is AL4.

Note, however, that a token and credential created according to these criteria may not necessarily provide that level of assurance for the claimed identity of the subscriber. Authentication can only be provided at the assurance level at which the identity is proven.

An enterprise and its specified service must:

AL4_CM_CRN_#010 Authenticated Request

Only accept a request to generate a credential and bind it to an identity if the source of the request can be authenticated as being authorized to perform Identity proofing at AL4.

AL4_CM_CRN_#020 Unique identity

Ensure that the identity (e.g., UserID) to which a credential is to be bound is unique within the Specified Service's intended community.

AL4_CM_CRN_#030 Token uniqueness

Allow the subscriber to select a unique token (e.g., UserID combined with PIN/password) that must be validated to be unique within the Specified Service's intended community and assigned uniquely to a single identity.

AL4_CM_CRN_#040 PIN/Password strength

Not use PIN/password tokens.

AL4_CM_CRN_#050 One-time password strength

Not use one-time password tokens.

AL4_CM_CRN_#060 Software cryptographic token strength

Not use software cryptographic tokens.

AL4_CM_CRN_#070 Hardware token strength

Ensure that hardware tokens used to store cryptographic keys:

- a) employ a cryptographic module that is evaluated against FIPS 140-2 Level 2 or higher.
- b) are evaluated against FIPS 140-2 Level 3 or higher for their physical security.
- c) require password or biometric activation by the subscriber.

AL4_CM_CRN_#080 Binding of key

If the Specified Service generates the subject's key pair, that the key generation process securely and uniquely binds that process to the certificate generation and maintains at all times the secrecy of the private key, until it is accepted by the subject.

AL3_CM_CRN_#090 Nature of subject

Record the nature of the subject of the credential, i.e., private person, a named person acting on behalf of a corporation or other legal entity, corporation or legal entity, or corporate machine entity, in a manner that can be unequivocally associated with the credential and the identity that it asserts.

3.7.2.4.3 Subject Key Pair Generation

An enterprise and its specified service must:

AL4_CM_SKP_#010 Key generation by Specified Service

If the Specified Service generates the Subject's keys:

- a) use a FIPS-approved algorithm that is recognized as being fit for the purposes of the service.
- b) only create keys of a key length and for use with a FIPS-approved public key algorithm recognized as being fit for the purposes of the service.
- c) generate and store the keys securely until delivery to and acceptance by the Subject;
- d) deliver the Subject's private key in a manner that ensures that the privacy of the key is not compromised and only the Subject has access to the private key.

AL4_CM_SKP_#020 Key generation by Subject

If the Subject generates and presents its own keys, obtain the Subject's written confirmation that it has:

- a) used a FIPS-approved algorithm that is recognized as being fit for the purposes of the service.
- b) created keys of a key length and for use with a FIPS-approved public key algorithm recognized as being fit for the purposes of the service.

3.7.2.4.4 Credential Delivery

An enterprise and its specified service must:

AL4_CM_CRD_#010 Confirm subject's details

Confirm the subject's contact details and notify the subject of the credential's issuance by:

- a) sending notice to the address of record confirmed during Identity proofing.
- b) unless the subject presented with a private key, issuing the hardware token to the subject in a manner that confirms the address of record supplied by the applicant during Identity proofing.
- c) issuing the certificate to the subject over a separate channel in a manner that confirms either the address of record or the email address supplied by the applicant during Identity proofing.

AL4_CM_CRD_#020 Subject's acknowledgement

Receive acknowledgement of receipt of the hardware token before it is activated and the corresponding certificate and its directory status record are published (and thereby the subscription becomes active or re-activated, depending upon the circumstances of issue).

3.7.3 PART C--CREDENTIAL REVOCATION

These criteria deal with credential revocation and the determination of the legitimacy of a revocation request.

3.7.3.1 Assurance Level 1 (Minimal)

An enterprise and its specified service must:

3.7.3.1.1 Not used

3.7.3.1.2 Not used

3.7.3.1.3 Secure Revocation Request

This criterion applies when revocation requests between remote components of a service are made over a secured communication.

An enterprise and its specified service must:

AL1_ID_SRR#010 Submit Request

Submit a request for revocation to the Credential Issuer service (function), using a secured network communication if necessary.

3.7.3.2 Assurance Level 2 (Moderate)

3.7.3.2.1 Revocation Procedures

These criteria address general revocation functions, such as the processes involved and the basic requirements for publication.

An enterprise and its specified service must:

AL2_CM_RVP#010 Revocation procedures

State the conditions under which revocation of an issued credential may occur, the processes by which a revocation request may be submitted, the persons and organizations from which a revocation request will be accepted, the validation steps that will be applied to ensure the validity (identity) of the revocant, and the response time between a revocation request being accepted and the publication of revised certificate status.

AL2_CM_RVP#020 Secure status notification

Ensure that published credential status notification information can be relied upon in terms of the enterprise being its origin (i.e., its authenticity) and its correctness (i.e., its integrity).

AL2_CM_RVP#030 Revocation publication

Ensure that published credential status notification is revised within 72 hours of the receipt of a valid revocation request, such that any subsequent attempts to use that credential in an authentication shall be unsuccessful.

AL2_ID_RVP#040 Verify revocation identity

Establish that the identity for which a revocation request is received is one that was issued by the Specified Service.

AL2_ID_RVP#050 Revocation Records

Retain a record of any revocation of a credential that is related to a specific identity previously verified, solely in connection to the stated credential. At a minimum, records of revocation must include:

- a) the Revocant's full legal name.
- b) the Revocant's current address.

- c) type, issuing authority and reference number(s) of all documents checked in the identity-proofing process for the Revocant.
- d) the Revocant's authority to revoke (e.g., subscriber themselves, someone acting with the subscriber's power of attorney, the credential issuer, law enforcement or other legal due process).
- e) the Subscriber's full legal name and, where applicable, unique service reference (e.g., certificate serial number, IP address).
- f) the Subscriber's date of birth.
- g) the Subscriber's current address of record.
- h) the Credential Issuer's identity (if not directly responsible for the Identity Proofing service).
- i) the identity associated with the credential (whether the Subscriber's name or a pseudonym).
- j) the reason for revocation.

AL2_ID_PNR#060 Record Retention

Retain securely the record of the revocation process for the duration of the Subscriber's account plus 7.5 years.

3.7.3.2.2 Verify Revocant's Identity

The enterprise should not act on a request for revocation without first establishing the validity of the request (if it does not itself determine the need for revocation).

In order to do so, the enterprise and its specified service must:

AL3_ID_RVR#010 Verify revocation identity

Establish that the credential for which a revocation request is received was one that was issued by the Specified Service.

AL2_ID_RVR#020 Revocation reason

Establish the reason for the revocation request as being sound and well-founded, in combination with verification of the Revocant, according to AL2_ID_RVR#030, AL2_ID_RVR#040 or AL2_ID_RVR#050.

AL2_ID_RVR#030 Verify Subscriber as Revocant

When the Subscriber seeks revocation of the Subscriber's own credential, the enterprise must:

- a) if in person, require presentation of a primary Government Picture ID document that must be electronically verified by a record check against the provided identity with the specified issuing authority's records, or
- b) if remote:
 - i. electronically verify a signature against records (if available), confirmed with a call to a telephone number of record, or
 - ii. authenticate an electronic request as being from the same Subscriber, supported by a credential at Assurance Level 2 or higher.

AL2_ID_RVR#040 ETSP as Revocant

Where an CSP seeks revocation of a Subscriber's credential, the enterprise must establish that the request is either:

- a) from the Specified Service itself, with authorization as determined by established procedures, or
- b) from the client Credential Issuer, by authentication of a formalized request over the established secure communications network.

AL2_ID_RVR#050 Verify Legal Representative as Revocant

Where the request for revocation is made by a law enforcement officer or presentation of a legal document, the enterprise must:

- a) if in person, verify the identity of the person presenting the request, or
- b) if remote:
 - i. in paper/facsimile form, verify the origin of the legal document by a database check or by telephone with the issuing authority, or
 - ii. authenticate an electronic request as being from a recognized legal office, supported by a credential at Assurance Level 3 or higher.

3.7.3.2.3 Secure Revocation Request

This criterion requires that revocation requests between remote components of the service be made with secured communications.

An enterprise and its specified service must:

AL2_ID_SRR#010 Submit Request

Submit a request for the revocation to the Credential Issuer service (function), using a secured network communication if necessary.

3.7.3.3 Assurance Level 3 (Substantial)

3.7.3.3.1 Revocation Procedures

These criteria address general revocation functions, such as the processes involved and the basic requirements for publication.

An enterprise and its specified service must:

AL3_CM_RVP#010 Revocation procedures

State the conditions under which revocation of an issued credential may occur, the processes by which a revocation request may be submitted, the persons and organizations from which a revocation request will be accepted, the validation steps that will be applied to ensure the validity (identity) of the revocant, and the response time between a revocation request being accepted and the publication of revised certificate status.

AL3_CM_RVP#020 Secure status notification

Ensure that published credential status notification information can be relied upon in terms of the enterprise being its origin (i.e., its authenticity) and its correctness (i.e., its integrity).

AL3_CM_RVP#030 Revocation publication

Ensure that published credential status notification is revised within 24 hours of the receipt of a valid revocation request, such that any

subsequent attempts to use that credential in an authentication shall be unsuccessful. The nature of the revocation mechanism shall be in accord with the technologies supported by the service.

AL3_ID_RVP#040 Revocation Records

Retain a record of any revocation of a credential that is related to a specific identity previously verified, solely in connection to the stated credential. At a minimum, records of revocation must include:

- a) the Revocant's full legal name.
- b) the Revocant's current address.
- c) type, issuing authority and reference number(s) of all documents checked in the identity proofing process for the Revocant.
- d) the Revocant's authority to revoke (e.g., subscriber themselves, someone acting with the subscriber's power of attorney, the credential issuer, law enforcement or other legal due process).
- e) the Subscriber's full legal name and, where applicable, unique service reference (e.g., certificate serial number, IP address).
- f) the Subscriber's date of birth.
- g) the Subscriber's current address of record.
- h) the Credential Issuer's identity (if not directly responsible for the Identity Proofing service).
- i) the identity associated with the credential (whether the Subscriber's name or a pseudonym).
- j) the reason for revocation.

AL3_ID_RVP#050 Record Retention

Retain securely the record of the revocation process for the duration of the Subscriber's account plus 7.5 years.

3.7.3.3.2 Verify Revocant's Identity

Revocation of a credential requires that the requestor and the nature of the request be verified as rigorously as the original identity proofing. The enterprise should not act on a request for revocation without first establishing the validity of the request (if it does not itself determine the need for revocation).

In order to do so, the enterprise and its specified service must:

AL3_ID_RVR#010 Verify revocation identity

Establish that the credential for which a revocation request is received is one that was initially issued by the Specified Service, applying the same process and criteria as would be applied to an original identity proofing.

AL3_ID_RVR#020 Revocation reason

Establish the reason for the revocation request as being sound and well-founded, in combination with verification of the Revocant, according to AL3_ID_RVR#030, AL3_ID_RVR#040 or AL3_ID_RVR#050.

AL3_ID_RVR#030 Verify Subscriber as Revocant

When the Subscriber seeks revocation of the Subscriber's own credential:

- a) if in-person, require presentation of a primary Government Picture ID document that must be electronically verified by a record check against the provided identity with the specified issuing authority's records, or
- b) if remote:
 - i. electronically verify a signature against records (if available), confirmed with a call to a telephone number of record, or
 - ii. authenticate an electronic request as being from the same Subscriber, supported by a credential at Assurance Level 3 or higher.

AL3_ID_RVR#040 Verify ETSP as Revocant

Where an CSP seeks revocation of a Subscriber's credential, establish that the request is either:

- a) from the Specified Service itself, with authorization as determined by established procedures, or
- b) from the client Credential Issuer, by authentication of a formalized request over the established secure communications network.

AL3_ID_RVR#050 Legal Representative as Revocant

Where the request for revocation is made by a law enforcement officer or presentation of a legal document:

- a) if in person, verify the identity of the person presenting the request, or
- b) if remote:
 - i. in paper/facsimile form, verify the origin of the legal document by a database check or by telephone with the issuing authority, or
 - ii. authenticate an electronic request as being from a recognized legal office, supported by a credential at Assurance Level 3 or higher.

3.7.3.3.3 Secure Revocation Request

This criterion requires that revocation requests between remote components of the service be made with secured communications.

An enterprise and its specified service must:

AL3_ID_SRR#010 Submit Request

Submit a request for the revocation to the Credential Issuer service (function), using a secured network communication if necessary.

3.7.3.4 Assurance Level 4 (High)

3.7.3.4.1 Revocation Procedures

These criteria address general revocation functions, such as the processes involved and the basic requirements for publication.

An enterprise and its specified service must:

AL4_CM_RVP#010 Revocation procedures

State the conditions under which revocation of an issued certificate may occur, the processes by which a revocation request may be submitted,

the persons and organizations from which a revocation request will be accepted, the validation steps that will be applied to ensure the validity (identity) of the revocant, and the response time between a revocation request being accepted and the publication of revised certificate status.

AL4_CM_RVP#020 Secure status notification

Ensure that published credential status notification information can be relied upon in terms of the enterprise being its origin (i.e., its authenticity) and its correctness (i.e., its integrity).

AL4_CM_RVP#030 Revocation publication

Ensure that published credential status notification is revised within 24 hours of the receipt of a valid revocation request, such that any subsequent attempts to use that credential in an authentication shall be unsuccessful. The nature of the revocation mechanism shall be in accord with the technologies supported by the service.

AL4_ID_RVP#040 Revocation Records

Retain a record of any revocation of a credential that is related to a specific identity previously verified, solely in connection to the stated credential. At a minimum, records of revocation must include:

- a) the Revocant's full legal name.
- b) the Revocant's current address.
- c) type, issuing authority and reference number(s) of all documents checked in the identity-proofing process for the Revocant.
- d) the Revocant's authority to revoke (e.g., subscriber themselves, someone acting with the subscriber's power of attorney, the credential issuer, law enforcement or other legal due process).
- e) the Subscriber's full legal name and, where applicable, unique service reference (e.g., certificate serial number, IP address).
- f) the Subscriber's date of birth.
- g) the Subscriber's current address of record.
- h) the Credential Issuer's identity (if not directly responsible for the Identity Proofing service).
- i) the identity associated with the credential (whether the Subscriber's name or a pseudonym).
- j) the reason for revocation.

AL4_ID_RVP#050 Record Retention

Retain securely the record of the revocation process for the duration of the Subscriber's account plus 7.5 years.

3.7.3.4.2 Revocation and Re-key

Revocation of a credential requires that the requestor and the nature of the request be verified as rigorously as the original identity proofing. The enterprise should not act on a request for revocation without first establishing the validity of the request (if it does not itself determine the need for revocation).

In order to do so, the enterprise and its specified service must:

AL3_ID_RVR#010 Verify revocation identity

Establish that the credential for which a revocation request is received is one that was initially issued by the Specified Service, applying the same process and criteria as would apply to an original identity proofing.

AL3_ID_RVR#020 Revocation reason

Establish the reason for the revocation request as being sound and well-founded, in combination with verification of the Revocant, according to AL4_CM_RVR#030, AL4_CM_RVR#040 or AL4_CM_RVR#050.

AL4_CM_RVR#030 Verify Subscriber as Revocant

Where the Subscriber seeks revocation of the Subscriber's own credential:

- a) if in person, require presentation of a primary Government Picture ID document that shall be verified by a record check against the provided identity with the specified issuing authority's records, or
- b) if remote:
 - i. verify a signature against records (if available), confirmed with a call to a telephone number of record, or
 - ii. authenticate an electronic request as being from the same Subscriber, supported by a different credential at Assurance Level 4.

AL4_CM_RVR#040 Verify ETSP as Revocant

Where an CSP seeks revocation of a Subscriber's credential, establish that the request is either:

- a) from the Specified Service itself, with authorization as determined by established procedures, or
- b) from the client Credential Issuer, by authentication of a formalized request over the established secure communications network.

AL4_CM_RVR#050 Legal Representative as Revocant

Where the request for revocation is made by a law enforcement officer or presentation of a legal document:

- a) if in person, verify the identity of the person presenting the request, or
- b) if remote:
 - i. in paper/facsimile form, verify the origin of the legal document by a database check or by telephone with the issuing authority, or
 - ii. authenticate an electronic request as being from a recognized legal office, supported by a different credential at Assurance Level 4.

Re-key of a credential requires that the requestor be verified as the subject with as much rigor as was applied to the original identity proofing. The enterprise should not act on a request for re-key without first establishing that the requestor is identical to the subject.

In order to do so, the enterprise and its specified service must:

AL4_CM_RKY#010 Verify Requestor as Subscriber

Where the Subscriber seeks a re-key for the Subscriber's own credential:

- a) if in-person, require presentation of a primary Government Picture ID document that shall be verified by a record check against the provided identity with the specified issuing authority's records, or
- b) if remote:
 - i. verify a signature against records (if available), confirmed with a call to a telephone number of record, or
 - ii. authenticate an electronic request as being from the same Subscriber, supported by a different credential at Assurance Level 4.

3.7.3.4.3 Re-key requests from any other parties must not be accepted.

3.7.3.4.4 Secure Revocation/Re-key Request

This criterion requires that revocation requests between remote components of the service be made with secured communications.

The enterprise and its specified service must:

AL4_ID_SRR#010 Submit Request

Submit a request for the revocation to the Credential Issuer service (function), using a secured network communication if necessary.

3.7.4 PART D--CREDENTIAL STATUS MANAGEMENT

These criteria deal with credential status management, such as the receipt of requests for new status information arising from a new credential being issued or a revocation or other change to the credential that requires notification. They also deal with the provision of status information to requesting parties having the right to access such information.

3.7.4.1 Assurance Level 1 (Minimal)

3.7.4.1.1 Status Maintenance

An enterprise and its specified service must:

AL1_CM_CSM#010 Maintain Status Record

Maintain a record of the status of all credentials issued.

AL1_CM_CSM#040 Status Information Availability

Provide, with 95% availability, a secure automated mechanism to allow Relying Parties to determine credential status and authenticate the subject's identity.

3.7.4.2 Assurance Level 2 (Moderate)

An enterprise and its specified service must:

AL2_CM_CSM#010 Maintain Status Record

Maintain a record of the status of all credentials issued.

AL2_CM_CSM#020 Validation of Status Change Requests

Authenticate all requestors seeking to have a change of status recorded and published and validate the requested change before considering processing the request. Such validation should include:

- a) the requesting source as one from which the Specified Service expects to receive such requests.
- b) if the request is not for a new status, the credential or identity as being one for which a status is already held.

AL2_CM_CSM#030 Revision to Published Status

Process authenticated requests for revised status information and have the revised information available for access within a period of 72 hours.

AL2_CM_CSM#040 Status Information Availability

Provide, with 95% availability, a secure automated mechanism to allow Relying Parties to determine credential status and authenticate the subject's identity.

AL2_CM_CSM#050 Inactive Credentials

Disable any credential that has not been successfully authenticated during a period of 12 [AL3: 9] [AL4: 3] months.

3.7.4.3 Assurance Level 3 (Substantial)

3.7.4.4 Assurance Level 4 (High)

3.7.5 PART E--CREDENTIAL VALIDATION/AUTHENTICATION

These criteria apply to credential validation and identity authentication.

3.7.5.1 Assurance Level 1 (Minimal)

3.7.5.1.1 Assertion Security

An enterprise and its specified service must:

AL1_CM_ASS#010 Validation and Assertion Security

Provide validation of credentials to a relying party using a protocol that:

- a) requires authentication of the Specified Service or of the validation source.
- b) ensures the integrity of the authentication assertion.

AL1_CM_ASS#020 No Post Authentication

Not authenticate credentials that have been revoked.

AL1_CM_ASS#030 Proof of Possession

Use an authentication protocol that requires the claimant to prove possession and control of the authentication token.

AL1_CM_ASS#040 Assertion Lifetime

No stipulation.

3.7.5.2 Assurance Level 2 (Moderate)

3.7.5.2.1 Assertion Security

An enterprise and its specified service must:

AL2_CM_ASS#010 Validation and Assertion Security

Provide validation of credentials to a relying party using a protocol that:

- a) requires authentication of the Specified Service itself or of the validation source.
- b) ensures the integrity of the authentication assertion.

AL2_CM_ASS#020 No Post Authentication

Not authenticate credentials that have been revoked.

AL2_CM_ASS#030 Proof of Possession

Use an authentication protocol that requires the claimant to prove possession and control of the authentication token.

AL2_CM_ASS#040 Assertion Lifetime

Generate assertions so as to indicate and effect their expiration 12 hours after their creation.

3.7.5.3 Assurance Level 3 (Substantial)

3.7.5.3.1 Assertion Security

An enterprise and its specified service must:

AL3_CM_ASS#010 Validation & Assertion Security

Provide validation of credentials to a relying party using a protocol that:

- a) requires authentication of the Specified Service itself or of the validation source.
- b) ensures the integrity of the authentication assertion.

AL3_CM_ASS#020 No Post Authentication

Not authenticate credentials that have been revoked.

AL3_CM_ASS#030 Proof of Possession

Use an authentication protocol that requires the claimant to prove possession and control of the authentication token.

AL3_CM_ASS#040 Assertion Lifetime

For non-cryptographic credentials, generate assertions that indicate and effect their expiration 12 hours after their creation; otherwise, notify the Relying Party of how often the revocation status sources are updated.

3.7.5.4 Assurance Level 4 (High)

3.7.5.4.1 Assertion Security

An enterprise and its specified service must:

AL4_CM_ASS#010 Validation & Assertion Security

Provide validation of credentials to a relying party using a protocol that:

- a) requires authentication of the Specified Service itself or of the validation source.
- b) ensures the integrity of the authentication assertion.

AL4_CM_ASS#020 No Post Authentication

Not authenticate credentials that have been revoked.

AL4_CM_ASS#030 Proof of Possession

Use an authentication protocol that requires the claimant to prove possession and control of the authentication token.

AL4_CM_ASS#040 Assertion Lifetime

Notify the Relying Party of how often the revocation status sources are updated.

3.7.6 COMPLIANCE TABLES

Use the following tables to correlate criteria and evidence offered/compliance achieved. A table is provided for each assurance level. The tables are linked to their respective criteria and vice-versa, to aid referencing between them. Service providers preparing for an assessment can use the table appropriate to the level at which they are seeking approval to correlate evidence with criteria or to justify non-applicability of criteria (e.g., specific service types not offered): Assessors can use the tables to record the steps they take in their assessment and their determination of compliance or failure.

(THESE TABLES, AND OTHER BLANK TABLES IN PART 3, WILL BE COOMPILETED PRIOR TO PUBLIC EXPOSURE OF THE FRAMEWORK IN JANUARY 2005.)

Table 3-5 CM-SAC - AL1 Compliance

Clause	Description	Compliance

Table 3-6 CM-SAC - AL2 Compliance

Clause	Description	Compliance

Table 3-7 CM-SAC - AL3 Compliance

Clause	Description	Compliance

Table 3-8 CM-SAC - AL4 Compliance

Clause	Description	Compliance

4 ACCREDITATION AND CERTIFICATION RULES

4.1 Assessor Accreditation EAP certified services can be offered only by a CSP who is EAP-certified. EAP certification can only be granted by an EAP accredited assessor. Assessor accreditation requires the following steps:

1. An assessor submits an application for accreditation.
2. The EAP evaluates the application according to the criteria set for accreditation.
3. The applicant is notified of the EAP decision.
4. In the event of a negative decision, the applicant is offered an appeal.

4.1.1 CRITERIA FOR ASSESSOR ACCREDITATION

The Board of Directors or any committee or other entity the Board may empower by delegation (the Board) may choose to recognize the accreditation of another body in lieu of its own accreditation or as a supplement to its own accreditation. The Board shall apply the following criteria when determining whether to approve the application of an assessor for accreditation.

4.1.1.1 Expertise With Relevant Standards

Prior to accreditation, the assessor must demonstrate expertise in the application of at least one of the following evaluation standards. In addition, the assessor must demonstrate competence in the application of any supplemental evaluation criteria formally identified by the EAP and against which CSPs are to be assessed for certification by the EAP.

4.1.1.2 Business Expertise

The assessor must:

- Have been in existence for more than 1 month
- Be financially solvent and stable and reasonably certain to remain so for the foreseeable future
- Have sufficient financial resources, either through direct reserves, insurance or otherwise, to absorb the cost resulting from wrongful certification of a CSP upon its recommendation for the period of such certification and for 1 year thereafter
- Demonstrate excellence, breadth and depth in the relevant fields of endeavor, including electronic authentication, federated identity management, information security and the processes and methods of assessment of such fields
- Not have any key personnel or personnel directly involved in assessments or development and delivery of assessment reports and recommendations to the EAP who have been convicted of a crime

4.1.2 ASSESSMENT

Prior to accreditation, assessors may be subject to an on-site evaluation by the EAP or a designee. This assessment is to determine compliance with the current EAP criteria for accreditation and to evaluate expertise, processes and equipment necessary to conduct the certifications of CSPs according to EAP certification criteria and rules. Whether an on-site inspection is scheduled or not, the assessor shall provide information as provided for in Section 4.1.1.1 and Section 4.1.1.2.

4.1.3 ACCREDITATION DECISION AND APPEAL

Within a reasonable time and at the discretion of the EAP, the EAP shall make a determination of accreditation and communicate that determination to the applicant.

In the event of a negative decision, the assessor may request an appeal of the accreditation decision by the EAP. Such request shall be considered by a three-member panel of the EAP Board of Directors or any committee or other entity the Board may empower by delegation, composed of people who have been uninvolved with the decision and are impartial.

4.1.4 MAINTAINING ACCREDITATION

After the initial year of accreditation, assessors may be subject to an on-site or remote surveillance evaluation. The surveillance assessment shall include review of at least the following:

- Internal audit reports
- Minutes of management review meetings
- Results of certification assessments, if any
- Any changes in key personnel, facilities and/or major test equipment
- Information on any other significant changes in the quality system of the assessor

The EAP, or a designee, may conduct an on-site reassessment or surveillance assessment of accredited assessors at a minimum of once every 2 years, for verification of continued compliance with EAP accreditation criteria and rules.

4.2 Certification of Credential Service Provider Offerings

Only a CSP whose product or line of business is currently certified by the EAP can issue or otherwise purvey certified credentials or validation of EAP certified credentials under an EAP brand or EAP business rules or for use within the EAP system.

4.2.1 PROCESS OF CERTIFICATION

The process of certification for each product or line of business for which certification is sought by a CSP includes the following steps:

1. A CSP seeking certification for a product or line of business begins the formal process by reviewing the list of EAP accredited and approved assessors. The CSP selects an assessor for commencing formal assessment, for which there shall be a separate contractual arrangement between the applicant and the chosen assessor.

2. The EAP accredited assessor selected by the applicant conducts an assessment of the CSP product or line of business. At the conclusion of the assessment process, the assessor and the CSP separately submit their respective materials to the EAP.
3. The assessor submits the assessment report and its recommendation regarding certification directly to the EAP.
4. The CSP submits an application for certification to the EAP, including agreement to the EAP business rules and other relevant EAP binding documents, as well as specification of each line of offerings for which certification is sought, and the assurance level (AL) at which each certification is sought.
5. After receiving the assessment and application materials from the assessor and CSP, respectively, the EAP evaluates the relevant information and makes a decision on certification.
6. The EAP communicates its decision on certification to the CSP and the assessor.
7. In the event of a negative decision, the CSP is afforded an appeal.
8. In the event of a positive decision, the CSP's certified product or line of business is added to the EAP Certified CSP offering list.

4.2.1.1 Application

The EAP shall provide an application form for certification as an EAP CSP both on the EAP web site and in paper form. The application shall include contact information; an agreement to abide by the EAP rules and any other applicable EAP requirements identified in the application, such as a license agreement or other terms and conditions; and an EAP appeal request form to request review of the final certification determination. In addition, the application shall require the applicant to specify the precise scope of each line of business for which certification is sought, the AL at which each certification is sought, and any existing applicable accreditation, certification or similar approvals granted to each specified line of business.

4.2.1.2 Initial Evaluation

Upon receipt of an application for certification, the EAP shall review the contents and audit report.

4.2.1.3 Assessment

Prior to certification, CSPs may be subject to an on-site assessment by the assessor. The assessment shall determine compliance with the current EAP Service Assessment Criteria.

An EAP accredited assessor will conduct an on-site reassessment or surveillance assessment of a CSP at least 1 year after certification and, at a minimum, once every 2 years thereafter, for verification of continued compliance with EAP certification requirements.

4.2.2 CRITERIA FOR CERTIFICATION OF CSP LINE OF BUSINESS

4.2.2.1 Standard Evaluation Criteria Used by Assessor

For each line of business for which certification is sought, the practices, operations, organization, personnel and other relevant aspects of a CSP must be assessed against one of the following evaluation standards:

Table 4-1. Evaluation Standards for Different Assurance Levels

Assurance Level	Evaluation Standard
1	tbd
2	tbd
3	tbd
4	tbd

When multiple offerings share one or more assessment criteria, the criteria need only be considered once per assessment. Such criteria may include management organization, physical security or personnel who are common to each line of business for which certification is sought. In addition, criteria that have been previously assessed positively by an adequate assessor and assessment process and that are equivalent to EAP criteria may be relied upon for purposes of an EAP assessment. Whether such criteria are deemed adequate and equivalent must be decided by the EAP Board. Such determination by the Board may be triggered by a request by a previously-assessed applicant CSP, an accredited assessor or on the initiative of the Board itself. Such determinations may be published from time to time as assessment guidance by the EAP.

4.2.2.2 Supplemental Criteria Used by Assessor

The criteria applied by assessors are identified in the EAP Service Assessment Criteria (Section 3).

4.2.3 CERTIFICATION DECISION

4.2.3.1 Assessor Delivers Report and Recommendation

Upon conclusion of the assessment, for each line of business for which certification has been sought, the assessor shall deliver to the EAP a final assessment report, including a recommendation on whether to certify the assessed CSP.

4.2.3.2 EAP Makes Certification Decision

Upon receipt of each assessment report and recommendation on certification from the assessor, the EAP shall determine, within a reasonable time to be set by the EAP Board, whether to deny certification to the CSP, certify the CSP, or take such other action as may be appropriate, including requesting further information, contractual agreements or provable action from the CSP by a certain date.

The decision of the EAP shall be communicated to both the CSP and the assessor within a reasonable time, to be set by the EAP Board.

4.2.4 APPEALS PROCESS

Upon receipt of the EAP decision on certification, a CSP may request an appeal of that decision. Upon receiving the Appeal Request from a CSP and within a reasonable period of time, to be set by the EAP Board, the EAP shall appoint a three-member review panel from among EAP Board of Directors or any committee or other entity the Board may empower by delegation, comprised of people who have been uninvolved with the decision at issue and are impartial. Said panel shall consider the request and make a final determination. The panel may make its determination based solely upon the information presented in the appeal request, including any attachments, or it may request additional information from one or more parties or schedule a hearing to permit the affected parties to further clarify and present their positions.

4.2.5 MAINTAINING CERTIFICATION

The CSP must notify the assessor and the EAP of any material change that may lower the assurance level of the certified product or line of business 60 days before the change is performed or immediately upon the incidence of any unplanned change. The EAP, in consultation with the assessor, will determine whether the changes are sufficient to require re-assessment. The re-assessment, if required, need only cover those elements that have changed.

Annual renewal agreements are required for a certification to remain in effect. The CSP warrants continued compliance with the criteria of the assessment in this agreement and provides annual audit results. An independent third party must audit any certified product or line of business assessed at AL2 or higher every 2 years. Other audits may be internal. The EAP, in consultation with the assessor, may require a partial reassessment if the scope of the audits does not include all applicable criteria. Additional maintenance activities may be stipulated in the participation agreement between the EAP and the CSP.

4.3 Process for Handing Non-Compliance

The following process for handling non-compliance applies both to accredited assessors and to certified CSPs, unless otherwise noted.

4.3.1 COMPLIANCE DETERMINATION

Upon receipt by the EAP of credible information that an assessor or CSP is not in compliance with the requirements for accreditation or certification, the EAP Board or staff or a committee at Board discretion shall determine whether the assessor or CSP is in fact in material non-compliance with EAP requirements and shall communicate the determination to the affected parties. The Board of Directors shall establish further criteria, as needed, detailing conduct or circumstances constituting material non-compliance with EAP rules or standards.

4.3.2 PERIOD TO CURE

An assessor or CSP found to be in material non-compliance shall be afforded an opportunity and period of time to remedy the non-compliance, provided such period does not unduly jeopardize the integrity of the EAP System or the rights or property of another party.

4.3.3 ADMINISTRATIVE REOURSE

Based on review of all available data and in light of all the relevant circumstances, the EAP Board of Directors may take administrative recourse against any signatory determined to be in material non-compliance with these business rules, to include, as needed, any of the following remedies.

4.3.3.1 Warning

The non-complying party may be given a warning. The warning may be confidential or may be publicized within the EAP or publicized more broadly, at the discretion of the EAP Board of Directors.

4.3.3.2 Credential Revocation

The non-complying party may be required to revoke one or more EAP-branded credentials or to remove the EAP brand from such credentials.

4.3.3.3 Non-compliance Fees

The non-complying party may be subject to a schedule of fees, to be specified by the EAP Board of Directors. The fees may increase according to the length of time before the party comes back into compliance.

4.3.3.4 Suspension

The non-complying party may have its participation in the EAP System suspended, including the suspension of accreditation or certification, pending coming back into compliance.

4.3.3.5 Termination

The non-complying party may have its participation in the EAP System terminated, including the termination of accreditation or certification.

4.4 Acceptable Public Statements Regarding EAP Accreditation and Certification

It is acceptable for a party to indicate that it is an "EAP Accredited Assessor" or an "EAP Certified Credential Service Provider" for any period during which such statement is true. However, no party may make any public claim, whether to media outlets, in bids and other proposals, in marketing materials or otherwise, regarding its status as an applicant for accreditation or certification, nor can it claim that it is in the process of achieving such status.

5 EAP GLOSSARY

Accreditation. The process used to achieve formal recognition that an organization has agreed to the EAP operating rules and is competent to perform assessments using the Service Assessment Criteria.

AL. See *assurance level*

Applicant. An individual or person acting as a proxy for a machine or corporate entity who is the subject of an identity proofing process.

Approval. The process by which the EAP Board accepts the compliance of a certified service and the ETSP responsible for that service commits to upholding the EAP Rules.

Approved encryption. Any cryptographic algorithm or method specified in a FIPS or a NIST recommendation. Refer to <http://csrc.nist.gov/cryptval/>

Approved service. A certified service which has been granted an approval by the EAP Board.

Assertion. A statement from a verifier to a relying party that contains identity or other information about a subscriber.

Assessment. A process used to evaluate an electronic trust service and the service provider using the requirements specified by one or more Service Assessment Criteria for compliance with all applicable requirements.

Assessor. A person or corporate entity who performs an assessment.

Assurance level (AL). A degree of certainty that a claimant has presented a credential that refers to the claimant's identity. Each assurance level expresses a degree of confidence in the process used to establish the identity of the individual to whom the credential was issued and a degree of confidence that the individual who uses the credential is the individual to whom the credential was issued. The four assurance levels are:

Level 1 (Minimal): Little or no confidence in the asserted identity's validity

Level 2 (Moderate): Some confidence in the asserted identity's validity

Level 3 (Substantial): High confidence in the asserted identity's validity

Level 4 (High): Very high confidence in the asserted identity's validity

Attack. An attempt to obtain a subscriber's token or to fool a verifier into believing that an unauthorized individual possesses a claimant's token.

Attribute. A property associated with an individual.

Authentication. Authentication simply establishes identity, not what that identity is authorized to do or what access privileges he or she has.

Authentication protocol. A well-specified message exchange process that verifies possession of a token to remotely authenticate a claimant. Some authentication protocols also generate cryptographic keys that are used to protect an entire session, so that the data transferred in the session is cryptographically protected.

Authorization. Process of deciding what an individual ought to be allowed to do.

Bit. A binary digit: 0 or 1

Brand. See EAP Branded Credential.

Certification. The EAP's affirmation that a particular credential service provider can provide a particular credential service at a particular assurance level.

Claimant. A party whose identity is to be verified.

Certification Body. An organization which has been deemed competent to perform assessments of a particular type. Such assessments may be formal evaluations or testing and be based upon some defined set of standards or other criteria.

Certified service. An electronic trust service which has been assessed by an EAP-recognized certification body and found to be compliant with the applicable SACs.

Credential. An object to be verified when presented in an authentication transaction. A credential can be bound in some way to the individual to whom it was issued, or it can be a bearer credential. Electronic credentials are digital documents that bind an identity or an attribute to a subscriber's token.

Credential management. DEFINITION REQUIRED

Credential service. A type of electronic trust service that supports the verification of identities (identity proofing), the issuance of identity-related assertions/credentials/tokens, and the subsequent management of those credentials (for example, renewal, revocation and the provision of related status and authentication services).

Credential service provider (CSP) . An electronic trust service provider that operates one or more credential services. A CSP can include a Registration Authority.

Credential service. A reliable, efficient means of disseminating credential information.

CSP. See *credential service provider*.

Cryptographic token. A token for which the secret is a cryptographic key.

EAP. See *Electronic Authentication Partnership*

EAP assessor. An organization that has agreed to the EAP Rules and that has been accredited to conduct assessments of credential service providers.

EAP-branded credential. Information indicating the individual identity of a natural person, according to a CSP certified by the EAP to issue, process, validate or otherwise purvey such credential.

EAP credential service provider. Organization that has agreed to the EAP Operating Rules and other applicable Rules, and that has been Certified to issue, process, validate, etc., an EAP Branded Credential.

EAP credential service provider. Organization that has agreed to the EAP Rules and other applicable rules, and that has been certified to issue, process, and validate, an EAP-branded credential

EAP-recognized assessor. A body that has been granted an accreditation to perform assessments against Service Assessment Criteria, at the specified assurance level(s).

EAP-recognized certification body. A certification body which has been accredited by, or whose qualifications have been otherwise established by, a scheme which the EAP Board has deemed to be appropriate for the purposes of determining an ETSP's competence to perform assessments against EAP's criteria.

Electronic Authentication Partnership (EAP). The multi-industry partnership working on enabling interoperability among public and private electronic authentication (e-authentication) systems.

Electronic credentials. Digital documents used in authentication that bind an identity or an attribute to a subscriber's token.

Electronic trust service (ETS). A service that enhances trust and confidence in electronic transactions, typically but not necessarily using cryptographic techniques or involving confidential material such as PINs and passwords

Electronic trust service provider (ETSP). An entity that provides one or more electronic trust services.

ETS. See *electronic trust service*

ETSP. See *electronic trust service provider*

Federated identity management. A system that allows individuals to use the same user name, password, or other personal identification to sign on to the networks of more than one enterprise in order to conduct transactions.

Federal Information Processing Standards (FIPS). Standards and guidelines issued by the National Institute of Standards and Technology (NIST) for use government-wide. NIST develops FIPS when the Federal government has compelling requirements, such as for security and interoperability, for which no industry standards or solutions are acceptable.

FIPS. See *Federal Information Processing Standards*

Identification. Process of using claimed or observed attributes of an individual to infer who the individual is.

Identifier. Something that points to an individual, such as a name, a serial number or some other pointer to the party being identified.

Identity authentication. Process of establishing an understood level of confidence that an identifier refers to an identity. It may or may not be possible to link the authenticated identity to an individual.

Identity. A unique name for single person. Because a person's legal name is not necessarily unique, identity must include enough additional information (for example, an address or some unique identifier such as an employee or account number) to make a unique name.

Identity binding. The extent to which an electronic credential can be trusted to be a proxy for the entity named in it.

Identity proofing. The process by which identity-related information is validated so as to identify a person with a degree of uniqueness and certitude sufficient for the purposes for which that identity is to be used.

Identity proofing policy. A set of rules that defines identity-proofing requirements (required evidence, format, manner of presentation, validation), records actions required of the registrar, and describes any other salient aspects of the identity-proofing function that are applicable to a particular community or class of applications with common security requirements. An identity proofing policy is designed to accomplish a stated assurance level.

Identity proofing service provider. An electronic trust service provider which offers, as a standalone service, the specific electronic trust service of identity proofing. This service provider is sometimes referred to as a Registration Agent/Authority (RA).

Identity proofing practice statement. A statement of the practices that an identity proofing service provider employs in providing its services in accordance with the applicable identity proofing policy.

Issuer. Somebody or something that supplies or distributes something officially.

Level of assurance. See *assurance level*

Network. An open communications medium, typically, the Internet, that is used to transport messages between the claimant and other parties.

Password. A shared secret character string used in authentication protocols. In many cases the claimant is expected to memorize the password.

Practice statement. A formal statement of the practices followed by an authentication entity (e.g., RA, CSP or verifier) that typically defines the specific steps taken to register and verify identities, issue credentials and authenticate claimants.

Public key. The public part of the asymmetric key pair that is typically used to verify signatures or encrypt data.

Public key infrastructure (PKI). A set of technical and procedural measures used to manage public keys embedded in digital certificates. The keys in such

certificates can be used to safeguard communication and data exchange over potentially unsecure networks.

Registration. An entry in a register, or somebody or something whose name or designation is entered in a register.

Relying party. An entity that relies upon a subscriber's credentials, typically to process a transaction or grant access to information or a system.

Role. The usual or expected function of somebody or something, or the part somebody or something plays in a particular action or event.

SAC. See *Service Assessment Criteria*

Security. A collection of safeguards that ensures the confidentiality of information, protects the integrity of information, ensures the availability of information, accounts for use of the system, and protects the system(s) and/or network(s) used to process the information.

Service Assessment Criteria (SAC). A set of requirements levied upon specific organizational and other functions performed by electronic trust services and service providers. Services and service providers must comply with all applicable criteria to qualify for EAP approval.

Signatory. A party that opts into and agrees to be bound by the EAP Rules according to the specified procedures.

Specified service. The electronic trust service which for the purposes of an EAP assessment is the subject of criteria set out in a particular SAC, or in an application for assessment, in a grant of an approval or other similar usage as may be found in various EAP documentation.

Subject. An entity that is able to use an electronic trust service subject to agreement with an associated subscriber. A subject and a subscriber can be the same entity.

Subscriber. A party that has entered into an agreement to use an electronic trust service. A subscriber and a subject can be the same entity.

Threat. An adversary that is motivated and capable to violate the security of a target and has the capability to mount attacks that will exploit the target's vulnerabilities.

Token. Something that a claimant possesses and controls (typically a key or password) that is used to authenticate the claimant's identity.

Trust framework. The body of work that collectively defines the industry-led self-regulatory framework for electronic trust services in the United States, as operated by the EAP. The trust framework includes descriptions of criteria, rules, procedures, processes, and other documents.

Verification. Establishment of the truth or correctness of something by investigation of evidence.

6 PUBLICATION ACKNOWLEDGEMENTS

The EAP would like to thank the following working group chairs and vice chairs for their commitment and dedication to the Trust Framework.

Interim Chair: James Lewis, The Center for Strategic and International Studies
Interim Vice Chair: David Temoshok, U.S. General Services Administration

Business Requirements & Processes Work Group
Chair: Linda G. Elliot, PingID Network
Vice Chair: Thomas Greco, beTRUSTed

Credential Services Assessment Criteria & Levels of Assurance Work Group
Chair: Robert J. Schlecht, Mortgage Bankers Association of America
Vice Chair: Von Harrison, U.S. General Services Administration

Credential Services Assessment Criteria Sub Work
Chair: Nancy Black, HollenGroup
Vice Chair: Richard Wilsher, The Zygma Partnership

Levels of Assurance Sub Work Group
Chair: Peter Alterman, National Institutes of Health
Vice Chair: Noel Nazario, KPMG LLP

Interoperability Sub Work Group
Chair: William E. Burr, National Institute of Standards and Technology
Vice Chair: Kurt Van Etten, eBay, Inc.

Evaluation, Accreditation & Compliance Work Group
Chair: Gary Glickman, Giesecke & Devrient Cardtech, Inc.
Vice Chair: Cornelia Chebinou, National Association of State Auditors, Comptrollers and Treasurers

EAP Governance Work Group
Chair: Paula Arcioni, State of New Jersey, Office of Information Technology
Vice Chair: Roger J. Cochetti, CompTIA

Consultants
Yuriy Dzambasow, A&N Associates, Inc.
Dan Greenwood, Commonwealth of Massachusetts
Richard Wilsher, The Zygma Partnership

Members of the various work groups include:

Khaja Ahmed, Microsoft Corporation
Michael A. Aisenberg, VeriSign, Inc.
Peter Alterman, National Institutes of Health
Paula Arcioni, State of New Jersey, Office of Information Technology
Jonathan Askins, ACXIOM Corporation
Asaf Awan, Parkweb Associates
Stefano Baroni, SETECS

Paul Barrett, Real User Corporation
Nancy Black, Hollen Group
Debb Blanchard, Enspier Technologies/GDT
Warren Blosjo, 3Factor
Daniel Blum, Burton Group
Iana Bohmer, Northrop Grumman Information Technology
Christine Borucke, Electronic Data Systems
Kirk Brafford, SSP-Litronic, Inc.
Mayi Canales, M Squared Strategies, Inc.
Richard Carter, American Association of Motor Vehicles Administration
Kim Cartwright, Experian
James A. Casey, NeuStar, Inc.
Ray Cavanaugh, Entegrity Solutions
Chuck Chamberlain, U.S. Postal Service
Cornelia Chebinou, National Association of State Auditors, Comptrollers and Treasurers
Rebecca Chisolm, Sun Microsystems Federal
Roger J. Cochetti, CompTIA
Dan Combs, Global Identity Solutions
John Cornell, U.S. General Services Administration
Sarah Currier, CheckFree Corporation
Chris Daly, IBM Corporation
Kathy DiMaggio, Sigaba Corporation
Yuriy Dzambasow, A&N Associates, Inc.
Josh Elliott, American Management Systems
Clay Epstein, Identrus LLC
Irving R. Gilson, Department of Defense
Gary Glickman, Giesecke & Devrient Cardtech, Inc.
James A. Gross, Wells Fargo
Kirk R. Hall, GeoTrust
Von Harrison, U.S. General Services Administration
Christopher Hankin, Sun Microsystems, Inc.
Michael Horkey, Global Identity Solutions
Katherine M. Hollis, Electronic Data Systems
Robert Housel, National City Corporation
Burt Kaliski, RSA Security, Inc.
Shannon Kellogg, RSA Security, Inc.
James Kobielski, Burton Group
Patrick Lally, SSP-Litronic, Inc.
Steve Lazerowich, Enspier Technologies/GDT
Phillip S. Lee, SC Solutions, Inc.
Peter Lieberwirth, Authentidate
Chris Louden, Enspier Technologies/GDT
J. Scott Lowry, Enspier Technologies/GDT
Adele Marsh, PA Higher Education Assistance Agency
Patty McCarty, Private ID Systems
Doug McCoy, SAFLINK Corporation
Ben Miller, InsideID
Larry Miller, Identrus LLC
Sead Muftic, SETECS
Noel Nazario, KPMG LLP
Michael R. Nelson, IBM Corporation
Simon Nicholson, Sun Microsystems, Inc.

Pete Palmer, HIMSS NHII Task Force Advisor, Guidant Corporation
Stephen Permison, Standards Based Programs
Bob Pinheiro, Independent Security Researcher
Stephen L. Ranzini, University Bank
Christiane Reinhold, BearingPoint
Donald E. Rhodes, American Banker Association
Randy V. Sabet, Cooley Goodward, LLP
Ravi Sandhu, NSD Security
Dean Sarff, Minerals Management Service
Donald Saxinger, FDIC
Robert J. Schlecht, Mortgage Bankers Association of America
Howard Scmidt, eBay, Inc.
Ari Schwartz, Center for Democracy and Technology
John Shipley, The Shipley Group
Stephen P. Sill, U.S. General Services Administration
Helena G. Sims, NACHA – The Electronic Payments Association
Bill Smith, Sun Microsystems, Inc.
Tadgh Smith, IBM
Judith Spencer, U.S. General Services Administration
William Still, ChoicePoint Public Sector
Michael M. Talley, University Bancorp
David Temoshok, U.S. General Services Administration
Richard Thayer, ComTech, Inc.
John Ticer, NeuStar, Inc.
Kevin Trilli, VeriSign, Inc.
Matthew Tuttle, beTRUSTed
A. Jerald Varner, U.S. General Services Administration
Martin Wargon, Wave Systems Corporation
Richard Wilsher, The Zygma Partnership
David Weitzel, Mitretek Systems, Inc.
Michael Wolf, Authentidate
Gordon R. Woodrow, ClearTran, Inc.
Steve Worona, EDUCAUSE

ISSUES ANALYSIS BRIEF: SNAP-IN CONTRACTS ARCHITECTURE

MAY 25, 2004, EAP BRP Workgroup

Prepared by Daniel Greenwood, Esq.,

Background

At the last meeting, the BRP workgroup was presented with four potential ways to meet the goals and requirements of the EAP, while also respecting the emerging areas of consensus of workgroup members developed at prior meetings. Of them, there was a strong consensus for option 2, called the "snap-in" contracts approach. The basic elements of each option are described in Appendix 1, below. More relevant background is included, so as to document the decision making process, in Appendix 2.

Business Goals

It is useful to reiterate the most relevant goals of the EAP for the BRP, as reflected on the EAP web site and the majority of the presentations. The other goals are included in Appendix 2.

Drafting 'rules of engagement' for relying parties that will allow them to use third party credentials. These rules would take the place of bilateral agreements.

Description of "Snap-In" Contract Option

Each EAP Credential Service Provider (CSP) presents for pre-approval one or more standard Relying Party contracts to the EAP. The contract or contracts of the CSP are made available to any prospective Relying Party in advance of the Relying Party deciding whether to accept a credential from that CSP.

Each such agreement would in effect be a contract of adhesion ("take it or leave it" contract). The contracts can be presented in a standard format, for ease of review by prospective Relying Parties. There is an opportunity for give and take on the substance of the contracts as part of the approval process at the EAP level. For example, there may be opportunities to include aggregate pricing, public sector discounts or other benefits to Relying Parties as a result of attaining CSP services through EAP rather than direct contracting outside of the EAP circle of trust.

The contracting device, to avoid re-negotiating and executing bilateral contracts anew between each Relying Party and CSP participating in the system would be to have the terms of pre-approved contracts incorporated by reference into an overarching set of contractually enforceable rules. Under such a method, a Relying Party would need only execute one opt-in contract to come under the rules, and the rules would explicitly include reference to the contracting terms with each CSP, updated as they are approved, amended or removed from the EAP circle of trust. To avoid coming under any particular CSP set of contractual provisions, a Relying Party would need only avoid accepting a Credential issued by that CSP under the Rules.

At the last BRP call, there was desire expressed that this process of contract approval operate on a separate track from the more technical Certification and Accreditation process. The reason being certification by auditors or other objective assessors appeared ill suited to the very subjective and nuanced evaluations needed for approving service terms of a contract. Such evaluations implicate subtle judgements involving legal, business, strategy, and even socio-political dimensions. The reasoning was that an EAP body (such as a sub-committee of the Board of Directors, or a proportionally appointed or elected stakeholder committee, for example) would be better suited to make such evaluations, to interpret in an evolving manner any criteria for approval that are set, and to engage in the back and forth with applicant CSPs on the content

of their contracts as part of the approval process. Whether a CSP would engage in contracts approval before, during or after certification by an accredited assessor was not discussed.

Pro's of Snap-In Option

The key positive elements of this approach include:

1. It provides a way to achieve the "no additional bilateral contracts" requirement. With the modular architecture of option 2, no additional procurements, bids, negotiations and completely stand-alone contracts are needed.
2. It is achievable with current technology. Once rules are set and opt in contracts are finalized, simple reference to existing technical standards and practices will suffice.
3. It does not require all CSPs and Relying Parties to agree to a single set of provisions. With option 3, by contrast, presumably all key stakeholders would have to reach consensus on a single set of rules that would cover multiple parties from the start. Eventual convergence around a small or single set of provisions may emerge over time and can be reflected in the rules or as a default master contract.
4. It provides sufficiently comprehensive, actionable and salient information in advance to Relying Parties. Relying Parties will have an opportunity to select from among the recognized EAP CSPs with reference to all of the relevant information needed to join the respective circle of trust. In this way, the EAP becomes a connecting circle, joining other circles of trust in a meaningful and actionable manner.
5. It represents a low bar to entry (by not requiring agreement to single terms for all or negotiation of new bilaterals every time), and hence provides a simple way for CSPs and Relying Parties to sign up, and rapidly scale up globally.
6. It provides a step toward option 3 (more comprehensive rules that do not leave out stakeholders) and does not preclude option 4 (automated contracting practices). It avoids having to resort to option 1 (jettisoning some requirements of EAP).
7. It is consistent with the desire for federated identity management by reflecting and supporting the circle of trust architecture. At no point would anybody be outside the circle, and the contract provisions assure they are all trusted.

Con's of Snap-In Option

Some key negative elements of Option 2 include the following:

1. It requires prior disclosure of contracts by Relying Parties. This represents a step in a process that will take time and require procedures.
2. It requires creating criteria to judge acceptability. There may be more than one opinion about what criteria should be set, and some criteria could favor some CSPs or Relying Parties over others. This will take time and executive level attention of participating EAP stakeholders.
3. It requires somebody to judge acceptability of CSP contracts based upon the criteria set. This is a functional role that remains to be allocated, and will require creation of procedures.
4. It requires some due diligence by each Relying Party AFTER signing up for rules of the EAP. The Relying Parties would, presumably, need to become familiar with the terms of each contract associated with credentials it may seek to rely upon.

5. It creates some transactional drag for amendments to CSP contracts, given that amendments would presumably need to be accepted as well. However, any drag in the amendment process may not be greater than that which would happen when amending the same contract with any one of the very large Relying Parties, including the US Federal Government.

Matrix of Key Elements of Various Options

Option	Bilateral Contracts Negotiated?	New Technology?	Same Terms For All Parties?
Narrow Scope	Yes	No	No
Snap-In	No	No	No
Prescriptive Rules	No	No	Yes
Auto-eContracting (like P3P)	No (select set provisions)	Yes	No (but finite # of provisions)

The above matrix is an oversimplification for ease of comparison across the four options presented. The first column, "Bilateral Contracts Needed?" indicates whether the option meets the EAP goals and requirements that there be no need for additional negotiation and execution of a bilateral contracts between each CSP and Relying Party using an EAP solution. The second column, "New Technology"? indicates whether new technology is needed that is not yet generally commercially available and adopted by a significant market of users. A "no" in this column assumes the technology is at least as available and adopted as implementations of the Liberty Alliance or the Microsoft Passport services and specifications. The third column, "One Contract For All Parties?" indicates whether a single set of contract terms and provisions are required for all parties. A yes means that, while there may be gradations of specificity or stringency of the terms, the same provisions at each level of proscriptiveness are in place for all CSPs and Relying Parties.

Open Questions (non-comprehensive and in no special order)

1. In view of a further week of consideration, and the above deeper analysis, is it still the will of the BRP Workgroup to focus efforts around this approach.
 - a) Would it be preferable to narrow the scope (according to option 1), and simply publish a "model contract" which could be modified at will by each party, resulting in bilateral contracts by and between the parties? This was specifically suggested by one comment on option 2.
 - b) Would it be preferable to pursue more prescriptive rules, as proposed in the third option?
2. What matters would be left to the rules and how would they fit into the whole?
 - a) Would matters like intellectual property and licensing of the EAP trust mark be left to the rules? Would it make sense to include more detailed dispute resolution in the overarching rules, which would apply no matter which CSP or Relying Party presented? Would it make sense to use the rules to create a reserve fund and decision making process for the internal absorption of some EAP risks (such as the Insurance Captive or other reserve explored in Appendix 2)?
 - b) What would be the "order of precedence" between the EAP rules and the CSP contracts incorporated by reference into those rules? That is, in the event of a conflict, would the terms of the CSP contract win or would the other terms of the EAP rules control?
3. What specific matters would be the subject of certification by accredited assessors, and how would they fit with the matters left to the rules and incorporated contracts? Would there be overlap or gaps? Which matters are most efficiently and effectively allocated to each of these sources of authority?

APPENDIX 1: The Four Basic Options (excerpted)

- 1. Narrow the Scope:** A system that works for the lowest assurance level and assumes no required additional contract. In other words, indicating that higher assurance levels (where the bilateral contract requirements arise more urgently) are out of scope, are simply out of scope (dealt with later or not). Alternatively, EAP could abandon the concept that a set of rules can or should replace bilateral agreements, and instead put forth a generic accreditation scheme that assumes every party also negotiates an individual contract.
- 2. "Snap In" Non-Standard Contracts of Adhesion by CSPs:** Each Certified CSP presents for pre-approval a standard Relying Party contract as part of the Certification process (or, alternatively, after Certification, as part of opting into the EAP Rules). This contract is made available to any prospective Relying Party in advance of the Relying Party deciding whether to accept a credential. Each such agreement would in effect be a contract of adhesion ("take it or leave it" contract). It would be possible to present the materials in a standard format and possibly to negotiate through EAP certification processes somewhat more beneficial terms (aggregate pricing, public sector discounts, etc) than would be available outside of the EAP circle of trust. A variation of this method would be to incorporate by reference into the EAP Rules the terms of each pre-approved contract, avoiding the need for parties to individually accept each such contract each time it is presented.
- 3. Standard OpRules More Prescriptive At Higher Assurance Levels:** An OpRules system with tiers, where use of Credentials at higher levels of assurance correlate to ever more prescriptive provisions of Operating Rules. This method assumes the relevant decision makers and counsel for each EAP stakeholder are prepared to negotiate conclusively on behalf of their organizations final terms that will be acceptable for use in place of the bilateral contracts otherwise required by each organization. A feature of forming this tighter knit circle of trust is ability to create a reserve fund to cover certain expenses, such as costs of disputes among parties or costs of credentials use.
- 4. Automatable Electronic MicroContracts:** A system that includes "framework" provisions, selectable at time of opt in, and incorporates standard templates for the rest of legal agreements (like the P3P contracting model). Modular, in some sense, as the CSP would "snap in" its terms to the standard template, for ease of review and contracting processing. Such terms could be marked up in a dialect of XML (such as the OASIS/LegalXML emerging specification for eContracts) and Relying Parties could set authentication systems to accept certain combinations or particular terms and reject others in advance of being presented with any given credential and affiliated set of terms. This option relies upon technologies and standards that are relatively cutting edge and still emergent. As such, this method would require more discussion before being ripe for outlining and modeling and thus is not expanded below.

APPENDIX 2: Background Information

BUSINESS AND LEGAL RULES TERMS SHEET VERSION 4.0, MAY 18, 2004 For the EAP BRP Workgroup

Presented by Daniel Greenwood, Esq., Semivirtual@yahoo.com or 857-498-0962.

Abstract: This iteration of the Terms Sheet presents four possible architectures to meet the goals of the EAP consist with the consensus reached at the prior meeting. The two areas of consensus were that the BRP should develop rules and practices that are not so prescriptive they exclude important credential providers and that assume a model whereby accreditation/certification operates along with a set of legal/business rules applicable to parties using EAP credentials. The EAP goal most relevant to the BRP is to replace bilateral agreements currently required for use of third party credentials. It is envisioned that this goal can be achieved by replacing the bilateral agreements with a set of Rules applicable to parties using credentials under an EAP umbrella. The BRP Workgroup is tasked with creating the Business Rules and Practices.

Business Goals: It is useful to reiterate the basic goals of the EAP, as reflected on the EAP web site and the majority of the presentations. The stated goals are to enable interoperability between public and private authentication systems by:

1. Drafting rules for credentials and authentication systems for different and hierarchical assurance levels. These rules should provide a standard set of criteria for evaluating credentials at each assurance levels.
2. Developing a means to (a) assess credentials and systems against the standard set of criteria and (b) convey that assessment to relying parties.
3. Drafting 'rules of engagement' for relying parties that will allow them to use third party credentials. These rules would take the place of bilateral agreements.
4. Creating operating rules for validating credentials and defining how validation of credentials will be conducted.

"Rules of Engagement"

The third goal, drafting "rules of engagement" to replace bilateral agreements, presents the task most relevant to the BRP. There is no known way to achieve this goal solely by use of a Trust Mark or other generic certification and accreditation system. The key issue is that a Trust Mark (or other certification issued to a CSP upon by an accredited organization based upon generic criteria) does not address various factors generally required by relying parties and CSPs prior to allowing reliance upon a credential. If it were assumed that EAP credentials required little or no assurance by the relying party, it would be possible to develop a meaningful Trust Mark based solely upon generic, non-legal and business level factors. Such non-legal or business level certification criteria may include matters like technical specifications used, physical and network security, identity proofing at time of credentialing, etc. However, such generic certification at multiple levels of assurance, is not capable of addressing the legal and business issues currently negotiated bilaterally. These issues include liability for the underlying transaction, payment to the credential service provider, use of intellectual property (including business trademarks) of each party, indemnities, service level agreements, and several other issues. Nor is it realistic to assume a widely usable system meeting the stated goals of the EAP absent direct treatment of these types of issues.

While it is possible to achieve the goal through use of a contractual and comprehensive set of overarching rules, creation of such a system is currently deemed out of scope of the EAP. It is desirable to avoid creating a system that is so comprehensive and detailed it would exclude

existing and relevant credential service providers that would otherwise participate in an EAP-enabled system. It is also desirable to avoid developing a set of rules that is overly complex and prescriptive at the outset of the EAP before much experience with the practical and technical aspects of such an undertaking has emerged. Rather, a more tiered and phased approach was desired at the last BRP workgroup call.

Four Possible Approaches to Solve the Problem: Overview

The four possible approaches are to 1. Narrow the goals of the EAP, or 2. Create a system whereby each accredited/certified CSP and Relying Party contract are collected in advance, put into standard formats, and incorporated by reference into a single opt-in master EAP contract, or 3. Negotiate a single contractual rule set with all the key CSPs and Relying Parties in advance whereby each agrees to accept the rules in place of its own contracts and where higher levels of assurance carry much more prescriptive, detailed and comprehensive terms, or 4. Develop a large library of standard applicable contract provisions that can be presented and parsed electronically, similar to P3P privacy preferences agreed between merchants and consumers.

Four Possible Approaches to Solve the Problem: Abstracts

1. Narrow the Scope: A system that works for the lowest assurance level and assumes no required additional contract. In other words, indicating that higher assurance levels (where the bilateral contract requirements arise more urgently) are out of scope, are simply out of scope (dealt with later or not). Alternatively, EAP could abandon the concept that a set of rules can or should replace bilateral agreements, and instead put forth a generic accreditation scheme that assumes every party also negotiates an individual contract.

2. "Snap In" Non-Standard Contracts of Adhesion by CSPs: Each Certified CSP presents for pre-approval a standard Relying Party contract as part of the Certification process (or, alternatively, after Certification, as part of opting into the EAP Rules). This contract is made available to any prospective Relying Party in advance of the Relying Party deciding whether to accept a credential. Each such agreement would in effect be a contract of adhesion ("take it or leave it" contract). It would be possible to present the materials in a standard format and possibly to negotiate through EAP certification processes somewhat more beneficial terms (aggregate pricing, public sector discounts, etc) than would be available outside of the EAP circle of trust. A variation of this method would be to incorporate by reference into the EAP Rules the terms of each pre-approved contract, avoiding the need for parties to individually accept each such contract each time it is presented.

3. Standard OpRules More Prescriptive At Higher Assurance Levels: An OpRules system with tiers, where use of Credentials at higher levels of assurance correlate to ever more prescriptive provisions of Operating Rules. This method assumes the relevant decision makers and counsel for each EAP stakeholder are prepared to negotiate conclusively on behalf of their organizations final terms that will be acceptable for use in place of the bilateral contracts otherwise required by each organization. A feature of forming this tighter knit circle of trust is ability to create a reserve fund to cover certain expenses, such as costs of disputes among parties or costs of credentials use.

4. Automatable Electronic MicroContracts: A system that includes "framework" provisions, selectable at time of opt in, and incorporates standard templates for the rest of legal agreements (like the P3P contracting model). Modular, in some sense, as the CSP would "snap in" its terms to the standard template, for ease of review and contracting processing. Such terms could be marked up in a dialect of XML (such as the OASIS/LegalXML emerging specification for eContracts) and Relying Parties could set authentication systems to accept certain combinations or particular terms and reject others in advance of being presented with any given credential and affiliated set of terms. This option relies upon technologies and standards that are relatively

cutting edge and still emergent. As such, this method would require more discussion before being ripe for outlining and modeling and thus is not expanded below.

Terms Sheet Outline Tracking Each Method

The following drafts contain only the most relevant and important terms and the substance of those terms serves only as placeholder text at this time. It is presumed that legal counsel and executive management of key EAP members would review, negotiate and agree upon final language in advance of finalization. Further, it is assumed that Membership agreements other than these rules and contracts would cover liability or other obligations and rights of Members of the EAP, including duties to pay dues and disclose intellectual property rights triggered by contributions to EAP standards.

Generic Terms (Expected under any of the 4 methods).

Scope:

These Rules govern the use, acceptance and validation of identity credentials issued by an EAP Certified Credential Service Provider (CSP) instantiated in a token bearing the branding of the EAP (EAP credential). These Rules apply to each Relying Party and CSP who issue, accept and/or validate an EAP Credential.

Eligibility and Opt In Contracts:

Relying Parties and CSPs: Each Relying Party and CSP must agree to be bound by these Rules by accepting the appropriate Opt In Contract [NOTE: include link here to then current official Opt In Contract for each party]. Before becoming eligible to Opt In to these EAP Rules, a Relying Party must first be Certified by an EAP Accredited Certifier to issue EAP Credentials at one or more levels of assurance. Before becoming eligible to accept, rely upon or validate an EAP Credential, a Relying Party must first accept the Relying Party Opt In Contract.

End Users: Each CSP agrees that every end-user identified by an EAP Credential and presenting it for identity authentication to a Relying Party has accepted an EAP End User Opt In Agreement [NOTE: Include link] prior to issuing an EAP Credential. Each Relying Party agrees that every end-user identified by an EAP Credential and presenting it for identity authentication by that Relying Party has accepted an EAP End User Identity Linking Agreement before relying upon and/or linking the EAP Identity to a Relying Party identifier for that end user.

Intellectual Property

EAP Trust Mark on Tokens, Web Sites and Other Materials: [Include authorized uses and prohibited uses here, as well as infringement and licensing terms].

Method 2 (Relevant Contracts Incorporated by Reference)

Pre-Approval of EAP Party Contracts Requiring Additional Assent

Pre-Approval of Contracts: Each CSP must either

1. Warrant that no additional contract is required in order for an EAP Credential to be used, relied upon and/or validated by an EAP Relying Party, other than the EAP Opt In Agreement and these EAP Rules, or
2. Present to [either the Accredited Certifier as part of Certification or to the EAP as part of Opt In to the Rules] each applicable contract at each assurance level necessary for any EAP Relying

Party to accept, rely upon and/or validate an EAP Credential issued by that CSP for prior approval.

CSP Application for Pre-Approval of Contracts: To be accepted for pre-approval, each such contracts must meet the minimum requirements of the EAP Certification requirements and also these EAP Rules, as applicable to the level of assurance for which the EAP credential is approved. A CSP may have one or more contracts accepted and one or more other contracts rejected. In the event one or more contracts are not accepted, the CSP applying for acceptance will be delivered the reasons for rejection and an opportunity to revise the contracts and re-submit them accordingly.

Relying Party Access to Pre-Approved Contracts: Each pre-approved contract of an EAP CSP shall be available for inspection by every EAP Relying Party at any time. [NOTE: Granting each EAP Relying Party authorization to an online access-controlled repository of pre-approved contracts for browsing and review would be an easy method.]

Manifestation of Assent to Pre-Approved Contracts: At the time of Validation of an EAP Credential by a Relying Party, the applicable pre-approved contract or a link to same shall automatically be presented to the Relying Party. The Relying Party shall not be permitted to validate the EAP Credential unless it accepts the applicable agreement. [Note: These Rules could list of affirmative acts constituting acceptance, such as clicking "ok" or sending back an automated message according to a unique and specified syntax and content by the Relying Party authentication system]. The validation process must permit the Relying Party to accept the pre-approved contract for that session and reliance usage only, or for a period of time during which the EAP Credential shall be available for multiple or unlimited acceptance, reliance and validation by the Relying Party. Any terms, including transaction fees, payments per use or period of time or other formula and other applicable terms must be presented clearly in the pre-approved contract.

Amendment: A CSP may apply to amend terms of pre-approved contracts at any time and may opt to either 1. Have the existing unamended pre-approved contract remain in place while the application for amendment is being processed or 2. Terminate future use of the pre-approved contract while the application for amendment is being processes, resulting in a removal of the EAP Credential for which that contract is required form the EAP Credential system until and unless a replacement contract is approved.

INCORPORATION BY REFERENCE VARIATION OF METHOD TWO

Incorporation by Reference: Upon being accepted [alt 1: "as part of CSP Certification" or alt 2 "as part of Opting into these EAP Rules by a Certified CSP"] a pre-approved contract shall be incorporated by reference into these EAP Rules and applicable to any EAP Relying Party that accepts, relies upon and/or validates an EAP Credential to which such contract applies.

Contract Number: Each contract accepted for pre-approval shall be identified by a unique number, referenced in the EAP Rules. The token in which each EAP Credential is instantiated shall not be capable of validation without reference to the contract number. (Alt: Require that any acceptance, reliance and/or validation somehow require reference to the contract number, not solely the validation process).

Voluntary Acceptance, Contract by Contract: Reliance upon an EAP by an EAP Relying Party shall constitute acceptance of the respective pre-approved contract. No EAP Relying Party is obligated to accept, rely upon and/or validate an EAP Credential. An EAP Relying Party may choose not to rely upon an EAP Credential and thereby avoid acceptance of the section of the EAP Rules referencing that contract. Acceptance of one EAP Credential and related pre-approved contract incorporated by reference does not imply or require acceptance of any other EAP Credential or any other pre-approved contract.

METHOD 3: (Rules More Prescriptive At Higher Assurance Levels)

Note: The following terms are presented as examples only, and derive from Yahoo! and MSN Passport publicly available web-based contracts applicable to third party use of credential issued by those CSPs. For more, but only partial, detail, see <http://ecitizen.mit.edu/EAP/Yahoo-Passport/> Other potential sources of applicable terms can be found at <http://ecitizen.mit.edu/EAP/RulesExamples/> (compilation of publicly accessible web-based Operating Rules). It is envisioned that this approach would contain several tiers, each becoming more detailed and comprehensive to address respectively higher levels of assurance by Relying Parties. The current Federal levels of assurance are: Level 1: Little or no confidence in the asserted identity's validity, Level 2: Some confidence in the asserted identity's validity, Level 3: High confidence in the asserted identity's validity, and Level 4: Very high confidence in the asserted identity's validity.]

Support

Lower Level "The EAP CSP will make reasonable efforts to maintain a support service for EAP Relying Parties for the purpose of receiving inquiries, complaints or urgent requests involving use or validation of an EAP Credential issued by that CSP. The EAP CSP reserves the right to establish limitations on the extent of any support provided for the Credential Service, and the hours at which it is available."

Higher Level "The EAP CSP will maintain a 24/7 call center for use by any EAP Relying Party in relation to the use of validation of EAP Credentials issued by that CSP. The CSP call center shall publish its escalation policy for review by any EAP Relying Party, detailing how complaints or urgent requests are taken in, assigned priority, and the conditions under which they are escalated to an executive decision maker within the CSP. The CSP call center shall be accessible by telephone and also by e-mail, and shall specify response times for each newly ticketed request for service no less than 2 hours from the time of intake."

Payment

Lowest Level: [Alt 1. No Fee] "There shall be no fee to Relying Parties for use of, reliance upon or validation of an EAP Credential that have been certified at Level One, the lowest level of assurance. Nothing in this section prohibits the Relying Party and CSP from agreeing upon the terms of other value-added services or products available from the CSP which may entail a fee. [Alt 2. Nominal Fee] "For each EAP Credential an EAP Relying Party accepts, relies upon and/or validates, the Relying Party shall pay a one time fee of \$X to the issuing CSP].

Higher Levels [Alt 1. Based upon Passport] There are two fees for licensing EAP Credential usage: a periodic compliance testing fee of US\$1,500 per URL where the Credential will be re-used by an EAP Relying Party and a yearly provisioning fee of US\$10,000 per EAP Relying Party. The provisioning fee is charged on a per-Relying Party basis and can be applied to multiple URLs. For example, if your company relies upon EAP Credentials on three distinct URLs, you would pay one yearly fee plus the periodic compliance testing fee for each of the three URLs. This entitles your company to unlimited volume use of the EAP Credential service at those URLs."

[Alt 2. Based upon idea of an "Insurance Captive" for authentication developed by MIT's E-Commerce Architecture Program, at <http://actuarinet.mit.edu>]. "Each Relying Party shall pay \$X USD into the Service and Risk Pool of the EAP annually in return for use of, reliance upon and validate of EAP Credentials. From that fund, a reserve account to mitigate or absorb the risk of loss events involving the EAP of no less than \$\$ (dollar amount, percentage or other formula) shall be maintained, and the remainder shall be distributed on a quarterly basis to every EAP CSP up to \$\$ (amount, pro-rata based on validations of credentials, or other formula), and any

excess amounts resulting in a proportional decrease of the fee paid in the subsequent year. " [NOTE: A variation on this alternative could include all parties, CSPs, and Relying Parties, and potentially others, all paying into the risk pool. Another variation could have this pool used only to absorb loss events and not also as a payment mechanism for CSPs. A final variation could have the CSPs be the only party paying into the pool and presumably passing the costs back to the end-users.]

Privacy Policy:

[Alt 1. Based upon Yahoo! Merchant Agreement] You agree (a) to post a privacy policy in Your site that, at a minimum, discloses any and all uses of personal information that You collect from users; (b) to include in Your privacy policy a paragraph provided or approved by the CSP that describes the CSPs collection and use of Credentialed User's information, (c) to provide a hypertext link to Your privacy policy on the home page of Your referring and on all pages where You collect personal information from users, including but not limited to all check out pages; and (d) to use personal information only as expressly permitted by Your privacy policy.

[Alt 2. Based upon MSN Passport, As paraphrased in Passport Review Guide]

The information stored in a EAP Credential account is not shared with EAP participating sites or services unless the user explicitly chooses to provide it by clicking the EAP sign in button.

By clicking on the sign in logo at your site or service, the user consents to have his or her selected EAP Credential profile information delivered to you. With the user's consent, within the guidelines of your own privacy statement, consistent with the Opt In agreement signed between EAP and your organization, and consistent with any privacy coalition program in which you participate (e.g. TRUSTe or BBBonline), you can then store and use the information you receive from the user's EAP Credential profile in exactly the same way you could have used this information if you had collected the information yourself. You can also use the EAPUID as the unique key identifier for the EAP Credentialed user inside your own database.

However, by signing the EAP Opt In contract you agree to some specific restrictions in your use of EAP Credential data. These include:

- You can use EAP profile information only to deliver the products and services requested by users.
- You cannot use EAP profile information to contact users for any purpose without obtaining the users' prior consent.
- You cannot assign, transfer, share, transmit, or publicly disclose EAP profile information—or any identifiable information gathered from Passport profile information—to any third party without the user's consent.
 - The only exception to this last requirement is when you need to transmit EAP Credential information to third parties in order to deliver goods and services requested by the Passport user (for example, if the participating site sends some of its business, such as shipping services, to an outside provider). In this case:
 - If the third party is another EAP participating site, you may transmit the EAPUID.
 - If the third party is not a participating organization, you may transmit profile data to third parties, with the following restrictions:
 - The data may only be sent for the purpose of allowing such third parties to participate in the delivery or fulfillment of a product or service requested by the user.

- Only the amount of profile data that is reasonably necessary for such third parties to receive in order to deliver the product or service requested by the user may be sent.
- Each third party that receives such data from you must have agreed in advance of receiving such information to:
 - Use such data only for the purpose of delivering the product or service requested by the user; and
 - Respect terms no less restrictive than these listed here.
- You agree to post privacy policies on your site and adhere to legal privacy requirements and industry standards. EAP also now calls for you to comply with the Platform for Privacy Preferences Project ("P3P") specifications set by the World Wide Web Consortium ("W3C"). This means that you expose your privacy statement in the form of an XML document that conforms to the W3C-P3P specifications. You also post a compact statement describing their use of cookies in the form of a mini-header that conforms to the W3C-P3P specifications.
- These documents and headers, in conjunction with the new Internet Explorer 6 support of P3P specifications, enable users to more easily understand a site's privacy statement and cookie usage. They also make it easier for users to define their default preferences for managing cookies.

Dispute Resolution

[Note: The following examples come from sources other than Yahoo! and MSN Passport]

Low Level of Assurance: [Derived from the MultiState Email Operating Rules, available at: <http://ecitizen.mit.edu/EAP/RulesExamples/EMAIL/oprules-v2.htm>] Disputes between a CSP and a Relying Party regarding use of, reliance upon or validation of an EAP Credential, shall be governed according to the terms and conditions contained within the underlying contract governing the transactions or other interactions engaged in by those parties for which EAP Credentials were used to authenticate one of the parties. Disputes arising out of or related to the application of these Operating Rules and related Opt In Agreements shall be resolved in accordance with the provisions of these Operating Rules and related agreements, and by agreement between the parties, where possible, through direct negotiation or, if appropriate, through voluntary mediation by a mutually agreed upon Mediator. In the event that parties are unable to reach agreement directly or through the use of mediation or other voluntary methods of Alternative Dispute Resolution, then, to the extent permitted by law and relevant regulation, all such disputes shall be subject to binding arbitration by a a mutually agreed upon arbitrator of the American Arbitration Association. The costs of any form of Alternative Dispute Resolution shall be paid equally by the disputants or as otherwise agreed by the parties."

Higher Level of Assurance:

[Alt 1. Detailed EBT Model] See Chapter 8 of the QUEST Operating Rules governing use of the Electronic Benefits Transfer Council, available on the web or at:
http://ecitizen.mit.edu/EAP/RulesExamples/QUEST/1.4_May_2002.pdf

[Alt 2. Risk Pool Approach proposed by MIT E-Commerce Architecture Program, at <http://actuarinet.mit.edu>] [Note, this approach works with Payment provision Alt 2 for the higher level of assurance, and is broadly consistent with the practices of Insurance Captives which self-insure across enterprises in a similar risk pool and also with the Visa approach to reserve funds for internal allocation to cover certain limited disputed costs or other losses among parties to that system.]

Disputes involving liability for money damages between EAP CSPs and EAP Relying Parties shall, in the first instance, be referred to the EAP Executive Council [by whatever name it is called] for non-binding determination [query - shall we give end-users of EAP Credentials standing to raise disputes as well?]

. The Executive Council may opt to apply informal investigative inquiries, formal mediation or formal arbitration or any other method it deems appropriate to develop a proposed resolution to the dispute. The Executive Council is authorized to propose any settlement terms, consistent with these EAP Rules and Opt In Agreements, and may include an offer to one or more disputants of direct monetary compensation to be disbursed from the EAP Reserve Pool up to [include limits here, based on hard ceiling, percentage or other formula].

All parties agree to refer disputes not capable of voluntary resolution by the parties through negotiation or mediation to an Arbitrator for binding decision. The judgment of the arbitrator may be entered by any court having jurisdiction. [See the EBT Model above for further detail on potential additional arbitration provisions]. The arbitrator may hold one or more parties jointly and severally liable for damages arising out of or related to any dispute presented. To the extent no party is deemed liable, the arbitrator may allocate monies from the Reserve Pool of the EAP up to [\$\$ amount, percentage or other formula] and may hold one or more parties to the dispute liable for the remaining damages, if any.

The Executive Council shall refer all disputes, including the final settlement arrangements, to a Risk Management Committee [by whatever name it goes in the final documents] to analyze and report back to the EAP recommendations to avoid, mitigate, transfer or otherwise address the cause of the dispute. These recommendations may include changes to these Rules or Opt In Contracts, changes to the practices governing contributions to and disbursement from the EAP Reserve Pool.

APPENDIX 2, Continued

BUSINESS AND LEGAL RULES IN TERMS SHEET: ALTERNATIVES FOR THE BRP WORK GROUP

Draft, May 11, 2004, by Daniel Greenwood, Esq., Semivirtual@yahoo.com or 857-498-0962.

Abstract: The following 2 paragraphs and 3 sets of alternatives frame the issues presented in this week's iteration of the "terms sheet" (business/legal rules for EAP): A. Do the rules cover underlying transaction risk, if not how is it handled, B. Is the system "open" or "closed", C. What is relation between Accreditation and these Rules? This memo and the Terms Sheet draft present closed, open a hybrid alternatives.

In federated "circles of trust" systems, Relying Parties and credential providers are all bound to each other under a contractual scheme defining rights, obligations, liability and other relevant terms. The EAP and federal use cases all assume a federated system in which credentials issued for one purpose (such as to a customer or employee) will be available for federal re-use for other transactions with potentially very different legal and business implications. Legal issues include liability for underlying transactions (as distinct from liability for mis-identification), use of intellectual property (such as trademarks or service marks of Credential Service Providers (CSPs) or Relying Parties). Business issues potentially include payment or other value from the Relying Party to the CSP in return for right to use credential and share customer and whether a CSP has the ability to limit which Relying Parties may use its issued credentials (e.g. whether it may prevent competitors from sharing customers or may define service level expectations, etc). These types of issues would be resolved and recorded through the process of contracting between the CSP and Relying Party when they created or joined a federation.

It has been stated that, ideally, EAP can result in a system whereby a large Relying Party, such as the U.S. Federal Government, need not negotiate a completely new contract for each CSP. To architect such a system, many business and legal issues would have to be addressed by the EAP contribution (either through the Accreditation process, through new sets of contractual business and legal rules applicable to all parties issuing or using EAP credentials, or otherwise). It is possible to imagine an EAP system whereby a very reduced number of large Relying Party contracts are necessary, perhaps in the order of the number of credit card industry contracts or mobile phone service provider contracts such parties now execute. Finally, it is possible that a large Relying Party could use an EAP Accreditation and Business/Legal Rule set as a type of "procurement schedule", whereby any CSP who is on an EAP list has proven reliable and stable enough to warrant a short standard agreement, such as a quoted price for a "scope of work", without the need for a full RFP, bid process and soup to nuts negotiation of all business and legal terms.

Revision of the Business/Legal Terms Sheet of the BRP requires further clarity on the following topics:

1. Scope of Business Rules:

Alternative A: Credit Card/ATM Model

The business rules and processes of the EAP follow the credit card industry model of a contractual multi-lateral rule set, defining all the relevant business and legal matters of the parties. Example: a "Visa" and "Cirrus" brands on a credit/ATM card reflect membership in a global, interoperable, membership system of issuers and relying parties (and others) who entered into contracts defining how each pays for services from the others, liability for underlying transactions, and other business and legal terms tailored to the transactions).

Alternative B: Trust Mark Model

The business rules and processes of the EAP follow the trust mark model of an accredited set of practices by the CSP, and assume each CSP and Relying Party will also need to negotiate a contract defining the relevant business and legal terms enabling transactions with credential holders. Example: A privacy seal or BBB seal, while conveying information relevant to "trust" decision, are not sufficient without other contracts or business context to support even small amounts of reliance).

2. Applicability of "Federation" and "Circle of Trust" Concepts to EAP

Alternative A: Closed Communities

EAP is a closed, membership based contractual circle of trust. The word "circle" in circle of trust means there is a boundary condition, and only parties who are "inside" the circle may participate. The word "trust" in "circle of trust" means the relevant enforceable terms structuring the business and legal relationships of all the parties inside the circle are sufficient to manage risk and assure predictable outcomes for disputes regarding the substantive transactions between parties. Federations are circles of trust almost always bounded by specific contracts (bi-lateral or multi-lateral) covering membership and delineating risk allocation for the underlying activities in the circle.

Alternative B: Open-PKI Model (Applied Technology Neutrally to Any Authentication Method)

EAP follows an Open-PKI Model, assuming an EAP credential would be like a Passport, used by potentially any relying party who chooses to trust the issuer, and can be used for virtually any purpose, with no permission or agreement from the issuer. There would be some standards that relate primarily to information field syntax, interoperability and naming conventions, but no limit on participation by any Relying Party (i.e.: no "circle") and would leave to other contracts, laws or agreements the determination of business and legal issues of the parties related to their underlying transactions and other activities.

Alternative C: Shortcut to Formation of Closed Communities, Built Upon EAP Foundation

EAP provides pre-vetting of various large and generally reliable (i.e.: deep pockets, sophisticated infrastructure, institutional commitment, etc) CSPs, and reduces the need for additional due diligence or contracting by prospective Relying Parties. The process of CSP/Relying Party match-making could be facilitated by EAP establishing such matters as the pool of Credential Holders (e.g. all AOL account holders, all Fleet account holders, all Sprint account holders, etc), the level of Assurance of the credential, the type and amount of insurance, and one or more standard contracts the CSP will accept from any potential Relying Party. Such "standard contracts" may require CSP giving a price, service quality and/or delay quote in response to a service request, and may permit the CSP to refuse to grant service under some circumstances. Depending upon the specific transactions sought, in some cases, Relying Parties and CSPs may choose to negotiate more precise or far reaching terms (such as co-branding details, joint advertising of the federated relationship, revenue-sharing, opening new lines of business, etc).

3. Relationship Between Accreditation of a CSP and the Business Rules and Processes

Alternative A: Accreditation is Eligibility for Becoming a Party to EAP Business/Legal Rules

Accreditation follows the model of certifying that a given party has proven eligible for membership in a closed EAP federation, or federation of federations (such as in alternative 2.B.) Example: Before certain large insurance companies will write a policy for particular types of so-called "cyber insurance" (e.g. covering lost business resulting from problems with web or other Internet usage), the applicant must pay for and undergo a detailed audit and information security review. A satisfactory certification that relevant practices, technology and agreements are in place must be achieved for eligibility to sign an insurance contract, opting into the contractual risk sharing community (and setting the premiums for that applicant).

Alternative B: Business Rules are a Factor Considered in Accreditation

Accreditation is the final step and conveys that the accredited party is certified to have in place business rules and practices that are generically sound. Example: A Certification Authority has a Certification Practice Statement and other agreements and policies and practices that are accredited to meet certain generic standards. This case assumes approaches like those in 1.B. and 2.B.

Alternative C: Business Rules and Accreditation Supplement Each Other

Accreditation address certain technical aspects of Credential issuance and maintenance, relevant to Relying Parties (such as the practices necessary to establish identity proofing measures, token strength and security of token delivery) while Business/Legal Rules of EAP address other aspects relevant to both Credential Providers and Relying Parties wishing to "do business". In this case, the Business/Legal rules could address the same types of matters contained in contracts underlying approaches in 1.A, 2.A and 3.A. However, the Accreditation could be relied upon in an open system whether or not the Relying Parties were

signatories to the Business/Legal Rules. However, applying some or all of the EAP rules, in this "supplementary" scenario, could shortcut or eliminate the negotiation and contracting steps otherwise probably necessary between Credential Providers and Relying Parties.

Terms Sheet Draft 3.0

Terms Sheet Draft 3.0 May 11, 2004

1. Title of Document, Definitions and Scope.

[NOTE: A basic scope question is: Are EAP these rules and accreditation the only business and legal connection between a Credential Provider and a Relying Party such as the US Federal Government? If so, then it remains to be determined how underlying risk and liability for the transactions and information transmitted will be addressed. Other possibilities include:

- * EAP Rules and Accreditation for Generic Identity Issues PLUS Contracts for Specific Business Issues. Example: The credit card model, where the federal government maintains a small number of independently negotiated contracts giving access to each major industry service provider with somewhat different legal terms, payment rates, etc, and a general set of policies applying to all credit card processing transactions government-wide.
- * EAP Rules and Accreditation Address Both Generic Industry/Party Neutral Issues and Business/Risk Issues Arising from Underlying Transactions. Example: The Electronic Benefit Transfer Council Operating Rules and Opt-In Contracts.
- * EAP Rules and Accreditation Address Generic Identity Issues, PLUS Modular Sections of Rules for Approved Pre-Existing Agreements by Participating Federated Identity Communities. This possibility could track alternatives 2.C and 3.C in the May 11, 2004 document "Business and Legal Rules in Terms Sheet: Some Alternatives for BRP Work Group".]

2. Roles and Functions

[NOTE: The following roles have been derived from EAP documents and meeting notes.]

2.1 Credential Service Provider

[NOTE: In order to operate under these rules, must a CSP be accredited first? If a CSP is accredited, must it also be recognized under the rules, or will/should it be necessary for the CSP to: 1. Sign an Opt-In Contract agreeing to the Rules, and/or 2. Become a Dues Paying Member of the EAP, and/or 3. Have Any Another Contract in Place With Relying Parties Addressing Industry-Specific, Transaction-Specific or Party-Specific Liability or Business Issues, and/or Other Requirements?]

2.2 Credential Holder (AKA User, Customer, Employee, Citizen)

[NOTE: This section would address: Minimum requirements for opt-in language, privacy disclosures, other rights or responsibilities such as maintaining security or getting/sending notices?]

2.3 Relying Parties

[NOTE: There remains a question as to whether the same rules and processes can and should apply to federal government external relying parties (the "C2G" scenario of the BRP WG) as will apply to private businesses. If the same rules are to apply, then all relying parties may be capable of treatment under one section.]

2.3.1 United States Government

2.3.2 Relying Party, Private Business

2.3.3 Relying Party, Other Credentialed Users

2.4 EAP Executive Committee

[NOTE: If there is to be an EAP decision making executive with authority over the rights and duties of other parties assuming roles within an EAP system, it would be consistent to identify that EAP executive in this section. The scope of authority over other parties should be identified here.]

[NOTE: There may be other roles, such as Accrediting Party, Auditor, Other Relying Parties, etc. The number and division of roles remains to be discussed by the BRP.]

3. EAP Membership

[NOTE: It remains to be determined whether EAP shall refer to CSPs and Relying Parties as "Members" or if the term Member shall only apply to a small set of representative parties playing a governance role and paying dues to have say over EAP rules. If the former, then this would be an appropriate section to deal with how a party becomes a member, how they are expelled, etc. If the latter, then this section can be left to the governance document or charter.]

3.1 Membership Eligibility, Rights and Duties of Members

3.2 Expulsion of Members

4. Dispute Resolution

[NOTE: KEY QUESTION: Shall dispute resolution - and the scope of EAP rules in general - deal with underlying transaction risk or simply deal with the narrow area of identity accuracy risk? See Liability note in section 5 of this document for further detail on option.]

4.1 Problem Reporting and Handling

4.2 Internal Problem Resolution

[NOTE: It may be appropriate to include role of EAP Executive arm in addressing determining interpretation of rules where Members or other contractual parties disagree, perhaps A. carving out a series of rules in the domain of the Executive to apply and other rules left to dispute resolution, or B. allowing the Executive to attempt to settle the disagreement on a voluntary internal basis, but allowing any unsatisfied party to seek resource externally through ADR.]

4.3 External Alternative Dispute Resolution

4.3.1 Mediation

[Note: It may be advisable to require or promote non-binding mediation by a neutral third party to attempt to resolve disputes among EAP system parties amicably before escalating to arbitration]

4.3.2 Arbitration

[NOTE: Issues include: how arbitrator is chosen, discovery and other process issues, whether there is a scope (monetary or otherwise) constraining possible awards, the binding nature of the arbitration, and the extent to which information from judgments and proceedings may factor into risk management or other evolution of EAP processes.

5. Liability

[Note: Key Question is how underlying transactional liability will be addressed by parties using EAP offerings. If such liability is not to be addressed by EAP, then it may be necessary for parties using EAP offerings to also negotiate and execute a bi-lateral or additional multi-lateral contract for every other party or circle of trust within the EAP. *Example: Company A (an online travel service) authenticates an individual via the Liberty spec. The individual proceeds to move to Company B (an online stock trading service) and explicitly links the accounts (federated SSO) via the Liberty spec. Said individual then attempts to sell a stock holding that is *dropping rapidly. For some reason, the authentication that Co A performed causes a glitch in Co B's systems -- and the individual is not logged in on a timely basis, and thus not able to execute the sale of their rapidly dropping stock. Who's at fault? Where are the lines of liability drawn?* [Attribution: <http://discuss.andredurand.com/newsItems>]

Whether liability disclaimers would apply solely to EAP as a legal entity, or would extend to structure liability allocation between parties, such as a CSP and Relying Party, is a key scoping issue.]

5.1. Liability Disclaimers

Types of damages to address (either by disclaiming them, allocating the risk, or shifting the risk to other parties through insurance, bonding, contracts or otherwise) include: direct, indirect, incidental, special, consequential, punitive or exemplary damages, including damages from loss of profits, revenue, good will, data, electronic orders or other economic advantage. Theories of liability to be disclaimed or otherwise addressed include contract breach, tort (including privacy breaches, trespass to chattels and negligence), and intellectual property infringement.

5.2 Liability for Inadequate Backup or Equipment

Liability for inadequate backup of data or sub-standard equipment or maintenance of equipment (including installing updates, patches or other upgrades) can be addressed separately.

5.3 Hold Harmless and Indemnity

Agreement to hold harmless, not to sue an EAP party, or the requirement to indemnify an EAP party may be addressed as part of liability. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so any such limitations would need to be tailored accordingly.

6. Authorized Use of Services

This section may set boundary condition around use of services of a CSP, Relying Party, EAP or other party to these Rules. For example, if a given CSP did not wish a direct competitor to share its customers, such a restriction could be noted here. Similarly, if it were necessary to receive a quote from a CSP defining price, quality and/or timeliness of service, such requirement and process may be noted here. A clause of this nature could be generic, applying to any EAP party, or could be partially or totally modular, allowing parties to select from among standard approved clauses reflecting how they already do business. This last approach mirrors the alternatives presented in 2.C and 3.C of the May 11, 2004 document "Business and Legal Rules in Terms Sheet: Some Alternatives for BRP Work Group".

7. Intellectual Property and Branding

Mandatory, permitted and prohibited use of the EAP or other relevant branding would be dealt with here. Licensing of the EAP marks or logos, as well as copyrights, business process patents or other trademark use would be detailed in this section. If these rules extend to underlying business factors, IP between EAP parties may also be addressed here. EXAMPLE: If a bank were to originate an authenticated user session between the bank's customer and a federal agency application from the bank's web site, then the details of framing and any bank branding affecting the federal agency web site may be dealt with here.

8. Amendments to the Terms

How these Rules are amended, by whom, with what notice and other relevant factors related to changing the terms would be addressed here.

Accreditation, Certification and Assessment Models

Prepared by Daniel Greenwood, Esq.

Delivered to the EAP EAC Workgroup on June 9, 2004

I. Introduction

This document represents the results of research and evaluation of several accreditation, certification and/or assessment models that provide relevant options for the EAP. This document is in response the Task Order and subsequent refining discussions with and by the EAP EAC Workgroup. The original Task Order is contained in Addenda 1. Addenda 2 includes all previous memos and case studies, to complete the record of original research.

II. Business Goals:

It is useful to reiterate the basic goals of the EAP, as reflected on the EAP web site and the majority of the presentations. The stated goals are to enable interoperability between public and private authentication systems by:

1. Drafting rules for credentials and authentication systems for different and hierarchical assurance levels. These rules should provide a standard set of criteria for evaluating credentials at each assurance levels.
2. Developing a means to (a) assess credentials and systems against the standard set of criteria and (b) convey that assessment to relying parties.
3. Drafting 'rules of engagement' for relying parties that will allow them to use third party credentials. These rules would take the place of bilateral agreements.
4. Creating operating rules for validating credentials and defining how validation of credentials will be conducted.

III. Five Models

1. National/International Accreditation/Testing Regimes

This contains the most detailed and evolved documentation, business models and system of cross-border recognition of all the options investigated to date. While many of the national organizations are governmental or quasi governmental, examples selected for this analysis are all private non-profits (hence, the German DAR has been replaced in this draft by the United Kingdom, and other relevant organizations have been added).

More information on the potential applicability and relevance of this model appears as attachment 1 of addenda 2.

2. Higher Education Accreditation (US Market)

This model was discussed in some detail at the last meeting. In the interests of time, a deeper written description will be deferred until the submission for the next draft so that the other models may be fully explored.

- CHEA (Recognizes organization that grant accreditation to institutions of higher learning)
- DETC (Grants accreditation to particular institutions of higher learning)

See attachment 3 of addenda 2 for more details.

3. Public/Private Accreditation by Economic Sector (US Market)

This model is also highly evolved, and involved close coordination between governmental regulators and non-governmental accreditation. Given the quasi-governmental nature of this model and the nature of the long standing institutions to which it applies, it is not a clear fit for the EAP business case. However, various elements of the model are relevant and re-usable, as can be seen in the analysis of each in the last draft (attached).

- Banking (Chartering, Self-Assessment, Audit and Examination)(see:)
- Healthcare (Government licensing or permitting with private accreditation, e.g.: JCAHO)

See attachment 3 of addenda 2 for more details.

4. Internet Trust Marks

This model, relying heavily upon self-assessment and later verification on an as-needed basis by the licensor of the mark, has clear application to the EAP business case.

- TRUSTe
- ICRA

The basics of these models can be found in attachment 2 of addenda 2.

5. Circles of Trust

This model provides options that are most relevant to the "rules of engagement" and "closed community" aspects of the EAP endeavor. The examples in these models do not pertain especially to accreditation as generically understood, but all contain some criteria for admission that can be seen as comparable to certification. In addition, each model contains specific technical interoperability requirements and continued monitoring.

- NACHA/EBT
- SWIFT

The SWIFT Model can be found in the appendix to attachment 3 of addenda 2. The EBT model is under final drafting and will be appended shortly. The key document of the EBT model is the Operating Rules, which can be found at: <http://ecitizen.mit.edu/EAP/RulesExamples/QUEST> (along with other key documents). In short, the QUEST operating rules have legal force and effect based on contractual opt-in agreements by the parties using and servicing the EBT system. The liability for underlying transactions is spelled out in detail, as are the dispute resolution process and other legal terms. The parties are all represented on a governance board which is responsible for devising and revising the Operating Rules and related contracts and policies. Visa is another oft cited example of the closed system circle of trust. Another example is SecuritiesHub, (owned by Citigroup, Credit Suisse First Boston, Goldman Sachs, JPMorgan Chase & Co., Lehman Brothers, Merrill Lynch, Morgan Stanley, UBS Warburg, and Communicator Inc), and discussed in the White Paper "Online Gated Communities", available at: <http://ecitizen.mit.edu/OnlineGatedCommunities/>.

IV. Key Options Relevant to Each Model

1. Liability of the EAP. It appears to be common practice for an accreditor to disclaim all liability from those whom it accredits, as well as others certified by the accredited organizations or from end users of the certified products or services. There are some counter-examples of accreditation organizations that accept limited liability, such as the United Kingdom Accreditation Service (UKAS), such as for death or personal injury caused by UKAS' negligence.

2. Accreditation Criteria. It appears to be common practice for an accreditor to either refer to widely accepted international standards (such as ISO standards) and/or to develop criteria internally. Internally drafted criteria, such as the self-assessment survey by TRUSTe, are frequently revised in consultation with stakeholders. In closed system circles of trust, it is common for stakeholders to have a direct representation and vote on the operating rules which define the terms of the system, what parties may participate, liability and other terms. QUEST rules for EBT, the Operating Regulations of Visa, the governance and contractual documents enabling Securities.HUB, and the SWIFT rules are examples.
3. Dispute Resolution. It is common for dispute resolution to be handled by a senior executive committee of the accreditation organization (e.g. a committee of the Board of Directors). An appeals process is frequently spelled out, including the types of decisions that are appealable and the time frame within which a request must be lodged, argued and decided. In closed models, such as the EBT system, it is typical to see clauses requiring binding third party arbitration of commercial disputes.
4. Continuing Obligations. It is nearly universal that accreditation organizations require a) that the accredited organization warrant it shall remain in compliance for the period that it has been accredited, b) that the accreditor be advised of any material change in the status of the accredited organization, c) that the accredited organization consent to planned or surprise site visits, d) that self-assessments (less typically third party audits) be continually performed and submitted to the accreditor or available for inspection by the accreditor during the re-accreditation cycle, and/or that complaints by third parties (including end users) be sent to (directly or indirectly) the accreditor and that such complaints may form the basis of information leading to further assessment.
5. Consequences for Failure to Meet Obligations. The most typical explicit remedy for failure to remain in compliance with the accreditation criteria after accreditation has been granted is some combination of suspension, revocation or other modification (such as narrowing the scope of products or services to which accreditation applies) of the accreditation. In some cases, the accreditor may explicitly also reserve the right to notify third party regulators or law enforcement authorities, if, for example, the non-compliance threatens health or safety. There is also precedent for making general public announcements (e.g. on web site, perhaps via a press release, etc) of de-accreditation (see the ICSA blurb on "Validity Period" in attachment 3 of addenda 2).
6. Assessors. There is precedent for requiring self-assessment by the applicant for accreditation, against which in-house staff by the accreditor evaluate the applicant (such as TRUSTe and ICRA). There is also precedent for requiring direct site inspection by agents of the accreditor (Higher Education, UKAS, etc). And there is precedent for out-sourced sub-contracting of third party labs and assessors to evaluate an applicant for accreditation (such as with the UL family of labs and assessors).
7. Best Practices. Finally, the practice of posting all application materials, forms, complaint processes, and criteria on the web appears to be a best practice. The UKAS has also availed itself of a government MOU by which it holds a special legitimacy by declaration of government intent, though the MOU holds no legally binding weight. Having the accredited party pay all costs, as well as fees for accreditation is also a best practice. And, finally, it appears to be a best practice to use the application process as the key moment at which the applicant agrees contractually to all terms and conditions and related rules, incorporated by reference, to the application agreement.

V. Relevant Issues Raised by Each Model

The basic issues raised and addressed by each model group as follows:

1. Does the model apply to an organization that recognizes other organizations that will do the assessment and certification, or does the model apply directly to the process of assessment and certification?
2. What is the process of assessment? Is it conducted by: a) Self-Assessment, b) Third Party Audit (e.g. CPA), c) Assessors of the Accreditor, and/or d) Government examiners? Specifically, are there site-visits or not? What training is required of the assessors?
3. What are the criteria against which the product, service or organization is assessed, and where do they come from? For example, are they international standards (like ISO 9000), national standards (like the CHEA requirements for US accreditation of institutions of higher education), or unique requirements developed by the certification organization (like the TRUSTe Self-Assessment criteria)?
4. What is the role of continuing assessment and monitoring? Are periodic and/or surprise inspections part of the process? How deep and broad are the continuing assessment obligations and what is the cost of compliance? Are third parties (such as customers of the certified company) provided a means to communicate complaints to the accreditor?
5. What are the penalties for non-compliance? Under what circumstances is the certified party given an opportunity to cure the problem? Are there appeals or due process protections? Who decides appeals? What is the liability between the parties for serious harms that could result from mistaken granting or failure to grant certification, or misuse of certification?
6. What other business and legal rules apply to the certified companies or other parties and how are they supposed to be enforceable? Does the application process include a declaration or other acceptance of other rules? Are the rules incorporated by reference? To what extent do the rules specify rules applicable to third parties interacting with the certified company (such as students of the recognized college, consumers of the certified firewall, customers of the testing lab, and so on)? Is the certified company legally obligated to pass forward certain obligations or rights to its customers as part of the certification?

ADDENDA 1: Original Request for Service

Research and provide six (6) examples of existing Certification and Accreditation schema's that the EAP can utilize in determining the best model/approach for their own customization and adoption. The schema's can be from any vertical market and do not have to be specific to the identity management functional area.

Detailed information should be provided for each of the six sample schema. At a minimum, the following functional areas should be fully described in each of the schema:

- * Functional Approach
 - o Is the schema model based on an internal or third party certification process?
 - * Example 1: Model owner directly conducts all certification/accreditation of identity issuers and relying parties
 - * Example 2: Model owner accredits a third party auditor to conduct assessments on their behalf, but maintains the process to provide final certification/accreditation of the identity issuers and relying parties
 - * Example 3: Any other model that are available to assess
 - o Define the decision making processes each model owner utilizes to develop and deploy their model
 - o Define the control/management processes each model owner utilizes to support their deployed model
 - o Define the liability framework associated with each named participant within the model, specifically as it applies to the certification and accreditation process
 - o Define the flow of money within the model, as it specifically applies to the certification and accreditation process (third party provider fees paid to the model owner for initial accreditation, third party continuing services/maintenance fees paid to the owner, identity issuer/relying party assessment fees paid to the third party auditor, identity issuer/relying party certification/accreditation fees paid to the owner)
 - o Define the dispute resolution process within the model, as it specifically applies to all named participants, within the certification and accreditation process
 - o Define the length of time that a third party auditor accreditation and/or identity issuer/relying party assessment and/or certification/accreditation would be valid for

The goal of this task is simply to collect six samples of differing certification and accreditation models that can be assessed from a functional, legal, business, technical, operational and maintenance/support perspective. EAP would like to review each of these six candidates and determine if one or more meet their perceived needs, customize as necessary and adopt for implementation.

/end/

ADDENDA B: Attachment of Previous Memos and Case Studies

ATTACHMENT 1:

Overview and Relevant Aspects of Internationally Recognized National Accreditation Models

The system seeks to enhance quality and cross-border recognition of accreditation and certification through the use of international standardization. In general, international bodies recognize national bodies which accredit organization that certify products or services. For example, the Underwriters Laboratory is accredited by the American National Standards Institute which is the United States member of the International Standards Organization (as well as of the Interamerican Accreditation Cooperation organization and the International Accreditation Forum). Similarly, English product certification organizations are accredited by the United Kingdom Accreditation Service (UKAS), which is also a member of the ISO and IAF. Though the name is somewhat confusing, given that it is primarily a US organization accrediting US companies, the International Accreditation Services organization (IAS) is itself a member of the Interamerican Accreditation Cooperation (IAAC) which is recognized by the IAF.

Here is an example of the food-chain:

A. International Accreditation Organizations

- International Accreditation Forum (IAF) (<http://www.iaf.nu/>)
- International Standards Organization (ISO) (<http://www.iso.org>)
- Interamerican Accreditation Cooperation (IAAC) (<http://iaac-accreditation.org/>)

B. National Accreditation Organizations (recognized internationally)

- American National Standards Institute (ANSI) (<http://www.ansi.org>)
- United Kingdom Accreditation Service (UKAS) (<http://www.ukas.com/>)
- International Accreditation Services (IAS) (primarily US) (<http://www.iasonline.org/>)

C. Examples of Companies Conducting Certifications (Granting Certification to Products/Services)

- UL
- ICSA

Applicability

The reference to internationally and nationally recognized standards, as well as the basic application and accreditation procedures followed by the following two organizations appear largely applicable to the EAP base case. However, for purposes of the EAP, it would appear beneficial to substantially simplify and reduce the complexity and size of the endeavor and standards. In addition, the addition of EAP Business Rules in addition to accreditation and certification procedures would require a somewhat different business architecture. Nonetheless, the following processes and substantive rules are among the highest relevance of any examined during this research task. .

Example I

International Accreditation Service of Whittier, California

Scope Predominantly United States

<http://www.iasonline.org/>

IAS, formerly part of ICBO Evaluation Service, Inc, has been in operation since 1975. IAS operates as a nonprofit public benefit corporation that assesses and accredits competent testing and calibration laboratories, inspection agencies and fabricator inspection programs.

Basic Information:

Application Information for Companies Seeking Accreditation:
<http://www.iasonline.org/PDF/Forms/index.html>

Accreditation Criteria
http://www.iasonline.org/Accreditation_Criteria/index.html

Listing of Accredited Organization
<http://www.iasonline.org/More/search.html>

The Process of Accreditation by IAS

1. Application Submission

"Inspection agency" (aka "licensee" or "applicant") submits an application for accreditation. The application includes an authorized signature by the applicant and an agreement to: be bound by certain legal conditions (which, among other things, incorporate by reference the Rules of Procedure and the Accreditation Criteria, as amended from time to time).

A. Rules of Procedure. These include agreement to, among other things:

- * Permit IAS to conduct "unannounced inspections" for which the licensee reimburses costs,
- * The grounds for accreditation revocation or modification with a right to a hearing (including failure to comply with conditions in the application or for misstatements of fact, or " Any other ground considered as adequate cause in the judgment of IAS") and accreditation revocation/cancellation without the right to a hearing (including failure to pay required fees, failure to furnish required material or data, failure to respond to a deficiency report or to permit on-site inspection)
- * The grounds for release of confidential data of the licensee by IAS (including pursuant to a court order)
- * Permission to publish accreditation certificates on the IAS web site
- * Refrain from referring to accreditation in any way that "indicates or implies" endorsement by IAS of any particular product.

B. Conditions for Application. This document, accepted by the licensee as part of the application, includes a long and detailed array of legal terms that strongly favor the accreditation authority, including:

- * Reiteration of permission for spot inspection and reimbursements
- * Comprehensive limitation of warranties:
 - "...accreditation does not imply any guarantee or warranty, express or implied and including but not limited to any warranty of merchantability or fitness for any particular purpose, of any product tested or certified by the applicant, or any guarantee or warranty of any nature by IAS concerning any tests or calibration conducted by the applicant."
- * Ceding various causes of action against IAS as the accreditor
 - "Applicant agrees that it shall have no cause of action or claim against IAS, International Code Council (ICC), or any of their affiliates, parent, or brother or sister corporations or their Successors-in-Interest or assigns, or the officers, directors, members and employees thereof, arising in any manner from any denial of this application or from any accreditation given pursuant to this application, whether or not such accreditation is or is not subject to any conditions."
- * Broad indemnity rights for IAS as the accreditor
 - "Applicant agrees to hold IAS, ICC, and their affiliates, Successors-in-Interest, parent, or brother or sister corporations or their Successors-in-Interest and assigns, and the officers, directors, members and employees thereof of such entities harmless, and to protect, defend and indemnify them, with respect to any claim, liability, demand, action,

judgment, proceeding, costs, damages and expenses (including attorneys' fees) whether for personal injury, wrongful death, property damage, or any type of injury or damage whatsoever, arising from: (i) any certification or approval services of any nature provided by the applicant; (ii) the use of any service of any nature offered by the applicant, or the use or operation by any person of any product tested/calibrated or certified by the applicant, whether related to the matters set forth in the first sentence of this paragraph or otherwise; or (iii) the reference to or reliance upon, actual or asserted, any product certification or approval given by the applicant or any testing or calibration services rendered by the applicant including but not limited to the results of any testing or calibration conducted by the applicant.

* Favorable severability provision for IAS as the accreditor

" If any part or portion of this paragraph, or any application thereof to particular facts, should be determined invalid, the provisions hereof shall be severable so as to achieve for IAS and ICC the maximum legal application." and

* Incorporation by reference and agreement to other rules and procedures of IAS

" In consideration of the processing of this application, the applying laboratory agrees to abide and be bound by any conditions attached to any listing or renewal thereof issued pursuant to this application, or any later amendment of said listing or renewal, the Rules of Procedure for Laboratory Accreditation, which by this reference are made a part hereof, the Accreditation Criteria for Testing Laboratories, which by this reference is made a part hereof, and the Accreditation Criteria for Calibration Laboratories, which by this reference is made a part hereof, and any additions, deletions, or changes to such Rules or Accreditation Criteria hereafter adopted. In agreeing to abide and be bound by the Rules of Procedure and the Accreditation Criteria for Testing Laboratories and Accreditation Criteria for Calibration Laboratories, the applying laboratory understands that the failure to do so may result in the revocation, suspension or modification of accreditation issued pursuant thereto in accordance with the terms of the Rules of Procedure."

Highlighting the important status of this document, another signature and date are required at the bottom of the Conditions form, in addition to the signature required on the application which this form is a part of.

Along with the application, the applicant also submits the appropriate fees and a copy of the companies quality manual (against which it is assessed for accreditation).

2. Fees for IAS accreditation are as follows:

* New Applications (one year period of validity)

Range is between \$1,000 (for Calibration Laboratories) to \$5,950 (for Fabrication Inspection Programs of 76 employees and above).

* Renewal Applications (one, two and three year validity)

Somewhat less, but comparable to the application fees for new applications, with deeper discounts the more years purchased.

* Assessment Fee

Assessment fees in the \$800/day range, as well as \$600/day travel expenses are also applicable.

3. An IAS Representative is assigned to the application, and contacts the applicant to assist in bringing its manual "into full compliance with the accreditation criteria"

4. Once the manual is in compliance, the IAS staff will conduct on-site visits to the head quarters and field operations of the applicant. This is the assessment.

5. The management of the applicant is provided with an "assessment report" which may include "reference to corrective actions that must be carried out" in order to be accredited.
6. Accreditation is awarded once the applicant has taken any required corrective actions and satisfied all the other criteria.
7. Accreditation is granted for one year initially, and thereafter for one, two or three years. However, on-site inspections must happen no less than every two years.

Standards

IAS bases its standards upon ISO/IEC 17020: 1998, General Criteria for the Operation of Various Types of Bodies Performing Inspection. Unfortunately, this standard is proprietary and not available free of charge. A fee must be paid to the ISO to gain access to this document. This appears to be a relevant document and the EAP would benefit from gaining access to it.

IAS also develops its own standards and guidelines. For example, in a guidelines document clarifying requirements for "internal audit", IAS indicates the need for particular types of documentation, training of auditing staff, written procedures for corrective action in the case of problems discovered during audits, the minimum time periods between internal audits and other relevant factors. Another document clarifies which personnel with signatory authority for test and assessment results are sufficiently significant to trigger a need to notify IAS when there are personnel changes in those roles. Many other guidelines and clarifications are also provided by IAS to assist the companies it accredits.

Example II

United Kingdom Accreditation Service of Feltham, UK

Scope Predominantly United Kingdom

<http://www.ukas.com/>

The United Kingdom Accreditation Service (UKAS) is the sole national accreditation body recognised by government to assess, against internationally agreed standards, organisations that provide certification, testing, inspection and calibration services. Accreditation by UKAS demonstrates the competence, impartiality and performance capability of these evaluators.

Basic Information:

Application Information for Companies Seeking Accreditation:

http://www.ukas.com/information_centre/accreditation_category_forms.asp

Accreditation Standards

http://www.ukas.com/about_accreditation/accreditation_standards.asp

http://www.ukas.com/information_centre/publications.asp

Listing of Accredited Organization

http://www.ukas.com/about_accreditation/accredited_bodies/default.asp

The Process of Accreditation by UKAS

1. Application Submission

Applicant (aka "licensor" or "accredited organization") submits an application for accreditation. It can take, typically, between half a year and a year and a half to achieve accreditation from the date of application, depending on the type of accreditation sought and the size/complexity of the applicant organization and process.

The application includes a "declaration" page, whereby the applicant agrees to "comply with the relevant European or International Standards, the applicable UKAS requirements, and UKAS Publications as listed on the website (www.ukas.com).". In this way, the various policies, procedures and other rules are incorporated by reference into the application process itself, with binding effect.

The declaration page also requires indication that two signed copies of the UKAS Agreement are enclosed with the application, along with the non-refundable £1200+VAT application fee. The signature line includes a warranty that the signatory is authorized to sign for the applicant and that all the information in the application is "correct and accurate to the best of my knowledge and belief."

The UKAS Agreement, signed and enclosed with the application, is an excellent and relatively balanced set of terms governing the entire accreditation process, including the following terms:

- * *Surprise Inspection.* UKAS reserves the right to carry out additional or unscheduled surveillance visits, as it may reasonably require.
- * *Discretionary revocation, suspension or other sanctions, if applicant fails to cure problem.* If, in UKAS' view, the applicant fails to comply with the terms of this Agreement, UKAS may suspend or withdraw accreditation, reduce the scope of accreditation, impose a moratorium on the issue of accredited certificates or extensions to scope, require re-assessment or impose such other sanctions as are appropriate and legal. Withdrawal of accreditation will not be imposed unless the Body fails to carry out the actions required to maintain accreditation in the requisite timescales as notified in writing by UKAS.
- * *Warranties to cooperate with business rules.* Applicant makes warranties it provides accurate, complete information, will open facilities for inspection, will remain in compliance with rules at all times, will notify UKAS of planned material changes (which are listed in the agreement), will "Not to use its accreditation in such a manner as to bring accreditation into disrepute", and will "make it clear in all contracts with its clients and in guidance documents that a certificate or report issued by it in no way implies that any product, service or management system certified is approved by UKAS.
- * *Promise to help investigate and resolve third party complaints.* "To assist UKAS in the investigation and resolution of any properly authenticated complaints made by third parties about the Body's accredited activities."
- * *Confidentiality.* Agreement to keep applicant information confidential, except in cases such as a court order.
- * *Relatively even-handed mutual liability and damages allocation, and exceptions.* "In providing the service(s), information or advice, neither UKAS nor any of its officers, employees or agents warrants the accuracy or completeness of any information, review, audit, accreditation or advice supplied. Except in respect of death or personal injury caused by UKAS' negligence or as set out herein, neither UKAS nor any of its officers, employees or agents (on behalf of each of whom UKAS has agreed this clause) shall be liable to the Body for any loss of profit or any indirect, special or consequential loss, damage, costs or expenses or other claims (whether caused by the negligence of UKAS, its officers, employees or agents or otherwise) which arise out of or in connection with the provision of the services or their use by the Body by reason of any representation (unless fraudulent) or any implied warranty, condition or other term, or any duty at common law or under the express terms of this Agreement, and the entire liability of UKAS under or in connection with this Agreement shall not exceed the higher of £25,000 or the agreed annual fee."

** Limited indemnity for the UKAS only for misuse of accreditation or breach by applicant.*
"The Body undertakes to indemnify UKAS against any losses suffered by or claims made against UKAS as a result of misuse by the Body of any Certificate of Accreditation or licence to use any accreditation mark granted by UKAS or as a result of any breach by the Body of the terms of this Agreement."

** Simple 90 day-notice mutual termination clause. And,*

** Prohibition against assignment absent written agreement by the parties.*

2. Fees for UKAS accreditation are as follows:

Application Fee

The fee is £1200 (£1410 including VAT)

Daily Rate for Pre and Initial Assessment Work

The daily rate for pre -assessment and initial assessment work is £775.

Daily Rate for Other Work

The daily rate for all other services, unless otherwise agreed, is £542.

Annual Accreditation Fees

The fee is calculated as a quarter of the total assessment effort in the four year program multiplied by the day rate for the standard set out below

Standard	£
ISO/IEC 17025, ISO/IEC Guide	43 83
ISO/IEC 17020	260
EN 45011/45012, ISO/IEC 17024, ISO/IEC Guide 66	285

A pro-rata fee will be charged if accreditation is granted during the year.

3. Application Received, Staff Allocated

Upon receipt, the application is reviewed by an Accreditation Manager who allocates an Assessment Manager to the case. The Assessment Manager is the case officer responsible for taking the applicant through the accreditation process and for maintaining and renewing accreditation in the future.

4. Applicant Contacted

The Assessment Manager contacts the applicant after studying the documentation submitted and discusses the need for a pre-assessment visit and the composition of the proposed assessment team.

5. Pre-assessment Visit, Provision of Firm Quote

UKAS normally recommends a pre-assessment visit by the UKAS Assessment Manager. This visit addresses the scope of accreditation requested and will normally involve between 1 and 3 man-days work. It is designed to confirm the applicant organization's readiness for full assessment. The Assessment Manager provides a quotation for the work involved.

6. Initial Assessment Visit

This is conducted by the Assessment Manager supported, as necessary, by technical assessors with the expertise to cover the scope of accreditation. The length of the visit will depend upon the scope of accreditation requested. Prior to the visit, the applicant receives a "visit plan" which provides a proposed timetable for the work to be assessed. Any nonconformities found against accreditation requirements are notified to the applicant in writing during or immediately following the assessment visit.

7. Granting of Accreditation and Renewal Periods

After being apprised of nonconformities, the applicant is then asked to advise UKAS on how it intends to clear the nonconformities. Once they have been cleared to the satisfaction of UKAS, applicant is granted accreditation. Accreditation is "confirmed on an annual basis by surveillance visits, with a full re-assessment every fourth year. The first surveillance visit takes place 6 months after the Grant of Accreditation."

Standards

The UKAS also relies upon ISO standards that are proprietary. In addition, however, it relies upon various highly relevant European standards that are freely available in English. One such key standard is [EA-7/01](#), The EA Guidance on the application of ISO/IEC Guide 62:1996, and [EA-7/03](#), [EA-6/02](#), [EA 6-01](#), and other EU and UKAS standards and guidelines available at http://www.ukas.com/information_centre/publications.asp.

MOU

Another interesting and relevant aspect of the UKAS example is the presence of an MOU between it and the government of the UK. The MOU is available at:

http://www.ukas.com/about_UKAS/memorandum_of_understanding.asp. This document is interesting because it exists solely in the realm of perception and trust and (by its own terms) it "does not create any rights, liabilities or obligations which would have binding effect in law." However, the UK government does use the non-binding language to communicate the UKAS is the "sole national body in the UK recognised by Government to provide accreditation of conformity assessment..." and indicates a willingness to encourage government and private organizations to use the services of UKAS and to provide public funds if needed to assist in creation of new accreditation services until they are self-funding. Though the document has no binding legal effect, it is a powerful message to organizations across the economy about the legitimacy and importance of the accreditation process and UKAS.

/end/

ATTACHMENT 2.

MODEL BLURB	WHO: TRUSTe WHAT: Internet Privacy Certification and Trust Mark Issuance URL: http://www.truste.org/																				
Internal or 3rd Party Assessors	Mix of Self-Assessment and final check by TRUSTe staff. Right to on-site inspection by CPA or other party is reserved, for cause (e.g. patterns of complaints).																				
Decision Making Process	The criteria appear to be developed by TRUSTe itself, in consultation with "consumers and government authorities".																				
Control and Mgmt. Processes	In the first instance, applicants for the privacy seal agree to a license agreement with many legal term and obligations, including submission of a truthful self-assessment of the companies privacy practices. The self-assessment is submitted and TRUSTe staff verified the information with the company typically (evidently) by talking on the phone with company staff and looking at the companies web site and other information. It is not part of the regular course of business to make a site visit to the company, but the right to do so is reserved by TRUSTe, for cause. "Once TRUSTe has processed your application, received your privacy statement, and obtained a completed self-assessment form, your account manager will contact you to set up a phone conference to review your site and privacy statement. For Web sites that have not launched yet, please keep in mind that you will need to provide TRUSTe access to the site for us to conduct our review and certification process."																				
Liability of Each Party	The liability of TRUSTe and companies that have been approved to use the TRUSTe privacy seal is detailed in the License Agreement, including: <ul style="list-style-type: none"> * A full warranty disclaimer by TRUSTe, * Indemnity by TRUSTe to licensee in event of IP infringement suit based on TRUSTe mark, * Indemnity by licensee to TRUSTe for a wide range of other potential sources of litigation based on use of the TRUSTe mark, * complete mutual waiver of consequential, indirect, incidental, punitive damages or damages from lost profits, or damage to good will, and * Liability limitations of the total amount actually paid apply to each party vis each other, except for damages, losses, expenses, and other costs to TRUSTe for misrepresentations by licensee. Note: the above is a simplification of the key legal terms. Also, there are more varied and detailed terms bearing on liability of parties.																				
Flow of Money	Pricing for companies with a single brand: <table> <thead> <tr> <th>Your Company's Annual Revenue in USD</th> <th>Cost Per Brand</th> </tr> </thead> <tbody> <tr> <td>\$0 - \$4,999,999</td> <td>\$599</td> </tr> <tr> <td>\$5,000,000 - \$9,999,999</td> <td>\$899</td> </tr> <tr> <td>\$10,000,000 - \$19,999,999</td> <td>\$1,999</td> </tr> <tr> <td>\$20,000,000 - \$49,999,999</td> <td>\$3,999</td> </tr> <tr> <td>\$50,000,000 - \$74,999,999</td> <td>\$4,999</td> </tr> <tr> <td>\$75,000,000 - \$99,000,000</td> <td>\$6,999</td> </tr> <tr> <td>\$100,000,000 - \$499,999,999</td> <td>\$8,999</td> </tr> <tr> <td>\$500,000,000 - \$1,999,999,999</td> <td>\$9,999</td> </tr> <tr> <td>\$2,000,000,000 and above</td> <td>\$12,999</td> </tr> </tbody> </table>	Your Company's Annual Revenue in USD	Cost Per Brand	\$0 - \$4,999,999	\$599	\$5,000,000 - \$9,999,999	\$899	\$10,000,000 - \$19,999,999	\$1,999	\$20,000,000 - \$49,999,999	\$3,999	\$50,000,000 - \$74,999,999	\$4,999	\$75,000,000 - \$99,000,000	\$6,999	\$100,000,000 - \$499,999,999	\$8,999	\$500,000,000 - \$1,999,999,999	\$9,999	\$2,000,000,000 and above	\$12,999
Your Company's Annual Revenue in USD	Cost Per Brand																				
\$0 - \$4,999,999	\$599																				
\$5,000,000 - \$9,999,999	\$899																				
\$10,000,000 - \$19,999,999	\$1,999																				
\$20,000,000 - \$49,999,999	\$3,999																				
\$50,000,000 - \$74,999,999	\$4,999																				
\$75,000,000 - \$99,000,000	\$6,999																				
\$100,000,000 - \$499,999,999	\$8,999																				
\$500,000,000 - \$1,999,999,999	\$9,999																				
\$2,000,000,000 and above	\$12,999																				

	<p>Corporate (up to 10 brands) \$25,000 Enterprise (up to 300 brands) \$75,000</p> <p>Pricing for companies with multiple brands: The \$25,000 Corporate and \$75,000 Enterprise rates are for companies with multiple brands that all share a common privacy policy and adhere to common information collection practices.</p>
Dispute Resolution Process	There is an appeal process for approval/non-approval decisions with decision by 2 privacy experts and 2 members of the TRUSTe Board of Directors. In addition, TRUSTe provides "watch dog" services to consumers with complaints about privacy practices of companies licensed to use the TRUSTe privacy seal. Evidently, TRUSTe attempts to help negotiate solutions and reserves the right to the following remedies:
Validity Period of Cert-ification	One or Two years. However, " licensees will submit a full self-assessment every three years, regardless of the length of their license term (with exceptions, e.g., in the case of an assignment or when the Program Requirements have changed). COPPA and EU Safe Harbor program participants must continue to complete a new self-assessment annually, in keeping with the specific requirements of those programs."
Notes/Ideas	Again, the ability to field complaints directly from customers of the company certified appears to be a major component of the reliability and assurance regime.
Parking Lot	

MODEL BLURB	<p>WHO: Internet Content Rating/ICRA What: Self regulatory parental ratings online system. URL: http://www.icra.org/</p>
Internal or 3rd Party Assessors	Self-Ratings by licensee of ICRA mark, with automated and manual checks to verify accuracy of rating.
Decision Making Process	ICRA as a non-profit corporation evidently makes final determination of the criteria. In this case, the criteria are content classifications (e.g. regarding nudity, violence, language, etc).
Control and Mgmt. Processes	A licensee submits an online application to become an Associate member or contacts staff directly to inquire about full membership. Membership evidently requires agreement to Terms and Conditions and other legal provisions covering the ratings and compliance process. The ICRA reserves the rights to conduct manual checks of content compliance in addition to the usual automated checking processes.
Liability of Each Party	<p>The legal pages associated with the membership form indicates the Licensee agree:</p> <ul style="list-style-type: none"> * not to impair the title, rights or interests of the ICRA in the ICRA marks (e.g. by registering the mark or using a confusingly similar mark), * " indemnify and hold ICRA™ harmless from any claims, suits, losses or damages (including reasonable legal fees incurred by ICRA), arising as a result of breach of this agreement or any other action taken by you in connection with any services, labelled site, misrepresentation, or violation of the registration questionnaire." * enter into this agreement without any representation or warranty of any kind being made by ICRA * actions by the ICRA " shall not give rise to any liability or obligations on the part of ICRA, or any rights of reliance by or for you or any third party, nor otherwise be deemed or construed as being for the benefit of

	<p>you or any third party. ICRA does not warrant or guarantee that the label will not infringe the trademark, service mark, trade name, copyright, or other intellectual property rights of any third party."</p> <p>NOTE: there does not appear to be any requirement that the licensee have a contract in place with others absolving the ICRA of liability to them or other third parties.</p>
Flow of Money	<p>Membership Categories and Subscription Levels Annual Subscription in US dollars Euros and Sterling (in that order):</p> <p>Corporations (With more than 100 employees) 30,000 35,650 21,350 Corporations (Fewer than 100 employees) 15,000 17,825 10,675 Non-profit (More than 100 employees)* 30,000 35,650 21,350 Non-profit (Fewer than 100 employees) 5,000 5,940 3,560 Associate member 100 100 70</p> <p>* ICRA Board may waive a portion of the fee</p>
Dispute Resolution Process	<p>There does not appear to be a formal dispute resolution process in place. However, in the event of revocation of a license because of misrepresentation of content, notification is sent to the licensee. "If the situation is not remedied two weeks after such notification ICRA reserves the right to take appropriate action including but not limited to, making the misrepresentation known through lists, web-postings and notifications to the press."</p>
Validity Period of Certification	<p>Apparently the validity period runs with the dues period, which is annual.</p>
Notes/Ideas	<p>The concept of automated testing, while clearly relevant to use of the filters and other standards applied by ICRA, may also have useful application for the EAP. Services of providers, use or validation of an EAP credential and other aspects of the work flow of the EAP system may be capable of processing and testing by automated means.</p>
Parking Lot	

ATTACHMENT 3.

Accreditation, Certification and Assessment Models

Prepared by Daniel Greenwood, Esq. for the EAP
May 27, 2004

Introduction

This overview is a partially complete analysis of research into several accreditation, certification and assessment models of potential application to the EAP. Not all models have been analyzed, and some are only partially complete. Attached at the end of the document are some preliminary summaries of some of the models done by research affiliates of mine and from which I am drawing basic references and links. I attach these summaries for your reference only, but they have not been fact checked and are not finished or presented work on this assignment.

Next steps are to finish analyzing the research and complete filling out the grid. Then, to look across each of the models in detail and evaluate similarities, differences and ideas drawn from each model.

Notes on grid nomenclature:

- * Information in brackets is tentative and based on apparent or probable facts, but not yet independently confirmed or traceable to a citation.
- * The phrase "decision making process" is applied primarily to the decisions regarding testing criteria. Other decision making, such as management, governance or corporate decisions are treated in the block for Control and Management Processes.
- * Not all information for all models are yet complete. Background information on many of the models can be found, in cached form (to guard against network unavailability at the source) at: <http://ecitizen.mit.edu/EAP/Accreditation/raw-research/> as well as through the links provided in the grids.
- * The "Parking Lot" item is reserved for particular issues, problems or prospects that arise in discussion a given model, but which must be returned to later in order to move forward with the bulk of the work in a timely manner. (In effect, they are put in the lot for later).
- * In no particular order, (in the form "Topic/Name") these are the Models currently being examined:
 - IT Security Products/ICSA
 - Network Administrators/Microsoft MSCE, Novell CNE
 - Higher Education/CHEA&DETCA
 - Electronics/UL
 - Computer Security Labs/NIST
 - Banks(FDIC)/Self Assessment Mix With Audit/Regulation
 - Hospitals/JCAHO
 - Internet Content Rating/ICRA
 - Global Payments/SWIFT
 - EMortgage eAuthentication/SISAC
 - National Accreditation Scheme (Germany)/DAR

Uniform Grid of Accreditation, Certification and Assessment Model

MODEL BLURB	Who: ICSA. What: Certification of Firewall. URL: http://www.icsalabs.com/html/communities/firewalls/index.shtml
Internal or 3rd Party Assessors	Model Owner Assesses and Certifies the firewall products. "Certification testing is performed either by skilled ICSA Labs security analysts or by third-party lab analysts trained and authorized by ICSA Labs for this purpose. As a design goal, testing is automated where possible, and is checklist oriented where not automated. The test procedures are reproducible, objective and not open to interpretation whatsoever. The testing personnel or authorized labs must have access to the product's associated help-desk, or the system's security personnel, to resolve questions. And there is an escalation procedure to resolve any potential conflicts or judgment questions." http://www.icsalabs.com/html/certification/index.shtml
Decision Making Process	Criteria used is developed by ICSA itself. Vendors of certified products are invited to join the Firewall Product Developers Consortium (FWDC) as a way to "influence" the process and criteria. " To develop and evolve appropriate and meaningful certification criteria, ICSA Labs uses a "notice of proposed certification criteria" system. ICSA Labs queries numerous specialists and organizations, potentially including affected vendors, developers, and users; the security expert community, the non-vendor specialists and experts, the Fortune-500 and vertical user consortia, unrelated or minimally related vendor consortia, academia, and other consumer and industry groups. A draft proposed criteria is then circulated within the appropriate people and groups before making the criteria final. Finally, ICSA Labs Certification criteria and processes are overseen by a Certification Oversight Board made up of well known security experts, which itself has broad representation."
Control and Mgmt. Processes	[Corporate lines of control internal to ICSA. Further information pending.]
Liability of Each Party	* ICSA secures contractual obligation by vendors to maintain their Certified products "that the product or system will be maintained at the current, published ICSA Labs Certification standards." Failure to meet this obligation, e.g. as identified during a spot test, leads to de-Certification (see Validity Period). * According to the site's FAQ, ICSA maintains an NDA with vendors seeking certification that precludes disclosing whether a vendor failed to achieve certification. Presumably, there is contractual liability for failure to meet these confidentiality obligations between ICSA and the vendors. Beyond this, no further information is available at this time. * ICSA publishes extensive information on avoiding Anti-Trust liability on its web site, called "ICSA Labs Anti-Trust Guidelines".
Flow of Money	Vendor pays for certification Vendor pays membership in Consortium (separate from certification) Customers view certification lists at no charge.
Dispute Resolution Process	Not available. [ICSA Labs urges vendors to be involved in the process of setting product standards. Then it urges vendors to patch or upgrade their products that fail the testing process. If a product is not performing to standard, ICSA communicates with the vendor's customer service people to see if they can remedy the problem.]
Validity Period	Approximately one year. However, spot testing is authorized. Failure

of Certification	<p>to remedy flaws discovered during spot test lead to public revocation of Certification. "If the shipping product or production system still does not meet current certification criteria by the end of this grace period, then ICSA Labs Certification is explicitly and publicly revoked."</p> <p>http://www.icsalabs.com/html/certification/index.shtml</p>
Notes/Ideas	<p>Accreditation is not used as a word, "Certification" is used to mean the process of testing a product leading to decision on whether it may use the ICSA trust mark (i.e.: is a "Certified firewall").</p> <p>ICSA offers membership as way to influence development of criteria by vendors on a vendor consortium. This is a different model from membership in a stakeholder council that makes the final decisions and is partially comprised of vendors (i.e.: CSPs) who are also the subject of Certification. ICSA method eliminates potential appearance of conflicts of interests. However, it also eliminates collaborative partnership benefits.</p>
Parking Lot	

MODEL BLURB	<p>Who: Council for Higher Education Accreditation</p> <p>What: Recognition of Higher Education Accreditors. CHEA "Recognizes" (i.e.: accredits) organizations that themselves Accredit institutions of higher education (such as the DETCA, below).</p> <p>URL: http://www.chea.org</p>
Internal or 3rd Party Assessors	<p>Model owner assesses organizations applying for recognition. CHEA "Committee on Recognition" is appointed by the CHEA Board of Directors. Committee membership is staggered and drawn from various stakeholder groups and is accountable to the Board. In discretion of the Committee, "peer review" may be added to assessment, whereby, in consultation with organization seeking recognition, a "site visitor" may be selected to perform an on-site inspection.</p>
Decision Making Process	<p>The criteria against which applicants for recognition are assessed are wholly developed by CHEA. See:</p> <p>http://www.chea.org/recognition/recognition.asp</p>
Control and Mgmt. Processes	<p>A detailed process is set out involving a "Self-Study" application (basically, self assessment against the criteria), back and forth between the Committee and applicant in written form, a possible site visit, a public presentation, opportunity for comments, and ability to seek decision review. Notice is built in at nearly every phase. The Board of Directors exercises ultimate ownership and control over the decision process, but the Committee is invested with authority to act based on the rules.</p>
Liability of Each Party	<p>Unknown at this time.</p>
Flow of Money	<p>The applicant for recognition pays all costs of recognition, including direct costs, annual participation fee, and other costs. There are also membership dues, sponsorships, fees for accreditation visits, conference revenue and other sources of funding for CHEA. See:</p> <p>http://www.chea.org/pdf/fact_sheet_5_operation.pdf and</p> <p>http://www.chea.org/recognition/recognition.asp#24</p>
Dispute Resolution Process	<p>This is addressed at three levels:</p> <p>1. Accrediting organizations seeking recognition from CHEA may seek review and appeal of a negative decision by the Recognition Committee,</p>

	<p>2. Accrediting organizations must have mechanisms by which an institution or program that is dissatisfied with a review may express its dissatisfaction and seek redress, and</p> <p>3. Accrediting organizations describe the terms and conditions under which a complaint can be lodged against an institution or program that is accredited (this includes complaints from the general public, by students or others).</p>
Validity Period of Certification	For a maximum of 10 years, with a five year interim report, but CHEA may review at any time "if the accredit or makes major changes in how it operates or if there are a series of documented concerns about the organization." http://www.chea.org/pdf/fund_accred_20ques_02.pdf
Notes/Ideas	
Parking Lot	

MODEL BLURB	Who: Distance Education and Training Council What: Accreditation of Institutions of Higher Education Using Distance Learning Technologies URL: http://www.detc.org/
Internal or 3rd Party Assessors	[Model owner directly assesses applicant institutions, including through use of on-site inspections]
Decision Making Process	[Model owner determines criteria and posts all relevant information on its web site.]
Control and Mgmt. Processes	[Model owner accreditation team, using self-appraisal information and site-visits, test applicant against criteria.]
Liability of Each Party	[Contractual obligations by applicant educational institution promising, among other things, to notify DETC of material changes and not to publish fact of accreditation in progress so as to avoid misleading the public as to accreditation status.]
Flow of Money	[Applicant pays all costs according to a published fixed cost schedule for site visits and other activities. Typical accreditation fee is \$7,000 - \$10,000 USD]
Dispute Resolution Process	[Process published to contest decision of DETC, but appeal is made to DETC, with due process protections in place. Also, process for third party complaints to DETC regarding accredited institutions is in place and publicized.]
Validity Period of Certification	[There are five-year re-accreditation reviews, with immediate status review when cause shown.]
Notes/Ideas	This is a very good model in terms of detailed practices and policies including many potentially useful ideas. All their processes and rules are available for free online.
Parking Lot	

MODEL BLURB	WHO: Underwriters Laboratory WHAT: Certification of Products Safety and Quality URL: http://www.ul.com
Internal or 3rd Party Assessors	Model owner tests products in UL Labs or other authorized labs in the "family of companies", and also conducts follow-up visits to test products after certification in the field. 60 laboratory, testing and certification facilities were part of the UL family of companies. UL staff examine how products

	<p>are constructed, conduct tests, evaluate results and develop safety standards. UL also has field representatives who visit manufacturers' facilities. They help confirm that products bearing the UL Mark comply with applicable UL safety requirements. UL conducted 547,708 follow-up visits in 2003 to audit compliance with product certification requirements.</p> <p>In addition, apparently UL has an MOU in place allowing other organizations to test to UL Safety Standards. "The UL family of companies maintains a number of agreements, called Memorandums of Understanding (MOUs), with product testing and certification organizations in international markets. The MOU provides a mechanism for the two participating agencies to work toward mutual recognition of each other's testing results for one or more specific product categories."</p>
Decision Making Process	<p>Model owner determines criteria.</p> <p>" UL Standards for Safety are developed under a procedure which provides for participation and comment from the affected public as well as industry. The procedure takes into consideration a survey of known existing standards and the needs and opinions of a wide variety of interests concerned with the subject matter of the standard. Manufacturers, consumers, government officials industrial and commercial users, inspection authorities and others provide input to UL." There are 876 UL Standards.</p>
Control and Mgmt. Processes	<p>Details not yet available. Evidently, there is a somewhat collaborative process whereby a company submits an application for testing, and is consulted as to the testing process, fees, scope, timing and other aspects during an initialization period.</p>
Liability of Each Party	<p>Details not yet available. [There may be some potential benefit in terms of evidence of non-negligence in judicial proceedings if a defendant can show certification by and compliance with UL standards in a product liability or other tort action. In addition, there are legal confidentiality requirements in the application contracts whereby applicant proprietary or trade secret information is kept confidential and UL employees sign NDA's to assure applicant information remains confidential.]</p>
Flow of Money	<p>Details to follow. "Cost varies depending on the product and complexity of test requirements. Once UL's engineering staff review your product information to determine the scope and time involved in the testing process, they will provide you with a cost estimate. UL will work with you in determining the time frame for testing, depending on when you need the project completed."</p>
Dispute Resolution Process	<p>There is some form of an internal appeals process for UL rejection of certification that, evidently, does not affect other aspects of the UL/applicant relationship. " If you have any questions about your test results, the interpretation of a requirement or any UL decision, the UL appeals procedure provides a method for your concerns to be heard by UL management without jeopardizing your relationship with UL. Just contact our engineering staff for more details."</p> <p>In addition, there are processes documented in the UL site FAQ regarding "Variations" (i.e. when a product is found not to comply after certification has been granted). To resolve the items written on the Variation Notice, the manufacturer can elect one of the following choices for each item:</p> <ul style="list-style-type: none"> • Rework the units to bring them into compliance, • Remove the UL Mark from the affected units, or

	<ul style="list-style-type: none"> Hold the units pending review by UL. <p>So called "variations" can result in withdrawal of the authorization to use the UL Mark.</p>
Validity Period of Cert-ification	Details not yet known. [Evidently, it is perpetual, with follow-up inspections paid for by applicant. "You must agree to participate in UL's Follow-Up Services program. You indicate your willingness to participate by signing and returning the Follow-Up Services Agreement."] There are a large number of different UL marks, each signifying different compliance or a different market (see: http://www.ul.com/mark/index.html)
Notes/Ideas	The relatively collaborative nature of the relationship between applicants and the UL lab staff who will conduct the testing was a surprise. Evidently, this somewhat flexible process has not negatively affected the quality or perceived reputation of the UL process.
Parking Lot	

MODEL BLURB	WHO: TRUSTe WHAT: Internet Privacy Certification and Trust Mark Issuance URL: http://www.truste.org/
Internal or 3rd Party Assessors	
Decision Making Process	
Control and Mgmt. Processes	
Liability of Each Party	
Flow of Money	
Dispute Resolution Process	
Validity Period of Cert-ification	
Notes/Ideas	
Parking Lot	

MODEL BLURB	Network Administrators/Microsoft MSCE, Novell CNE (http://www.novell.com/training/certinfo/ http://www.microsoft.com/learning/mcp/mcse/default.asp)
Internal or 3rd Party Assessors	
Decision Making Process	
Control and Mgmt. Processes	
Liability of	

Each Party	
Flow of Money	
Dispute Resolution Process	
Validity Period of Certification	
Notes/Ideas	
Parking Lot	

MODEL BLURB	Computer Security Labs/NIST http://csrc.nist.gov/sec-cert/ca-process.html and http://csrc.nist.gov/nssc/1998/proceedings/paperE1.pdf
Internal or 3rd Party Assessors	
Decision Making Process	
Control and Mgmt. Processes	
Liability of Each Party	
Flow of Money	
Dispute Resolution Process	
Validity Period of Certification	
Notes/Ideas	
Parking Lot	

MODEL BLURB	Banks(FDIC)/Self Assessment Mix With Audit/Regulation (See, generally, http://ecitizen.mit.edu/EAP/Accreditation/raw-research/BANKS/Research/)
Internal or 3rd Party Assessors	
Decision Making Process	
Control and Mgmt. Processes	
Liability of Each Party	
Flow of Money	
Dispute Resolution Process	

Validity Period of Certification	
Notes/Ideas	
Parking Lot	

MODEL BLURB	Hospitals/JCAHO http://www.jcaho.org
Internal or 3rd Party Assessors	
Decision Making Process	
Control and Mgmt. Processes	
Liability of Each Party	
Flow of Money	
Dispute Resolution Process	
Validity Period of Certification	
Notes/Ideas	
Parking Lot	

MODEL BLURB	Internet Content Rating/ICRA http://www.icra.org/
Internal or 3rd Party Assessors	
Decision Making Process	
Control and Mgmt. Processes	
Liability of Each Party	
Flow of Money	
Dispute Resolution Process	
Validity Period of Certification	
Notes/Ideas	
Parking Lot	

MODEL BLURB	Global Payments/SWIFT http://www.swift.com/
Internal or 3rd Party Assessors	
Decision Making Process	
Control and Mgmt. Processes	
Liability of Each Party	
Flow of Money	
Dispute Resolution Process	
Validity Period of Cert- ification	
Notes/Ideas	
Parking Lot	

MODEL BLURB	EMortgage eAuthentication/SISAC http://www.sisac.org/
Internal or 3rd Party Assessors	
Decision Making Process	
Control and Mgmt. Processes	
Liability of Each Party	
Flow of Money	
Dispute Resolution Process	
Validity Period of Cert- ification	
Notes/Ideas	
Parking Lot	

MODEL BLURB	National Accreditation Scheme (Germany)/DAR http://www.dar.bam.de/qmh_e/
Internal or 3rd Party Assessors	
Decision Making	

Process	
Control and Mgmt. Processes	
Liability of Each Party	
Flow of Money	
Dispute Resolution Process	
Validity Period of Certification	
Notes/Ideas	
Parking Lot	

Accreditation and Certification Potential Matrix

[Note: It remains to be seen how meaningfully to capture information in each cell. However, this is a draft matrix in a proper form to do a single comparison chart.]

Name	Internal or 3 rd Party Assessors	Decision Making Process	Control and Mgmt. Processes	Liability of Each Party	Flow of Money	Dispute Resolution Process	Validity Period of Certification
FDIC	Mixed	Gov't	Gov't	Complex	UserPays		
JCAHO							
ICRA							
ICSA							
SWIFT							
CHEA							
DETC							
SISAC							
UL							
TRUSTe							

APPENDIX: Raw Research Summaries

Model name: Combination self-assessment and external examination

Representative of the model: US National Banks

Summary: A chartered bank must satisfy standards established by a third party, namely regulators such as the Office of the Comptroller of the Currency, the FDIC and the Federal Reserve. To meet those standards, a bank hires executive officers to manage the bank in accordance with the standards. A bank must set up a board of directors and an internal audit function that monitors compliance constantly. The board of directors and internal auditors do the lion's share of the accreditation work. Next, building on the work performed by the board of directors and the internal auditors, external CPA auditors examine the bank periodically. The internal auditors and external auditors must be independent of each other. See Interagency Policy Statement on Internal Audit and Internal Audit Outsourcing, March 17, 2003, [OCC 2003-12](#). Then, building on the work of the internal and external auditors, third-party examiners (from government regulators) examine the bank. See "About the OCC" at <http://www.occ.treas.gov/aboutocc.htm>.

Is the schema model based on in internal or third party certification process?

The model is based on a combination, including both internal and third party review. The third-party component includes review by both an external CPA and a third party regulator. In a variation of the model, the third party regulator could be replaced by a private industry association.

Define the liability framework associated with each named participant within the model, specifically as it applies to the certification and accreditation process.

By law, the executive officers and the board of directors assume liability to investors, depositors and other creditors. In theory, internal auditors assume professional liability, but in practice they are sued only in extreme circumstances; internal auditors are usually just mid-level employees. The external CPA auditors assume a measure of professional malpractice liability. The third party regulator (or industry association) assumes no liability, but it has a reputation to uphold.

Define the flow of money within the model, as it specifically applies to the certification and accreditation process (third party provider fees paid to the model owner for initial accreditation, third party continuing services/maintenance fees paid to the owner, identity issuer/relying party assessment fees paid to the third party auditor, identity issuer/relying party certification/accreditation fees paid to the owner).

The bank pays

- * salary to the executive officers
- * fees to the members of the board of directors,
- * salary to the internal auditors,

- * fees to the external auditors
- * periodic dues to the third party regulator (regarding dues to the Office of the Comptroller of the Currency, see “About the OCC” at <http://www.occ.treas.gov/aboutocc.htm>).

Define the dispute resolution process within the model, as it specifically applies to all named participants, within the certification and accreditation process.

Those parties identified above as bearing liability can be sued by investors, depositors and other creditors of the bank.

The bank can fire the directors and auditors with which it disagrees. If a bank disagrees with an examiner, the bank has right to appeal within the regulatory framework governing the examiner.

Define the decision making processes each model owner utilizes to develop and deploy their model.

The standards are established by regulators in consultation with the banks and the public. Regulators are constantly reviewing their standards and revising them. To meet the standards, the bank board of directors is responsible for authorizing and monitoring internal measures. The executive officers are responsible for implementing internal measures.

Define the control/management processes each model owner utilizes to support their deployed model.

Regulators possess a range of sanctions they can bring against banks that fail to comply, including fines, changes in capital requirements and the power to bar individuals from serving as bank officers.

The results of regulatory examinations are normally not made public, although the FDIC does publish some quarterly information about each bank’s financial condition. see “About the OCC” at <http://www.occ.treas.gov/aboutocc.htm>.

Define the length of time that a third party auditor accreditation and/or identity issuer/relying party assessment and/or certification/accreditation would be valid for.

A bank’s status can change almost immediately. Regulatory examination and discipline can occur at any time.

The goal of self-assessment by the board of directors and internal audit is to ensure constant compliance with standards and real-time correction when a deviation occurs.

Model name: Honor system labeling

Representative of the model: Internet Content Rating Association

Summary:

“The Internet Content Rating Association is an international, independent organization that empowers the public, especially parents, to make informed decisions about electronic media by means of the open and

objective labelling of content. . . . Web authors fill in an online questionnaire describing the content of their site, simply in terms of what is and isn't present. ICRA then generates a Content Label (a short piece of computer code) which the author adds to his/her site.

"Users, especially parents of young children, can then set their internet browser to allow or disallow access to web sites based on the objective information declared in the label and the subjective preferences of the user." http://www.icra.org/_en/about/

In large measure, the ICRA model is a voluntary honor system.

"ICRA makes both automated and manual checks on sites to verify that labels are in place and that they are applied appropriately." http://www.icra.org/_en/webmasters/#matrix

Is the schema model based on internal or third party certification process?

A web site wishing to participate reviews its web content and then labels it in accordance with the ICRA terms and guidelines. ICRA monitors use of its label primarily through automated and artificial intelligence searches. ICRA can conduct manual inspections. And, as an additional level of review, ICRA invites complaints from the public.

Define the liability framework associated with each named participant within the model, specifically as it applies to the certification and accreditation process.

"Displaying an ICRA logo button or 'Labelled with ICRA' text link without carrying the label is a breach of our terms and conditions." http://www.icra.org/_en/webmasters/#matrix

The ICRA labelling and filtering systems are protected by the U.S. Copyright laws and the ICRA name and logo are protected by the U.S. Trademark laws. http://www.icra.org/_en/legal/#notice

ICRA claims the right to sue someone who abuses its label.

Define the flow of money within the model, as it specifically applies to the certification and accreditation process (third party provider fees paid to the model owner for initial accreditation, third party continuing services/maintenance fees paid to the owner, identity issuer/relying party assessment fees paid to the third party auditor, identity issuer/relying party certification/accreditation fees paid to the owner).

"The ICRA labelling system is free for use by webmasters. Similarly, the ICRAfilter is free for use by parents and other concerned adults providing it is for their own personal use."

http://www.icra.org/_en/legal/#notice ICRA is funded by sponsorships/donations.

ICRA appears to get some revenue from advertising on its web site and possibly advertising in the filter it distributes to parents.

An alternative implementation of this model would entail the sponsoring organization charging for use of its label and filter, and perhaps charging for automated and manual audits.

Define the dispute resolution process within the

model, as it specifically applies to all named participants, within the certification and accreditation process.

ICRA will contact web sites that appear to abuse its label and seek resolution. ICRA may sue if its label is abused. ICRA may also publicize information about an abusive web site and recommend that access to it be blocked by user filters.

Define the decision making processes each model owner utilizes to develop and deploy their model.

Web site administrators are urged to participate as a way to be responsible citizens and to help avoid liability and condemnation.

Parents adopt the ICRA filter to protect their children.

ICRA monitor's use of its label and seeks resolution when it discovers abuse.

Define the control/management processes each model owner utilizes to support their deployed model.

Web administrators act voluntarily.

ICRA monitors use of its label and acts when it sees abuse.

Define the length of time that a third party auditor accreditation and/or identity issuer/relying party assessment and/or certification/accreditation would be valid for.

Web administrators are expected to keep the label current at all times.

Model name: Product certification

Representative of the model: ICSA Labs, which certifies IT security products, such as firewalls and anti-virus software. See <http://www.icsalabs.com>

Summary: ICSA Labs sponsors industry consortia within various segments of IT security products. One such segment is firewalls and another is anti-virus software. Within each product segment, ICSA tests and certifies products.

Although ICSA sets the standards/criteria by which it tests products, each consortium influences those standards and criteria. <http://www.icsalabs.com/html/communities/firewalls/index.shtml>

Each consortium serves as a source of information and ideas about the latest threats and responses. In addition to the consortia, ICSA openly consults with experts and industry customers as it sets standards. <http://www.icsalabs.com/html/certification/index.shtml>

Products that achieve certification are permitted to bear the ICSA Labs seal. ICSA publishes on its web site lists of the products that are certified, together with highly detailed reports on the testing of each product, including strengths, weaknesses and unique issues.

Testing is an interactive process. Vendors are allowed to assist ICSA by patching products or changing configuration. All this assistance is noted in the testing reports.

<http://www.icsalabs.com/html/communities/firewalls/faqs/index.shtml>

Certification is not an event. It is an on-going process. ICSA continuously deploys each certified product on-site and expects the vendors to maintain the product as it would at a customer site. Any product that is certified can lose its certification at any time. In order to keep current with the latest IT attacks, ICSA regularly reviews and changes its testing criteria and can apply the criteria against certified products at any time. Vendors thus have constant incentive to upgrade their products.

http://www.icsalabs.com/html/library/DataSheets/Firewall_Data.pdf

ICSA uses a “black box” approach to testing. This means it devotes little effort to critiquing the engineering behind a product. Instead, it tests the product’s performance. If the product performs to standard, then it is certified.

In addition to certifying products, ICSA sponsors surveys, buyer’s guides and other materials to help educate customers of security products. <http://www.icsalabs.com/html/communities/firewalls/index.shtml>

Is the schema model based on internal or third party certification process?

The model is purely third party certification. Testing is performed either by ICSA staff or by third parties authorized by ICSA.

Define the liability framework associated with each named participant within the model, specifically as it applies to the certification and accreditation process.

It does not appear that ICSA Labs has given much if any thought to liability. It openly publishes its certifications on its web site, with no disclaimers.

ICSA has probably never experienced any allegation of liability and has probably never sought counsel on the subject. ICSA could easily lower its exposure to product customers by publishing a disclaimer on its web site.

ICSA could also lower any exposure to vendors by contract with the vendors. ICSA does have a form of contract, but it simply focuses on an attestation by the vendor that it will continually provide all the information and support ICSA needs to perform its test.

<http://www.icsalabs.com/html/communities/firewalls/certification/program/Checklist.rtf>

ICSA does warn/educate its consortium members about antitrust liability. It publishes antitrust guidelines informing members they should not use the consortium to discuss prices or market allocation.

<http://www.icsalabs.com/html/library/Antitrust.pdf>

Vendors are liable to their customers according to the contracts between them.

Define the flow of money within the model, as it specifically applies to the certification and accreditation process (third party provider fees paid to the model owner for initial accreditation, third party continuing services/maintenance fees paid to the owner, identity issuer/relying party assessment fees paid to the third party auditor, identity issuer/relying party certification/accreditation fees

paid to the owner).

ICSA Labs charges vendors fees for testing and membership in the consortia. Customers can view certification/testing reports at no charge.

The parent company of ICSA Labs apparently gives access to product buyers' guides at no charge, though the parent probably tries to sell other products and services to customers.

<https://www.trusecure.com/premium/login.shtml>

Define the dispute resolution process within the model, as it specifically applies to all named participants, within the certification and accreditation process.

ICSA Labs urges vendors to be involved in the process of setting product standards. Then it urges vendors to patch or upgrade their products that fail the testing process. If a product is not performing to standard, ICSA communicates with the vendor's customer service people to see if they can remedy the problem.

Define the decision making processes each model owner utilizes to develop and deploy their model.

ICSA sets standards, conducts tests and publishes results. In setting standards seeks input from customers, experts and vendor consortia.

The only decision a vendor makes is whether it wants to participate.

The decision a customer makes is whether it wishes to assign weight to the results published by ICSA Labs.

Define the control/management processes each model owner utilizes to support their deployed model.

ICSA sets standards, conducts tests and publishes results. In setting standards seeks input from customers, experts and vendor consortia.

Define the length of time that a third party auditor accreditation and/or identity issuer/relying party assessment and/or certification/accreditation would be valid for.

ICSA Labs repeats the full testing process on an annual basis, but each product is subject to spot testing at any time. If a product fails spot testing and the vendor fails to remedy the problem within a short grace period, then the certification is revoked.

<http://www.icsalabs.com/html/certification/index.shtml>

Model name: Accreditation of an Institution

Representative of the model: Joint Commission on Accreditation of Healthcare Organizations - Hospital accreditation

Summary: This model accredits the staffing, resources and procedures within an institution, i.e. a hospital. The accreditation body is a private sector, industry association.

"An independent, not-for-profit organization, JCAHO is the nation's predominant standards-setting and accrediting body in health care. . . . JCAHO is governed by a 29-member Board of Commissioners that includes nurses, physicians, consumers, medical directors, administrators, providers, employers, a labor

representative, health plan leaders, quality experts, ethicists, a health insurance administrator and educators. . . JCAHO's corporate members are the American College of Physicians-American Society of Internal Medicine, the American College of Surgeons, the American Dental Association, the American Hospital Association and the American Medical Association.” <http://www.jcaho.org/about+us/index.htm>

A hospital is not required to be accredited, but accreditation helps a hospital with insurance, liability, winning of managed care contracts and so on. <http://www.jcaho.org/about+us/index.htm>

In most states, hospitals are licensed by government. JCAHO accreditation complements state licensure. It fulfills licensure requirements in many states, thus relieving the state of much of the burden of examination.

JCAHO publishes standards in consultation with experts and interest groups. JACHO provides interpretations about its standards. Then it surveys hospitals to determine whether they are meeting the standards. A survey results in a detailed report, including suggestions for improvement, which is kept private.

JCAHO publishes on its web site the accreditation status of a hospital (accredited, provisionally accredited, and so on), as well as a performance report, which “provides detailed information about an organization's performance and how it compares to similar organizations.” <http://www.jcaho.org/about+us/index.htm>
JCAHO will publicly place a hospital on “accreditation watch” status when JCAHO learns of a special event at a hospital that calls for attention.

In published performance reports, JCAHO will identify areas requiring improvement, and give hospitals a period of time to demonstrate improvement. JCAHO then revises the performance report to show the improvement whether the improvement was made.

Before a hospital is surveyed, it must announce to the public that a survey is planned so that members of the public can provide input. <http://www.jcaho.org/htba/hospitals/survey+process/public+information.htm>
Through its web site, JCAHO solicits complaints about accredited hospitals.
<http://www.jcaho.org/quality+check/guides/hos.htm>

The objective of accreditation is not merely for a hospital to pass the triennial survey. It is for the hospital to satisfy the standards all the time. A hospital is required to maintain records about its performance across time. <http://www.jcaho.org/htba/hospitals/survey+process/preparing+for+survey.htm>
Surveyors look for evidence that the hospital maintains procedures and resources for sustained compliance.

JCAHO maintains an independent affiliate named Joint Commission Resources. JCR provides confidential advice and education to hospitals, but JCAHO and JCR keep a Chinese wall between themselves. They do not share information as to the accreditation status of a hospital or the delivery of advice from JCR.
<http://www.jcaho.org/about+us/index.htm>

Is the schema model based on in internal or third party certification process?

JCAHO is a third-party accrediting body, and it employs its own examiners.

Define the liability framework associated with each named participant within the model, specifically as it applies to the certification and accreditation process.

JCAHO publishes a detailed policy on how it releases information (including certain information about performance and complaints) and which information it keeps confidential. The purpose of keeping some information confidential is to encourage candor on the part of surveyed hospitals.

<http://www.jcaho.org/lwapps/perprep/infplcy.htm>

In connection with the accreditation and performance reports that JCAHO publishes openly on its web site, there appear to be no disclaimers of liability. Evidently JCAHO has not sensed any exposure to liability to hospital customers reading report. JCAHO could easily publish a disclaimer that reduces potential liability.

Given that JCAHO publishes detailed policies on how it uses and discloses information, a hospital that participates in a survey implicitly agrees to those policies and cannot sue for defamation so long as the policies are followed.

Define the flow of money within the model, as it specifically applies to the certification and accreditation process (third party provider fees paid to the model owner for initial accreditation, third party continuing services/maintenance fees paid to the owner, identity issuer/relying party assessment fees paid to the third party auditor, identity issuer/relying party certification/accreditation fees paid to the owner).

A hospital pays a fee when JCAHO surveys it. The amount of fee varies depending on such factors as the size of the hospital.

<http://www.jcaho.org/htba/hospitals/cost+of+survey.htm>

Hospital customers do not pay JCAHO.

Define the dispute resolution process within the model, as it specifically applies to all named participants, within the certification and accreditation process.

When JCAHO cites a hospital for areas in which it can improve, the hospital is given time to show improvement.

Accreditation by JCAHO is a voluntary process. Revocation of accreditation is a blow to a hospital's reputation, but does not necessarily put the hospital out of business.

A revocation of state license could put a hospital out of business. Procedures for license and revocation vary from state to state, but normally state license law will provide an avenue for appeal if a state authority acts to revoke a license.

Define the decision making processes each model owner utilizes to develop and deploy their model.

JCAHO is a non-profit owned and controlled by leading members of the healthcare community. It sets standards based on community input. It communicates accreditation results by publication and by private consultation with subject hospitals.

State licensure of hospitals is normally government by a state regulatory agency.

Define the control/management processes each model owner utilizes to support their deployed model.

Hospitals are expected to set up internal teams to promote compliance with JCAHO standards. JCAHO, a third party industry association, then surveys hospitals for compliance. Apart from surveys, it also accepts and acts on complaints from the public.

Define the length of time that a third party auditor accreditation and/or identity issuer/relying party assessment and/or certification/accreditation would be valid for.

“To earn and maintain accreditation, an organization must undergo an on-site survey by a JCAHO survey team at least every three years.” <http://www.jcaho.org/about+us/index.htm>

JCAHO also performs random, unannounced surveys.
<http://www.jcaho.org/htba/hospitals/cost+of+survey.htm>

Model name: Closed Contractual Club

Representative of the model: SWIFT

Summary:

“SWIFT is the industry-owned cooperative supplying secure, standardised messaging services and interface software to 7,600 financial institutions in 200 countries. The SWIFT community includes banks, broker/dealers and investment managers, as well as their market infrastructures in payments, securities, treasury and trade.” http://www.swift.com/index.cfm?item_id=413225/25/2004

Historically, SWIFT’s physical infrastructure was an X.25 network (in other words, an EDI Value-Added Network). Recently SWIFT launched a more versatile IP network called SWIFTNet.

Historically, SWIFT membership was generally limited to financial institutions regulated by national governments. SWIFT has many categories of membership, but generally membership required status as a regulated entity and in some cases approval/sponsorship by a committee representing the membership candidate’s home country. See SWIFT corporate rules at http://www.swift.com/index.cfm?item_id=41961

Today, SWIFT has started to allow corporations to use SWIFTNet to communicate with one or more banks (but not with other corporations). In order for a corporation to participate, it must be sponsored by a member bank. Gianfranco Tabasso, “SWIFTNet – The Next Revolution in International Cash Management?”

www.treasury-management.com/Research/Byissues/03/jan03/Tabasso.pdf The sponsoring member bank is required under SWIFT Corporate Rule 2.3 to know and monitor the corporate participant. The member bank certifies to the SWIFT community the identity of the corporate participant.

http://www.swift.com/index.cfm?item_id=41961

In this model, permission to participate is based more on reputation, prestige and sponsorship than on the satisfaction of particular financial, technical or security criteria. This model is relevant to the present study because private parties in an authentication network may be satisfied with one another (or at least with some special participants) so long as each participant is sufficiently large, has enough reputation at stake or is sponsored by a qualified party.

For example, the network might be supported at its core by several well-established trade associations (e.g., US Chamber of Commerce), and the reputation of each association may be sufficient to justify its membership regardless of financial or technical criteria. In effect, the associations could decide each can participate based on mutual consent. What is more, each core trade association may be permitted to sponsor participation by particular corporations using standards selected by the association. In the

alternative, an association might be permitted to sponsor only, say, publicly-traded corporations with market capitalizations of at least \$2 billion.

The advantage of basing participation on reputation, recommendation, sponsorship and/or consent is that, in the proper environment, it is much more practical and efficient than requiring third-party audits and accreditation.

It may be possible that certain members of a network, based on reputation, recommendation or sponsorship, are expected to provide less in the way of audits or accreditation.

This model reminds us that rigid legal requirements and allocations of liability are not the only way to create an effective community among institutional peers.

Is the schema model based on internal or third party certification process?

It is based on reputation, recommendation or sponsorship.

Define the liability framework associated with each named participant within the model, specifically as it applies to the certification and accreditation process.

Contracts govern the division of operational liability among the SWIFT network and its members. But those contracts do not cover the subject of liability for the admission, recommendation or sponsorship of an unqualified party into the SWIFT community. Although the SWIFT by-laws and corporate rules provide procedures for admitting new participants, including sponsorship, recommendation and vote-based consent, they do not formally assign liability to entities that make mistakes in sponsoring, recommending or voting for participants. Still, under the by-laws participants may be expelled for such general matters as an “act of negligence which may be prejudicial to the interest of the Company.” SWIFT By-laws Article 13 d and General Terms and Conditions Clause 7.3. http://www.swift.com/index.cfm?item_id=7229

Define the flow of money within the model, as it specifically applies to the certification and accreditation process (third party provider fees paid to the model owner for initial accreditation, third party continuing services/maintenance fees paid to the owner, identity issuer/relying party assessment fees paid to the third party auditor, identity issuer/relying party certification/accreditation fees paid to the owner).

In order for a corporation to be sponsored by SWIFT member, the corporation will need to have a good relationship with the member. In practice, this means the corporation would have a banking relationship with the member substantial enough to justify the member going to the trouble, and risking its reputation, to sponsor the corporation.

Define the dispute resolution process within the model, as it specifically applies to all named participants, within the certification and accreditation process.

A member that sponsors a corporation is expected to have procedures for monitoring and presumably expelling the corporation if warranted.

The By-laws provide procedures for the board of directors to expel members with cause.

Define the decision making processes each model owner utilizes to develop and deploy their model.

Decision-making is a consultative process. Often, membership decisions are based on recommendations and input from industry representatives from a membership candidate's home country. Membership decisions are often based on votes and sponsorship.

Define the control/management processes each model owner utilizes to support their deployed model.

When a member sponsors a corporation, the member is responsible for monitoring the corporation and ensuring compliance with standards such as anti-money laundering laws. Shortcomings can lead to the withdrawal of sponsorship.

The SWIFT board of directors monitors the performance of members, and can expel members if cause is present.

Define the length of time that a third party auditor accreditation and/or identity issuer/relying party assessment and/or certification/accreditation would be valid for.

Monitoring occurs continually and expulsion can happen at any time.

/end/

Appendix B: E-Authentication Federation

Attachment 1: Draft Legal Document Suite, November 23, 2004

Attachment 2: Draft Legal Document Suite, October 14, 2005

Appendix

Included in the following pages is the current draft of the E-Authentication Federation's "Business Rules: E-Authentication Federation."

Version 1.0

November 23, 2004

FINAL DRAFT

Written by [Daniel Greenwood](#), Esq., with Input from Linda Elliott and RJ Schlecht

E-Authentication Business Rules Table of Contents

1. Title	1
2. Scope	1
2.1. Scope of Rules	1
2.2. Agreements and Conduct Outside Scope of Rules	1
2.3. Rules Appearing in Multiple Documents	1
3. Participation	1
3.1. Eligibility	1
3.2. Participation Requirements	1
3.2.1. Relying Parties	1
3.2.2. CSPs	1
3.2.3. End-Users	2
4. Roles and Obligations	2
4.1. GSA Role and Obligations	2
4.1.1. Operating Authorization	2
4.1.2. Promulgation and Amendment of Business Rules and Other Documents	2
4.1.3. Relying Party and CSP Approval	3
4.1.4. Service Offerings	3
4.1.4.1. Architectural Components	3
4.1.4.2. Interoperability Requirements	3
4.1.5. Contact Information	3
4.2. Relying Party Role and Obligations	3
4.2.1. Relying Party Participation Agreement	3
4.2.2. Interface Specification, Approved Software Use and Upgrade	3
4.2.3. Security and Privacy Compliance	4
4.2.4. Reasonable Reliance and Level of Assurance	4
4.3. CSP Role and Obligations	4
4.3.1. CSP Certification	4
4.3.2. CSP Participation Agreement	4
4.3.3. CSP Continuing Audit Requirement	4
4.3.4. Material Change to CSP, Credential Services or Credential	5
4.3.5. Interface Specification	5
4.3.6. End-User Notice Terms	5
4.4. General Obligations	5
4.4.1. Record Keeping	5
4.4.2. Federation Security and Reliability	5
4.4.3. Federation Interoperability	6
4.4.4. Operational and Ongoing Requirements	6
4.4.5. Authentication of Approved Parties	6
4.4.6. End-User Privacy	6
5. Enforcement	6
5.1. Dispute Resolution	6
5.2. GSA Investigation	7
5.2.1. Federation Participant Request for Investigation	7
5.2.2. GSA Initiated Investigation	7
5.3. Recourse	7
6. General Legal Terms	7
6.1. Limitation Of Liability	7
6.2. Governing Law	7

Federated Identity: Are We There Yet?

6.3. Order of Precedence.....	7
6.4. Assignment, Succession and Bankruptcy.....	8
6.5. Severability.....	8
6.6. Counterparts.....	8
6.7. Waiver.....	8
6.8. Responsibility For Taxes, Expenses.....	8
7. Interpretation and Amendment.....	8
Appendix 1. CSP Participation Agreement.....	9
Appendix 2. Relying Party Participation Agreement.....	11
Appendix 3. Business Rules Amendment Process.....	13
Appendix 4. General Overview.....	14
Appendix 5. Glossary.....	17
Appendix 6. Endnotes.....	19

Drafting Notes:

This document complies with the following drafting conventions. Where another document is referenced within this document, an endnote is provided with additional information about that document such as the citation, full formal name or a URL where it can be found. Where another section of the Business Rules is referenced from within the Business Rules, the title is capitalized (for example, when the remedies of section 5.3 are referenced, the term "Recourse" is used). Defined terms are also capitalized when used throughout the document. The definitions of such terms are contained in Appendix 5, the glossary. Defined terms include other parts of speech of the same word when that word has been capitalized in this document (for example, the words "Approved" and "Approve").

It is expected that this document will be used as a "template", meaning it will serve as an initial version that can be amended as the E-Authentication Federation evolves. To achieve clarity and ease of use, only the minimum necessary overlay of legal and contextual verbiage was included. Where possible, other documents containing additional more specific language have been included by reference. In addition, commercial terms and conditions customary in GSA contracts are expected to result from a future solicitation and procurement process in connection with the E-Authentication Federation.

The E-Authentication Federation Business Rules and Participation Agreements were prepared for the General Services Administration and drafted by Daniel J. Greenwood, Esq. with input from Linda Elliott and RJ Schlecht.

Business Rules
E-Authentication Federation
Version 1.0, 2004-NOV-23

1. Title

This document shall be known and may be cited as the "E-Authentication Federation Business Rules", or, as referenced herein, as "Business Rules".

2. Scope

2.1. Scope of Rules

Signatories to these Business Rules agree that these Business Rules govern participation in the E-Authentication Federation, administered by the General Services Administration of the U.S. Federal Government (GSA). The GSA, or its authorized agent, shall Certify Credential Services of a Credential Service Provider (CSP). Certified Credentials of a GSA Approved CSP may be accepted, validated and relied upon by GSA Approved Relying Parties. Such acceptance, validation or reliance need not require the use of any additional contract between an Approved CSP and an Approved Relying Party.

2.2. Agreements and Conduct Outside Scope of Rules

Nothing in these Rules shall be construed to prevent Approved CSPs and Relying Parties from executing such additional agreements among themselves as they see fit, including agreements covering the use of services, transactions or Credentials, including identity assertions or parts of such assertions. However, nothing in such additional agreement or services, transactions or Credentials covered by such agreement may conflict with any part of the Rules, processes or technologies specified or referenced in these Business Rules. Any activity covered by an addenda to the Participation Agreement, an addenda to these Business Rules or by any other contract or agreement other than the Participation Agreement or these Business Rules, is subject to the terms of that other agreement and is outside the scope of these Business Rules.

2.3. Rules Appearing in Multiple Documents

Any provision of these Business Rules that duplicates or emphasizes identical or similar provisions of other normative documents governing the E-Authentication Federation shall not be construed as to lessen the enforceability of any other provisions that have not been duplicated or emphasized.

3. Participation

3.1. Eligibility

The United States Federal Government or any State or Local government of the United States is eligible to become a CSP or a Relying Party under these Rules, provided it is a legal entity and the other requirements set forth in these Rules are satisfied. In addition, any legal entity, including a non-governmental organization, is eligible to become a CSP under these Rules, provided the other requirements set forth in these Rules are satisfied.

3.2. Participation Requirements

3.2.1. Relying Parties

Approval by the GSA is necessary for a Relying Party to participate in the EAuthentication Federation. A Relying Party must be a signatory to these Business Rules as a prerequisite to approval by the GSA. A party becomes a signatory Relying Party by executing the Relying Party Participation Agreement with GSA. Each such Relying Party Participation Agreement includes obligations whereby these Business Rules, as periodically amended, are incorporated by reference and consented to.

3.2.2. CSPs

Approval by the GSA is necessary for a CSP to participate in the E-Authentication Federation. A CSP must be a signatory to these Business Rules as a prerequisite to approval by the GSA. A party becomes

a signatory CSP by executing the CSP Participation Agreement with GSA. A CSP Participation Agreement may be executed directly with the GSA, or as part of a formal solicitation and procurement process the GSA may require. Each such CSP Participation Agreement includes obligations whereby these Business Rules, as periodically amended, are incorporated by reference and consented to.

A signatory CSP must also have one or more Credential Services Certified according to the applicable requirements of GSA, including the Credential Assessment Framework Suite (CAF)¹, and be added to the E-Authentication Federation Trusted Credential Service Provider List² as a prerequisite for Approval by GSA to participate in the EAuthentication Federation.

3.2.3. End-Users

Any party participating in the E-Authentication Federation as an End-User must have an agreement with an Approved CSP. Such agreement must contain such minimum terms as are required under these Business Rules and the CSP Participation Agreement. End-Users are considered participants in the E-Authentication Federation, but are not direct signatories to these Business Rules.

4. Roles and Obligations

4.1. GSA Role and Obligations

The General Services Administration of the United States Federal Government (GSA) is the party responsible for policy and operations related to the E-Authentication Federation. The GSA is responsible for defining and managing the roles, relationships and mutual obligations among parties operating in the E-Authentication Federation. The GSA uses Business Rules and Participation Agreements as a method of defining these roles, relationships and obligations in a formal and, as needed, enforceable manner. The GSA shall provide processes for determining qualification of any party in the E-Authentication Federation. In the course of such activities, as well as ongoing oversight of participant and system performance, the GSA shall act as coordinator and policy enforcement body for the E-Authentication Federation. The GSA may designate offices, departments or other organizational units within the GSA or otherwise within the United States Federal Government to exercise such rights or obligations defined under these Business Rules.

4.1.1. Operating Authorization

GSA actions in administering the E-Authentication Federation support the authentication component of the U.S. Federal Enterprise Architecture³. The President's Management Agenda of 2001⁴ directed GSA to lead the operation of the E-Authentication Federation, which implements OMB- M04-04⁵ and NIST SP 800-63⁶.

4.1.2. Promulgation and Amendment of Business Rules and Other Documents

GSA shall formalize and may amend these Business Rules pursuant to its duty to administer and manage the E-Authentication Federation. Amendments to these Business Rules must comply with the E-Authentication Federation Business Rules Amendment Process⁷. In addition to these Business Rules, the following materials are also formal normative documents defining rights, obligations, processes and other binding statements relative to the E-Authentication Federation: the CSP Participation Agreement, the Relying Party Participation Agreement, the Credential Assessment Framework⁸, the Technical Architecture⁹, the Interface Specification¹⁰ and the Relying Party Requirements Document.

4.1.3. Relying Party and CSP Approval

The GSA is responsible for determining whether to Approve a Relying Party for participation in the E-Authentication Federation. The GSA shall formalize and may amend periodically requirements for CSP Certification and is responsible for making approval decisions for participation in the E-Authentication Federation by Certified CSPs. The GSA shall formalize, maintain and update as needed a Trusted Credential Service Provider List¹¹ of Approved and Certified CSPs participating in the E-Authentication Federation. This list shall be a public document and include, at a minimum, the names of each CSP that has been successfully Certified, and the Level of Assurance of each Certified Credential Service of that CSP. The GSA shall determine what continuing audit and other compliance requirements shall satisfy maintenance of Certification and the terms of these Business Rules.

4.1.4. Service Offerings

To facilitate use of the E-Authentication Federation, the GSA will provide policies, various Architectural Components, business relationship management, Business Rules and Participation Agreements and other offerings.

4.1.4.1. Architectural Components

GSA may implement and make available to Approved Parties Architectural Components to facilitate use of the E-Authentication Federation, including the EAuthentication Portal identified in the Technical Architecture¹², Step-Down Translator(s), Schema Translator(s) and Validation Services. The GSA may incorporate additional components.

4.1.4.2. Interoperability Requirements

The GSA shall operate an interoperability laboratory for the purpose of testing interoperability of products, software, communication specifications and other relevant aspects of current and potential future enhancements to the EAuthentication Federation.

4.1.5. Contact Information

For current information related to the E-Authentication Federation and these Business Rules, contact the contact E-Authentication Program Director of the General Services Administration of the U.S. Federal Government or see <http://cio.gov/eauthentication/>.

4.2. Relying Party Role and Obligations

4.2.1. Relying Party Participation Agreement

A Relying Party is obliged to execute a Relying Party Participation Agreement as a prerequisite to approval for participation in the E-Authentication Federation. The current Relying Party Participation Agreement is included as Appendix 2.

4.2.2. Interface Specification, Approved Software Use and Upgrade

A Relying Party is obliged to comply with and use the E-Authentication Interface Specification¹³ to participate in, communicate through or connect with the EAuthentication Federation. A Relying Party is obliged to use software on the Approved Communications Software¹⁴ list or interface software otherwise approved by GSA. In order to maintain Approval to participate in the Federation, each Relying Party is obliged to follow requirements set by GSA to stay current with Approved Communications Software¹⁵.

4.2.3. Security and Privacy Compliance

The following Rules apply to any information system supporting the Agency Application of the Relying Party that is part of the U.S. Federal Government. An Approved Relying Party is obliged to comply with OMB Circular No. A-130¹⁶ including Appendix III to OMB Circular No. A-130¹⁷, with respect to any information technology system of the Relying Party.

An Approved Relying Party is obliged to comply with the Privacy Act of 1974¹⁸ and OMB Memorandum M-03-22¹⁹, including where required, performing a Privacy Impact Assessment with respect to the handling of personally identifiable information of an End-User.

An Approved Relying Party that is not part of the U.S. Federal Government must certify to the GSA that it is in compliance with equivalent safeguards and relevant requirements. GSA, in its discretion, shall determine whether such certification is sufficient.

4.2.4. Reasonable Reliance and Level of Assurance

A Relying Party is obliged to determine for itself whether to rely on the authentication status of an End-User and whether to authorize usage of the Agency Application. In order to determine the authentication status of an End-User, a Relying Party must:

. Determine for itself the level of Agency Application risk, and therefore the needed Level of Assurance, as per the guidance in OMB M-04-04²⁰ and NIST SP 800-63²¹, using the GSA-provided ERA tool or any other method it deems acceptable;

- . Determine communications or other interactions through the Federation are with Approved CSPs, in accordance with the Approved Party Authentication requirements in Section 4.4.5 of these Rules;
- . Determine that the Level of Assurance of an Approved Credential is not less than the Relying Party required Level of Assurance for its Agency Application; and
- . Determine that the credential is currently valid as per the E-Authentication Technical Architecture²², including, as relevant, the Interface Specification²³.

Communications and other interactions with a CSP or End-User by a Relying Party must comply with the requirements in this Section in order to be within the scope of the EAuthentication Federation and governed by these Business Rules.

4.3. CSP Role and Obligations

4.3.1. CSP Certification

An Approved CSP is obliged to achieve Certification and be added to the Trusted Credential Service Provider List²⁴. Certification is achieved upon successful completion of policy mapping, assessment of the CSP according to the CAFs²⁵ and operational testing.

4.3.2. CSP Participation Agreement

A CSP is obliged to execute a CSP Participation Agreement as a prerequisite to approval for participation in the E-Authentication Federation, thereby agreeing to abide by these Business Rules. The current CSP Participation Agreement is included as Appendix 1.

4.3.3. CSP Continuing Audit Requirement

An Approved CSP is obliged to undergo an audit, no less than annually, confirming compliance with continuing requirements arising out of Certification and with the obligations and other relevant terms of these Business Rules and the CAF²⁶. An audit planned or undergone by a CSP unrelated to the E-Authentication Federation may be sufficient to meet this requirement in whole or in part, in the discretion of the GSA.

4.3.4. Material Change to CSP, Credential Services or Credential

An Approved CSP may be required by the GSA to undergo an additional Certification in whole or in part, to re-Certify one or more Credential Services at the same or different Levels of Assurance or to accept Suspension or Termination of Certification and Participation in the E-Authentication Federation when audit results indicate material changes in the CSP, the Certified Credential Services or in the Credentials it issues or other relevant changes that bring the CSP out of compliance with continuing requirements.

4.3.5. Interface Specification

A CSP is obliged to comply with and use the E-Authentication Technical Architecture²⁷ to participate in, communicate through or connect with the E-Authentication Federation.

4.3.6. End-User Notice Terms

E-Authentication Federation End-User notice terms include agreement to maintain the security of each Approved Credential, including any Token housing each Credential, and to report to the appropriate authorities of the CSP or otherwise any known or reasonably suspected compromise of such Credential or Token.

Every Approved CSP is encouraged to assure the affirmative manifestation of assent by each End-User to E-Authentication Federation notice terms. Every Approved CSP is obliged to assure that each End-User has, at least, been given notice of and the opportunity to review E-Authentication Federation End-User notice terms

4.4. General Obligations

Every Approved Relying Party and Approved CSP (Approved Party) is obliged to comply with the following Rules.

4.4.1. Record Keeping

Any Approved Party may be requested to transmit to GSA transaction information for the purpose of investigating and correcting interoperability issues that may arise between parties operating in the E-Authentication Federation. In addition, every Approved Party, in order to facilitate GSA resolution of disputes under Section 5 of these Business Rules, is obliged to keep records sufficient to preserve relevant evidence of the facts related to the dispute in question. To the extent that information identified in this Section constitutes Personally Identifiable Information within a System of Records under the Privacy Act of 1974²⁸, nothing in this section shall be construed to authorize or permit the communication of such information about an End-User without that End-User's informed consent.

4.4.2. Federation Security and Reliability

Every Approved Party agrees to coordinate with the GSA in safeguarding the security and reliability of the E-Authentication Federation. GSA may render inaccessible any Architectural Component of the E-Authentication Federation to prevent or cease serious harm to the Federation. Every Approved Party agrees the GSA reserves the right to suspend participation by any Participant in the E-Authentication Federation in accordance with the E-Authentication Federation Participation Suspension Policy²⁹, and only under extraordinary circumstances necessary to prevent or cease serious harm to the EAuthentication Federation.

To assure the reliable operation of the E-Authentication Federation, every Approved Party must inform GSA through appropriate channels of any material change in a web site, use of an Architectural Component or other technology or business modification that can reasonably be expected to disrupt, significantly delay or prevent communications through the Federation. This notice must occur in a timely manner prior to the date of any such planned modification.

4.4.3. Federation Interoperability

To assure the efficacy and operation of the E-Authentication Federation, every Approved Party must demonstrate to the GSA that its interactions and communications through the Federation comply with the E-Authentication Technical Architecture³⁰ and will interoperate with the architectural components of the Federation. To this end, every Approved Party must conduct tests of its planned Federation interactions and communications in the Interoperability Lab, or through such other process GSA may designate, to demonstrate compliance and interoperability requirements for the Federation have been met.

4.4.4. Operational and Ongoing Requirements

Every Approved Party is obliged to comply with application, testing, piloting, production and continuing maintenance requirements set forth by the GSA. These ongoing requirements include continued compliance with the provisions of the CAF³¹ and with applicable requirements documents defining operational sufficiency for participation in the E-Authentication Federation. Nothing in this section, however, shall be construed to prevent any Approved Party from extending, adding to or otherwise applying other technologies or services in accordance with Section 2.2 of these Rules.

4.4.5. Authentication of Approved Parties

Communications through the E-Authentication Federation are subject to mandatory authentication by the communicating Approved Parties to prevent participation in the Federation by non-Approved Relying Parties or CSPs. To this end, Approved Parties must implement and comply with the E-Authentication Federation Technical Architecture³² specifications for authenticating approved parties.

4.4.6. End-User Privacy

Every Approved Party is obliged to assure that each End-User has provided Informed Consent to the sharing of any personally identifiable information related to the End-User by the Approved Party with any other party operating within the E-Authentication Federation, including any personally identifiable information contained in a certificate or other identity assertion as included in the Interface Specification. Under these Business Rules, no Approved CSP or Approved Relying Party is permitted to share

personally identifiable information about an End-User beyond the information provided for in the Interface Specification.

5. Enforcement

5.1. Dispute Resolution

Every Approved Party agrees to attempt in a timely manner to resolve any dispute arising out of or related to the application of these Business Rules or the Participation Agreement executed by that Approved Party in good faith with the other disputants and parties related to the dispute. Each such dispute, the date and successful or attempted resolutions, including changes in policy, practices or technology implementation, shall be reported to the GSA in a timely manner.

To the extent that information identified in this Section constitutes Personally Identifiable Information within a System of Records under the Privacy Act of 1974³³, nothing in this section or any sub-section shall be construed to authorize or permit the communication of such information about an End-User without that End-User's informed consent.

In the event parties to a dispute are unable, despite their best good faith efforts, to resolve a dispute among themselves, any party may request GSA investigate the dispute potentially leading to Recourse for the aggrieved party.

5.2. GSA Investigation

GSA shall respond to every request to investigate a dispute in a timely manner. GSA may request additional information from one or more parties to the dispute.

5.2.1. Federation Participant Request for Investigation

In the event good faith efforts to resolve a dispute are not successful among the disputants and other parties, any Participant in the E-Authentication Federation may request that GSA investigate the matter, propose a resolution and, if necessary arbitrate a resolution of the matter. Each such request must be accompanied by a full report of all the relevant information related to the dispute.

5.2.2. GSA Initiated Investigation

GSA may initiate an investigation based upon the request of any Participant in the EAuthentication Federation, or may initiate an investigation whenever it deems appropriate based on any information it regards as relevant and credible. Without limitation, such information may include reasonable suspicion that an Approved Party is not in compliance with continuing obligations required under these Business Rules.

5.3. Recourse

Based upon the results of its investigation and in accordance with the E-Authentication Federation Participation Suspension Policy³⁴, and only under extraordinary circumstances necessary to prevent or cease serious harm to the E-Authentication Federation, the GSA may suspend participation of any Participant in the E-Authentication Federation or render inaccessible any Architectural Component of the Federation by one or more Participants. If the result of an Investigation indicates that an Approved Party is not in compliance with any requirement included directly or by reference under these Business Rules, GSA may require such additional audit, re-Certification or Certification at different Levels of Assurance, to the extent necessary to prevent or cease serious harm to the Federation.

6. General Legal Terms

6.1. Limitation Of Liability

Recourse against the United States for damage caused by negligence of a government employee is controlled by the Federal Tort Claims Act³⁵, 28 USC Section 1346 et seq. A non-governmental Approved CSP operating in accordance with the terms of the CSP Participation Agreement and these Business Rules may assert the government contractor defense to tort claims arising under the CSP Participation Agreement and these Business Rules.

There shall be no Recourse for any claim arising out of or in relation to use of or reliance upon an Approved Credential or the E-Authentication Federation against any Approved Party under any theory of liability, beyond the Recourse available under the Federal Tort Claims Act³⁶, unless agreed by contract among the relevant parties.

6.2. Governing Law

These Business Rules and any related materials governing the E-Authentication Federation shall be construed and adjudicated according to the laws of the United States of America.

6.3. Order of Precedence

In the event of a conflict between the terms of various E-Authentication Federation related documents, each such document shall be accorded the following order of priority: the Participation Agreement shall be construed to prevail over conflicting terms of any other E-Authentication Federation document, followed in order of precedence by the terms of these Business Rules, followed by the terms of any normative document listed in Section 4.1.2 of these Rules, followed by the terms of any other policies, agreements or other materials formally promulgated for the purpose of documenting legal terms governing participation in the E-Authentication Federation.

6.4. Assignment, Succession and Bankruptcy

No Approved Party may sell, rent, lease, sublicense, assign, grant a security interest in or otherwise transfer any right and/or obligation contained in these Business Rules or the Participation Agreement executed by that Approved Party, except as permitted herein. Any Approved Party may request of GSA permission for assignment or succession to a different party, including a creditor of the Approved Party, of part or all of the rights and/or obligations contained in these Business Rules or the Participation Agreement executed by that Approved Party.

6.5. Severability

If any provision, set of provisions or part of a provision of these Business Rules is held to be unenforceable or otherwise invalid in whole or in part, the remaining provisions shall remain in full force and effect and shall be construed to the maximum extent practicable as a consistent and reasonable entire agreement.

6.6. Counterparts

These Business Rules may be executed as an agreement simultaneously in one or more counterparts, each of which shall be deemed to be an original, but all of which together shall constitute one and the same instrument.

6.7. Waiver

Neither party's failure to enforce strict performance of any provision of these Business Rules will constitute a waiver of a right to subsequently enforce such a provision. No written waiver shall constitute, or be construed as, a waiver of any other obligation or condition of these Business Rules.

6.8. Responsibility For Taxes, Expenses

Each Approved Party agrees that it is solely responsible for the payment of taxes or expenses incurred by that Approved Party arising out of or related to participation in the EAuthentication Federation.

7. Interpretation and Amendment

The terms of these Business Rules shall be interpreted by the GSA so as to avoid conflict or inconsistencies between the various provisions and between these Business Rules, applicable Participation Agreements and other relevant E-Authentication Federation materials. These Business Rules may be amended according to the E-Authentication Federation Business Rules Amendment Process³⁷, however no such amendment shall go into legal effect earlier than 90 days from the time notice is afforded to Approved Relying Parties and Approved CSPs. Notice may be provided of amendment to these Business Rules and other matters related to the operation of the E-Authentication Federation by electronic mail to the contact person(s) indicated for each

Approved Party and by posting to the E-Authentication Federation web site.

Appendix 1
E-Authentication Federation
CSP Participation Agreement

Version 1.0, 2004-NOV-23

Drafted by [Daniel Greenwood](#), Esq.

[personal email and telephone redacted in public draft and replaced by URL]

<http://www.civics.com>

1. Recitals

This Participation Agreement constitutes the legal basis for an organization to become a Credential Service Provider (CSP) within the E-Authentication Federation.

2. Parties

The parties to this Participation Agreement are the General Services Administration of the United States federal government (GSA) and _____ (CSP).

3. Agreement to Abide by Business Rules

By signing this Participation Agreement, the CSP agrees to abide by the E-Authentication Federation Business Rules, as in effect during the period of CSP participation in the E-Authentication Federation, and which are expressly incorporated into and make a part of this Agreement.

4. Dispute Resolution: Notice, Investigation, Resolution and Recourse

CSP agrees that the E-Authentication Business Rules Dispute Resolution and Recourse provisions cover issues between Approved CSPs and Relying Parties operating in the Federation. Any dispute resolution process and rules between the CSP and an End-User must be defined and pursued between the CSP and the End-User, and such terms are not within the scope of the Business Rules of this Participation Agreement.

5. Termination and Suspension

The terms of this Participation Agreement and the Business Rules cease to apply to any CSP as of the effective date of termination of Participation in the E-Authentication Federation.

5.1. Voluntary

Participation in the E-Authentication Federation may be terminated by CSP through written notice to GSA, to avoid the imminent effect of amended language to the Business Rules. Such notice shall be effective no less than 30 calendar days from the date of receipt by GSA. Participation in the E-Authentication Federation may be terminated by mutual agreement between the GSA and CSP.

5.2. Involuntary

GSA may suspend the participation of CSP in the E-Authentication Federation, in accordance with the E-Authentication Federation Participation Suspension Policy³⁸, under extraordinary circumstances necessary to prevent or cease serious harm to the E-Authentication Federation. GSA may terminate the participation of CSP in the E-Authentication Federation in writing for cause, including breach by the CSP of the terms of this Participation Agreement or the Business Rules.

6. Confidentiality and Non-Disclosure

GSA agrees to execute any reasonable confidentiality and/or non-disclosure agreements with the CSP that may be required as a condition of accepting credentials of that CSP and according to the Business Rules. GSA further agrees to require consent to the relevant terms of such agreements by any Relying Party to whom the terms may apply.

7. Legal Terms

7.1. Limitation Of Liability

Recourse against the United States for damage caused by negligence of a government employee is controlled by the Federal Tort Claims Act³⁹, 28 USC Section 1346 et seq. A non-governmental Approved CSP operating in accordance with the terms of this CSP Participation Agreement and the E-Authentication Federation Business Rules may assert the Government Contractor Defense to tort claims arising under this CSP Participation Agreement and the E-Authentication Federation Business Rules.

There shall be no Recourse for any claim arising out of or in relation to use of or reliance upon an Approved Credential or the E-Authentication Federation against any Approved Party under any theory of liability, beyond the Recourse available under the Federal Tort Claims Act⁴⁰, unless agreed by contract among the relevant parties.

7.2. Governing Law

This CSP Participation Agreement and any related materials governing the E-Authentication Federation shall be construed and adjudicated according to the laws of the United States of America.

7.3. Integration and Order of Precedence

This CSP Participation Agreement and the E-Authentication Federation Business Rules constitute the entire agreement of the parties with respect to participation in the E-Authentication Federation. In the event of a conflict between the terms of various E-Authentication Federation related documents, documents shall be accorded the following order of priority: This CSP Participation Agreement shall be construed to prevail over the terms of any other document, followed in order of precedence by the terms of the E-Authentication Federation Business Rules, followed by the terms of any other policies, agreements or other materials formally promulgated for the purpose of documenting legal terms governing participation in the E-Authentication Federation.

7.4. Assignment, Succession and Bankruptcy

CSP agree it may not sell, rent, lease, sublicense, assign, grant a security interest in or otherwise transfer any right and/or obligation contained in this CSP Participation Agreement or the E-Authentication Federation Business Rules except as permitted herein. CSP may request of GSA permission for assignment or succession to a different party, including a creditor of the CSP, of part or all of the rights and/or obligations contained in this CSP Participation Agreement or the E-Authentication Federation Business Rules. Any prohibited assignment shall be null and void.

7.5. Severability

If any provision, set of provisions or part of a provision of this CSP Participation Agreement is held to be unenforceable or otherwise invalid in whole or in part, the remaining provisions shall remain in full force and effect and shall be construed to the maximum extent practicable as a consistent and reasonable entire agreement.

7.6. Responsibility For Taxes, Expenses

CSP agrees that it is solely responsible for the payment of taxes or expenses incurred by the CSP arising out of or related to participation in the E-Authentication Federation.

8. Amendment

This Participation Agreement may be amended by agreement of the parties, reflected by a signed writing.

9. Signatures

CSP

GSA

Appendix 2
E-Authentication Federation
Relying Party Participation Agreement

Version 1.0, 2004-NOV-23

Drafted by [Daniel Greenwood](#), Esq.

[personal email and telephone redacted in public draft and replaced by URL]
<http://www.civics.com>

1. Recitals

This Relying Party Participation Agreement constitutes the legal basis for an organization to become a Relying Party within the E-Authentication Federation.

2. Parties

The parties to this Participation Agreement are the General Services Administration of the United States federal government (GSA) and _____ (Relying Party).

3. Agreement to Abide by Business Rules

By signing this Participation Agreement, the Relying Party agrees to abide by the EAuthentication Federation Business Rules, as in effect during the period of participation in the EAuthentication Federation, and which are expressly incorporated into and make a part of this Agreement.

4. Compliance With Requirements

Relying Party agrees that satisfactory completion of the GSA Relying Party Requirements Document, including confirmation of required privacy, regulatory compliance and technical practices, is a pre-requisite to participation in the E-Authentication Federation and must be finalized approval for inclusion in the E-Authentication Federation. Relying Party agrees to maintain continuing compliance with the requirements and other terms contained in the EAuthentication Federation Business Rules, including compliance with the technical, policy and procedural documents incorporated by reference in the E- Authentication Federation Business Rules.

5. Dispute Resolution: Notice, Investigation and Resolution

Relying Party agrees that the E-Authentication Business Rules Dispute Resolution and Recourse provisions cover issues between Approved CSPs and Relying Parties operating in the Federation. Any dispute resolution process and rules between the Relying Party and an End-User must be defined and pursued between the Relying Party and the End-User, and such terms are not within the scope of the Business Rules of this Participation Agreement.

6. Termination and Suspension

The terms of this Participation Agreement and the Business Rules cease to apply to any Relying Party as of the effective date of termination of Participation in the E-Authentication Federation.

6.1. Voluntary

Participation in the E-Authentication Federation may be terminated by written notice to GSA, to be effective no less than 30 calendar days from the date of receipt by GSA. Participation in the E- Authentication Federation may be terminated by mutual agreement between the GSA and Relying Party.

6.2. Involuntary

GSA may suspend the participation of any Relying Party in the E-Authentication Federation in accordance with the E-Authentication Federation Participation Suspension Policy⁴¹, and only under extraordinary circumstances necessary to prevent or cease serious harm to the EAuthentication Federation.

7. Confidentiality and Non-Disclosure

Relying Party agrees to execute any reasonable confidentiality and/or non-disclosure agreements participating CSPs may require as a condition of accepting credentials of that CSP and according to the Business Rules.

8. Liability

There shall be no Recourse for any claim arising out of or in relation to use of or reliance upon an Approved Credential or the E-Authentication Federation against any Approved Party under any theory of liability, beyond the Recourse available under the Federal Tort Claims Act⁴², unless agreed by contract among the relevant parties.

9. Amendment

This Participation Agreement may be amended by agreement of the parties, by a signed, writing.

10. Signatures

Relying Party
14

GSA

Appendix 3

E-Authentication Federation Business Rules Amendment Process

Version 1.0, 2004-NOV-23

The E-Authentication Federation Business Rules may be amended according to the following process. Any Approved CSP or Relying Party may certify a request for consideration of a proposed Amendment of the Business Rules to the GSA, including the reasons therefor and proposed amended language. Any such proposed Amendment shall trigger the Consultative Amendment Process, defined below. The GSA may also propose an Amendment triggering the Consultative Amendment Process.

Consultative Amendment Process

Notice of a proposed Amendment requested by an Approved Party, no later than 30 days from the time the request is received by the GSA, shall be communicated to each Approved Party in the E-Authentication Federation for consideration and comment. Said notice shall be delivered by e-mail to the named contact person(s) in the Participation Agreements of the Approved Parties and may also be posted to the official E-Authentication Federation web site. A period of not less than 30 days shall be afforded Approved Parties to consider, comment upon and, at their discretion, indicate agreement with, disagreement with and/or alternative proposed language to the GSA. The GSA may hold one or more consultative meetings of interested Approved Parties to discuss any proposal and may extend the period for consideration and comment, as needed to accommodate the needs of the parties.

Disposition of Amendment Proposal

No more than 10 days after the period for consideration and comment has closed, the GSA shall communicate to each Approved Party notice of the disposition of the proposal, including whether the proposal has been rejected and no Amendment will be pursued, or the proposal has been modified, or the proposal has been accepted. Said notice shall be delivered by e-mail to the named contact person(s) in the Participation Agreements of the Approved Parties and may also be posted to the official E-Authentication Federation web site. If the proposal is modified, the modified proposal shall trigger a new Consultative Process, defined above. If the proposal is accepted, it shall trigger the Amendment Incorporation Process defined below.

Amendment Incorporation Process

An Amendment that has been accepted after a Consultative Amendment Process according to the notice provisions specified in the Disposition of Amendment Proposal process shall go into legal effect no less than 90 days from the date notice has been sent, or such later time as specified in the notice. Any Approved Party may terminate participation in the E-Authentication Federation no less than 30 days from the time of sending notice of termination to the GSA according to the Business Rules, and in every case reserves the right to terminate participation prior to any Amendment coming into full force and effect.

Appendix 4

General Overview

Version 1.0, 2004-NOV-23

The E-Authentication Federation is designed to allow electronic access to government services by examining electronic credentials to verify the End-User's identity. This Federation is run by the General Services Administration of the U.S. Federal Government under the name of the EAuthentication Initiative. The E-Authentication Initiative is one of twenty-four Electronic Government (E-Gov) services from the President's Management Agenda, which is intended to improve interfaces between citizens, businesses, and all levels of government.

The credentials may be issued by government agencies, but may also be issued by commercial entities for this purpose or for other purposes. In those cases, the E-Authentication Federation would be providing for reliance on commercially-issued, re-usable credentials. The EAuthentication Federation, including public and private organizations, uses such credentials along with a common technical, policy and legal infrastructure. These Business Rules, and the related Participation Agreements form the cornerstone of the legal aspect of the infrastructure. The Federal Government, in order to support the electronic government initiatives, is undertaking the E-Authentication initiative to allow for federation of identity and creating federation for the government and other entities so that citizens can authenticate to the government. The EAuthentication Federation requires policy and technology infrastructure as well as business rules and participation agreements. The technology infrastructure includes Architectural Components such as a validation service, a discovery portal, a step-down translator and a protocol translator. These components make it possible for parties using different technologies to federate identities from one organization to another. The E-Authentication Federation is the authentication component of the federal enterprise architecture.

The E-Authentication Federation has these key participants: Credential Service Providers (CSPs), End-Users, Relying Parties who are operating Agency Applications (RPs), and the General Services Administration of the U. S. Government, who acts as the administrative, operational, and policy arm of the E-Authentication Federation. End-Users, who will use credentials to access Agency Applications may be government employees or contractors or private citizens who are affiliated with one or more CSPs. That affiliation could include a customer, employee or partnership relationship. Relying Parties may include government agencies at the Federal, State, or local levels.

Credential Service Providers issue credentials to End-Users, who in turn use those credentials to get access to Government services over the world wide web. The E-Authentication Initiative facilitates this process through its service model, which includes policy services, technology services, and customer service.

The E-Authentication Federation utilizes industry standard technologies, implemented through Commercial Off the Shelf Products (COTS). Use of Approved COTS Software is required of all Approved CSPs, Relying Parties and for all communications occurring through the EAuthentication Federation. A complete explanation of the technical architecture is available in the publication 'Technical Approach for the Authentication Service Component'. The architecture supports the concept of credentials at each of four Assurance Levels, allowing the Relying Party to match their acceptance of credentials to the Risk Assessment they will have completed for their Agency Application. Risk assessment guidance is contained in OMB M-04-04⁴³. Guidance for credentials at each of the four assurance levels is contained in NIST SP 800-63⁴⁴.

The E-Authentication Federation uses the Security Assertion Markup Language (SAML) and also PKI as enabling technologies allowing for federation of credentials across organizations in both the public and private sectors. Any CSP in the private or public sector issuing credentials that comply with the SAML standard when configured in accordance with the GSA issued Interface Specification can be considered for Approval by GSA to participate in the E-Authentication Federation at Assurance Levels 1 and 2. In

addition, the CSPs operating within the Federal Public Key Infrastructure, PKI Bridge, and issuing credentials under the ACES, FICC, and FPKIPA programs can also be considered for participation at any Assurance Level. Any CSP, whether a provider of SAML or PKI based credentials, must execute a Participation Agreement legally binding it to the E-Authentication Business Rules in order to be Approved for participation. Other technical standards and specifications may be accepted for use within the E-Authentication Federation as they become available at the sole discretion of the GSA.

Both CSPs and RPs will need to meet a number of requirements for participation in the EAuthentication Federation. Guidance on these requirements is contained in documents published by the GSA including E-Authentication Handbook for Federal Government Agencies, EAuthentication Handbook for Credential Service Providers, and the E-Authentication Cookbook. The GSA evaluates the qualifications of potential participants, assists them in matriculating through the qualification, testing, and activation process, and maintains oversight of the EAuthentication Federation operation. In addition, the GSA operates a conformance testing service for COTS products, an interoperability testing service, and runs some technical services that are designed to lessen the technical burden on the participants.

These Business Rules are intended to define the legal terms and overall structure, including roles and obligations governing participation in the E-Authentication Federation. CSPs and Relying Parties sign Participation Agreements which obligate them to the terms of these rules as well as the policies of the GSA. End-Users, while considered participants, do not sign Participation Agreements directly with GSA. Rather, End-Users sign agreements containing approved E-Authentication Federation terms with the CSP who has issued and Approved Credential to that user. Details of operational processes are contained in GSA documents, including the ones referenced above, and many more that are relevant to various aspects of EAuthentication Federation participation, such as interoperability testing. Documents are available through the E-Authentication Federation website at <http://www.cio.gov/eauthentication/>

The following diagram illustrates the organizations which oversee the E-Authentication Federation within the US Government, and the major areas of responsibility for both policy (within the Office of Government-wide Policy) and operations (within the Project Management Office or PMO) for the E-Authentication Federation.

Federal E-Authentication Initiative Overview

In 2001, President Bush initiated several government reform efforts, collectively known as the President's Management Agenda (PMA). The five government-wide efforts focus on Strategic Management of Human Capital, Competitive Sourcing, Improved Financial Performance, Expanded Electronic Government, and Budget and Performance Integration. The Chief Information Officers (CIOs) of the federal agencies have a major role in the achievement of the PMA goals. They lead the implementation of many of the programs that help expand electronic government and provide support to others.

CIO Council contributed to several government-wide initiatives, focusing on reducing costs and improving services to citizens. To facilitate efforts to transform the Federal Government the Office of Management and Budget (OMB) is developing the Federal Enterprise Architecture (FEA), a business-based framework for Government-wide improvement.

Operating under the authority of the OMB, the General Services Administration (GSA) is responsible for the Federal government's electronic authentication effort. Whether through electronic authentication evolution or historical events the Federal Enterprise Architecture is a combination of pre-PMA and new efforts. The Federal government established several significant efforts related to electronic authentication, prior to creation of the Electronic Authentication Initiative. These efforts include Federal Public Key Infrastructure (FPKI), Access Certificates for Electronic Services (ACES), Federal Identity Credentialing Committee (FICC). The E-Authentication Initiative (EAI) provides for incorporation of these prior efforts into the e-Authentication Federation...

Federal e-Authentication Diagram

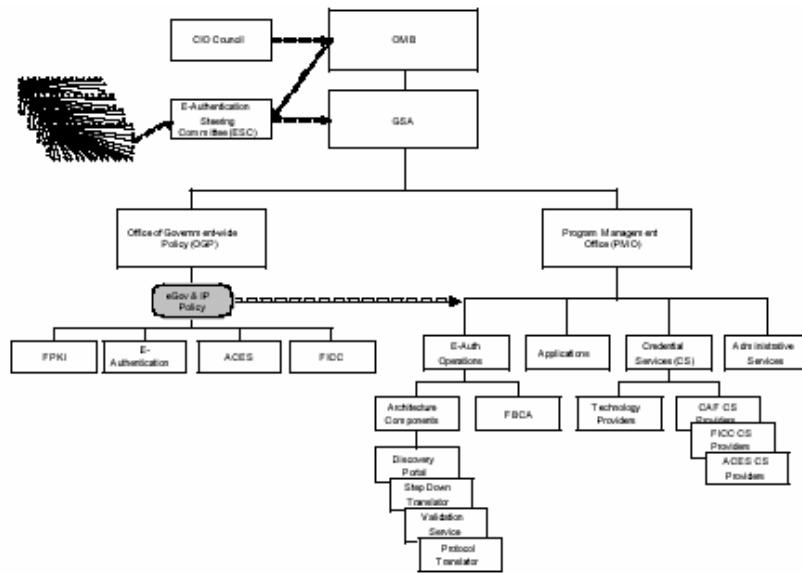


Diagram 1

The Federal authentication architecture is basically divided into two functional areas, policy and operations. Within both policy and operations there are various initiatives to meet the diverse demands of the government. These include historical agency authentication services, various levels of identity assurance, private sector COTS, technical interoperability, and compliance. Please note that this overview uses terms that are not defined and does not use every defined term according to its formal definition. Rather, the document was written for readability and to provide an informal basis to generally understand the overall initiative at a glance.

Appendix 5

E-Authentication Business Rules Glossary

Version 1.0, 2004-NOV-23

Agency Application

A computer applications of a Relying Party that is uniquely identifiable when used within the E-Authentication Federation.

Approved

Authorization or other acceptance by the GSA for purposes of participation or other inclusion or use in the E-Authentication Federation.

Approved Credential

A Credential issued by a Certified Credential Service of an Approved Credential Service Provider to an End-User.

Approved Credential Service Provider (Approved CSP)

A Credential Service Provider that has been approved by the GSA to participate in the EAuthentication Federation.

Approved Parties

Any Approved Relying Party and Approved Credential Service Provider.

Approved Relying Party

A Relying Party that has been approved by the GSA to participate in the E-Authentication Federation.

Certified Credential Service

A Credential Service judged to meet the requirements identified in the Credential Assessment Framework Suite.

Credential

Digital information used in authentication and access control that bind an identity or an attribute to an End-User's Token or some other property such as his or her current network address. Note that this glossary distinguishes between Credentials, and Tokens while other documents may use the terms interchangeably.

Credential Service

A service of a Credential Service Provider that provides credentials to subscribers for use in electronic transactions. If a Credential Service Provider offers more than one type of credential then each one is considered a separate Credential Service.

Credential Service Provider

An organization that offers one or more Certified Credential Services, also known in this document as a CSP.

End-User

An individual person that has been issued an Approved Credential by an Approved Credential Service Provider and who communicates through the E-Authentication Federation with an Approved Relying Party and whose identity is verifiable with reference to that Credential.

Informed Consent

Consent voluntarily signified by an End-User who is competent and who understands the terms of the consent and who has been provided in a clear statement with the appropriate knowledge needed to freely

decide without the intervention of any element of force, fraud, deceit, duress, over-reaching or other ulterior form of constraint or coercion.

Levels of Assurance

Four levels of authentication defined based upon consequences of a false positive authentication or misuse of a Credential. These levels are documented in OMB Memorandum M-04-04.

Participant

Any Approved Relying Party, Approved Credential Service Provider or End-User.

Relying Party

A party that relies upon a Credential issued by a Credential Service Provider.

Relying Party Requirements Document

This document contains the checklist of items necessary for a Relying Party to be approved by GSA for participation in the E-Authentication Federation.

Rule

A provision or term of the E-Authentication Business Rules.

Security Assertion Markup Language (SAML)

The XML Schema specified by the open standards organization OASIS-OPEN defining a standard framework for creating and exchanging security information between online partners. The specification, and other information provided by the authoring technical committee, may be found at:

http://www.oasisopen.org/committees/workgroup.php?wg_abbrev=security.

Technology Architecture Components

Inclusive of the portal defined in the E-Authentication Federation Technology Architecture, the step-down translator, validation services and the protocol translator.

Token

Something that the End-User possesses or knows (typically a key or password) that can be used to remotely authenticate the claimant's identity. Technically, the Token includes a userid and password that ensures Token uniqueness within a Credential domain.

Appendix 6

E-Authentication Business Rules Endnotes

Version 1.0, 2004-NOV-23

¹ Credential Assessment Framework Suite (CAF)

The GSA published documents defining a process for the Certification of Credential Services of Credential Service Providers, including the Interim PKI Credential Assessment Profile, Interim Password Credential Assessment Profile, Interim PIN Credential Assessment Profile, Interim Credential Assessment Framework, Interim Credential Assessment Guidance and Interim Common Credential Assessment Profile. This suite of documents collectively can be found at <http://cio.gov/eauthentication/CredSuite.htm>.

² E-Authentication Federation Trusted Credential Service Provider List

The list of Certified Credential Services and their associated Levels of Assurance. This list is published at <http://cio.gov/eauthentication/TCSList.htm>.

³ U.S. Federal Enterprise Architecture

A business and performance-based framework to support cross-agency collaboration, transformation, and government-wide improvement, including reference models for business, service components, data, and a technical reference model. Information about this architecture, and the architecture itself, can be found at: <http://www.feapmo.gov/>.

⁴ President's Management Agenda

A collection of government reform efforts initiated in 2001 including strategic management of human capital, competitive sourcing, improved financial performance, expanded electronic government and budget and performance integration. Information about these initiatives can be found at:

http://www.cio.gov/documents/CIO_Council_Strategic_Plan_FY04.pdf.

⁵ OMB Memorandum M-04-04

This document is published by OMB regarding e-authentication guidance for federal Agencies. This document can be found at:

<http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>.

⁶ NIST SP 800-63

This document is published by the National Institute of Standards and Technology entitled Electronic Authentication Guideline. This document can be found at:

http://cio.gov/eauthentication/documents/SP800-63V6_3_3.pdf.

⁷ E-Authentication Federation Business Rules Amendment Process

Definition of the circumstances and procedures necessary to formally amend the EAuthentication Federation Business Rules. This document can be found in Appendix 3 of the Business Rules.

⁸ See note 1.

⁹ E-Authentication Federation Technical Architecture

Suite of documents defining required implementations and configurations of technology for use in the E-Authentication Federation, including the Interface Specification relevant to use of SAML and path discovery and validation requirements relevant to PKI. This suite of documents can be found at: <http://cio.gov/eauthentication/TechSuite.htm>.

¹⁰ Interface Specification

Interface specifications for the SAML Artifact Profile for use in the E-Authentication Federation. This document can be found at:

<http://cio.gov/eauthentication/documents/SAMLspec.pdf>.

¹¹ See note 2.

¹² See note 9.

¹³ See note 10.

¹⁴ Approved Communication Software

Software approved by the GSA for communications through the E-Authentication Federation. The list of such software, along with the technology providers of those

products, can be found at:

<http://www.cio.gov/eauthentication/documents/ApprovedProviders.htm>

¹⁵ See note 14.

16 OMB Circular No. A-130

This document is published by OMB regarding the management of federal information resources. This document can be found at:

<http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html>.

¹⁷ **OMB Circular No. A-130, Appendix III**

This document is published by OMB regarding security of federal automated information resources. This document can be found at:

http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html.

¹⁸ **Privacy Act of 1974**

Federal legislation defining allowed federal collection, use or dissemination of personal information. This legislation may be cited as 5 USC § 552a, and can be found at:

http://www.law.cornell.edu/uscode/html/uscode05/usc_sec_05_00000552--a000-.html.

¹⁹ **OMB Memorandum M-03-22**

This document is published by OMB regarding guidance for implementing the privacy provisions of the e-government act of 2002. This document can be found at:

<http://www.whitehouse.gov/omb/memoranda/m03-22.html>.

²⁰ See note 5.

²¹ See note 6.

²² See note 9.

²³ See note 10.

²⁴ See note 2

²⁵ See note 1.

²⁶ See note 1.

²⁷ See note 9.

²⁸ See note 18.

29 E-Authentication Federation Participation Suspension Policy

A policy defining the extraordinary circumstances under which an Approved Party may have participation in the Federation suspended. As of the date of publication of version 1 of the E-Authentication Business Rules, this document is not yet finalized.

³⁰ See note 9.

³¹ See note 1.

³² See note 9.

³³ See note 18.

³⁴ See note 29.

35 Federal Tort Claims Act

Federal legislation defining U.S. Federal Government liability under tort law. This legislation may be cited as 28 USC § 1346 et seq. and can be found at:

http://www.law.cornell.edu/uscode/html/uscode28/usc_sup_01_28_10_VI_20_171.html.

³⁶ See note 35.

³⁷ See note 7.

³⁸ See note 29.

³⁹ See note 35.

⁴⁰ See note 35.

⁴¹ See note 29.

⁴² See note 35.

⁴³ See note 5.

⁴⁴ See note 6.



E-Authentication Federation Interim Legal Document Suite

Version 4.0.7
10/14/05

Release Notes

Effective October 14, 2005.



Document History

Status	Release	Date	Comment	Audience
Draft	0.0.1	8/15/05	Initial draft release.	Limited
Draft	0.0.2	8/17/05	<ul style="list-style-type: none"> • Added CSP Participating Agreement v2.1.0, Relying Party Participation Agreement v2.1.0, Business Rules v2.1.0, and Operating Rules v0.3.0. • Made format changes. • Made minor grammatical changes. • Added Operating Rules to section 2.3 title. • Placed operating rule footnotes into endnotes. • Added Operating Rules to section 3.4.1.2 title. • Replaced “Initiative” with “Federation” in section 4 title. • Replaced “section 10” with “this section” in 4.10.1 and 4.10.4, 	Limited
Draft	3.0.0	8/25/05	<ul style="list-style-type: none"> • Changed to version 3.0.0 to eliminate confusion on current version. 	Limited
Draft	3.0.1	8/30/05	<ul style="list-style-type: none"> • Reference numbers 4.2.1, 4.4.3, 4.4.5, 4.6.4, 4.6.11, 4.7.1, 4.7.12, 4.7.18, 4.8.5, 4.8.10, 4.8.28, 4.8.31, 4.10.6, 4.10.8, 4.10.12, 4.14.3, 4.20.4, and 4.20.5. Modified section reference numbers as needed. • Added new reference numbers 4.3.4, 4.3.13, 4.4.5, 4.5.1, 4.8.5, 4.12.6, 4.17.9, and 4.20.4. Modified section reference numbers as needed. • Minor wording changes were made throughout the document. • Added definition for compatible to Appendix A. • Added S/MIME to Appendix B. • Added text from 4.7.1 to 4.7.2 and changed “Primer” to “FAQ”. • Added two new bullets (numbers 1 and 5) to 4.8.11. • Added a new bullet (number 2) to 4.8.25. • Changed “EAI” to “EAI PMO” where appropriate. 	Limited
Draft	3.1.0	9/12/05	<ul style="list-style-type: none"> • Added “logs as defined in these rules” to reference number 4.3.11. • Added “appropriate” to reference number 4.3.13. • Added “via means accessible only to Federation Members” to reference numbers 4.4.3 and 4.4.4. • Changed “Federal PKI” to “Federation” and provided footnote pointing to Trust List to reference number 4.4.5. • Added “subject to the terms of this agreement” to reference number 4.5.4. • Added “based on the criteria in Appendix D” to reference number 4.5.9. • Added “defined in section 4.10” to reference number 4.6.5. • Added “and trusted” to reference number 4.17.13. • Added “or subsequent revisions” to reference number 4.8.2. • Added “or appropriately destroy” and “logs required by these rules “ to reference number 4.8.9. • Added “relevant” to reference number 4.8.10. • Added “reasonable” and sentence “A list externally facing 	Limited

Status	Release	Date	Comment	Audience
			<p>systems..." to reference number 4.8.11.</p> <ul style="list-style-type: none"> • Added "or confidential" to reference number 4.8.17. • Deleted "or suspected" from reference number 4.10.10 #1. • Added "CSs may delay these new connections so that no more than three (3) new RP connections are established in any one 90 day period" to reference number 4.12.3. • Added "Assertion-based RPs may delay these new connections so that no more than three (3) new CS connections are established in any one 90 day period" to reference number 4.12.4. • Deleted reference numbers 4.12.6 and 4.20.4. • Changed section 4.16 title to "Customer / Citizen Service". • Added new definition for compatibility to Appendix A. • Added SSA provided text to reference numbers 4.5.2 and 4.5.10. • Changed Business Rules and Participation Agreements to reflect discussion of meetings held on August 29, 2005. • Incorporated Fidelity and Treasury reactions to prior drafts of Business Rules and Participation Agreements. 	
Draft	3.2.0	9/13/05	<ul style="list-style-type: none"> • Made changes to Appendix E. • Added text for add-on services to reference numbers 4.14.2, 4.14.3, and 4.14.4. 	Limited
Draft	3.2.1	9/14/05	<ul style="list-style-type: none"> • Removed Appendix E. 	Limited
Draft	3.2.2	9/19/05	<ul style="list-style-type: none"> • Revised reference number 4.9.1 #2. • Added Appendix E & F. 	Limited
Draft	3.2.3	9/26/05	<ul style="list-style-type: none"> • Various typos removals, non-substantive wording clarifications, deletion of duplicative wording and format improvements were made throughout the Business Rules and Participation Agreements. • Deleted reference to taxes and fees from Relying Party agreement, former section 2.8.10. • Deleted reference to bankruptcy and assignment of rights to creditors from Relying Party agreement, section 2.8.11 • Deleted section 3.4, where the change control rules may have been housed. These rules are now an appendix of the Legal Suite. • Second paragraph of section 1.2, further specifying role of DFA/CSP, was deleted. • Sections 1.4 and 2.5 were deleted, in favor of consolidating all dispute resolution terms into a single section of each agreement. • Section 1.4.1 and 2.5.1 were clarified to indicate all parties have orderly wind-down responsibilities. • Sections 1.6.1 and 2.6.1 clarify that proposed changes in policy, practices or technology must be reported to GSA. • Subsections within sections 1.5 and 2.6, addressing Dispute Resolution, were each consolidated. • Sections 2.6.2 and 1.5.2 were amended to reference a 	Limited

Status	Release	Date	Comment	Audience
			<p>"reasonable determination" as opposed to the more relaxed standard of a "reasonable suspicion".</p> <ul style="list-style-type: none"> • Sections 1.6.2 and 2.7.3 were clarified to indicate the liability limitation applies to circumstances related to the Agreement or to use of the Federation. • Section 1.6.11 and 2.7.3 were clarified to indicate that surviving terms will be applicable whether the party has been terminated or suspended. • Section 3.3.5.3 clarified to indicate only material non-compliance triggers need the provisions of this clause. • Section 3.3.6.1 was clarified to indicate that the notice of emergency suspension or termination must be given to the other party that signed the Participation Agreement (e.g. a CSP must give notice to GSA and vice versa). • Section 1.6.5, assignment, clarified point that a Treasury DFA can select agents and others to perform tasks. • End-Notes were deleted from the Business Rules and Participation Agreements, as unnecessary, at request of commenters. • Section 3.2.2 was clarified by deleting confusing language regarding conflicting terms of other agreements outside the Federation. • All references to binding documents have been changed to the new section 3.3.3.2. • 1.6.4 and 2.7.5 have been modified to delete the integration clause, because there are a number of other agreements at play between various of the parties. • 3.3.5.5. – deleted wording that GSA reserves right to approve DFA, because the interagency agreement Draft already includes a process for collaborations. 	
Draft	3.2.4	09/28/05	<ul style="list-style-type: none"> • Made acronym changes throughout the document. • Removed references to the RPAF. • Changed "AA" to "RP" in section 4.1. • Added "the following rules apply" to each rule section in the operating rules. • Provided new text for 4.2.1. • Changed "numerous" to "particular" in section 4.3. • Changed "EAI" to "Federation" in section 4.4. • Provided text stating that RP and CSP reports are to be provided monthly. • Changed text to say "active Federation Members in good standing" in 4.4.3 and 4.4.4. • Changed "EST" to "ET" throughout document. • Changed "seven (7) days per week" to "Monday through Friday" in 4.6.2. • Changed "750 pixels by 80 pixels" to "140 pixels by 40 pixels" in 4.7.10. • Replaced "RPAF" with "NIST SP 600-53" in 4.8.2. • Changed "pass" to "participate in a suitable background evaluation" in 4.8.7. 	Limited

Status	Release	Date	Comment	Audience
			<ul style="list-style-type: none"> • Changed text in reference number 4.8.9 specifying confidential information from the EAI PMO. • Added “intrusive testing” to 4.8.11, number 3. • Added “and confidential” to 4.8.16. • Changed text in 4.8.18 specifying when outside the firewall and attempting to access a Federation system root. • Changed “should” to “must”, added “and unused”, and added the sentence “It is recommended that unneeded services be removed”. • Removed session management section. • Removed bullet one and change bullet five text stating “unauthorized changes” in section 4.10 (now 4.9). • Added “publish” to 4.11.5 (now 4.10.5). • Changed text in 4.12.1 (now 4.11.1) to “substantial changes that affect other Federation Member systems”. • Changed “one” to “given” in 4.12.4 (now 4.11.4) and 4.12.5 (now 4.11.5). • Deleted “if they are restricted under privacy regulations, policy, and law” from 4.13.1 (now 4.12.1) • Changed section 4.16 (now 4.15) to “End-User Service”. • Added “as amended from time-to-time” to section 4.20 (now 4.19). • Provided new text for section 4.21 (now 4.20). • Removed DRAFT watermark. 	
Release	4.0.0	09/29/05	Official document release.	Public
Release	4.0.1	10/03/05	Deleted section 4.1.2 and added text for the TBDs in Appendix F.	Public
Revision	4.0.2	10/10/05	<ul style="list-style-type: none"> • Made sentence wording changes throughout the document. • Changed section reference to 1.6.11 in section 1.4. • Changed section reference to 3.3.6.6 in section 3.2.2. • Added an additional sentence to the end of section 3.3.5.5. • Deleted “This document is a normative specification” from section 4.1.1. • Changed section reference to 1.6.8 in section 4.7. • Deleted reference numbers 4.8.17 and 4.8.22. • Changes section 4.19 title to “Authoritative Documents”. • Added text from section 1.7 to section 2.8. 	Limited
Revision	4.0.3	10/11/05	<ul style="list-style-type: none"> • Added “Interim” to title of document. • Added “Interim” to section 3 title. • Removed reference to suspension policy. • Made additional sentence wording changes. 	Limited
Revision	4.0.4	10/13/05	<ul style="list-style-type: none"> • Capitalized all defined terms throughout the document. • Capitalized “section” throughout the document. • Added 3rd party to section 1.6.5. • Added new text for section 1.6.7 and 1.6.8. • Changed date to October 31, 2006 in section 1.6.15. • Added new sub-sections from CSP Agreement to section 2. 	Limited

Status	Release	Date	Comment	Audience
			<ul style="list-style-type: none">• Added new text to section 2.7.2.• Deleted section 2.7.7.• Changed date to October 31, 2006 in section 2.7.12.• Changed reference to 3.3.6.2 in section 3.3.3.4.2.• Added sentence for scope of auditing in section 3.3.5.2.• Deleted section 3.3.6.4.• Revised text in section 3.3.6.6.• Deleted reference number 4.8.9.• Replaced “certified” with “approved” throughout the document.• Revised definition of Relying Party.• Added definitions for Business Rules, Agency, Boarding Process, Binding Documents, Contractor, Operational Readiness Review, Designated Financial Agent, and Sensitive Information.• Added updated governance diagram to Appendix E.• Changed the effective date to October 14, 2005.	
Revision	4.0.5	10/13/05	<ul style="list-style-type: none">• Added definition for “The Approved Technology Provider List”.• Replaced “EAI PMO” with “GSA”.• Removed definition for “Certified Credential Service”.• Provided new definition for “Availability”.• Removed “RPAF” from the acronym list.• Changed “certify” to “approve”.• Made minor sentence modifications throughout the document.	Limited
Revision	4.0.6	10/14/05	<ul style="list-style-type: none">• Removed EAI from section 4.• Changed title of section 4.12 to “Optional Attributes”.• Revised 1st paragraph and added new paragraph for CSPs in section 3.3.1.• Revised 1st sentence in section 3.3.3.3.• Replaced “through” with “in conjunction with” in section 3.3.6.5.	Limited
Revision	4.0.7	10/14/05	<ul style="list-style-type: none">• Added new sentence to section 3.3.1.	Limited

Editors

Chris Louden	Dave Silver	J.T. Lazo
Chris Broberg	David Simonetti	Steve Lazerowich
Glenn Ballard	Andrew Chiu	Dan Greenwood

Table of Contents

RELEASE NOTES	I
DOCUMENT HISTORY	II
EDITORS	VI
TABLE OF CONTENTS	VII
1 E-AUTHENTICATION FEDERATION CSP PARTICIPATION AGREEMENT	1
1.1 SCOPE AND APPLICATION	1
1.2 PARTIES AND CONTACT PERSON.....	1
1.3 AGREEMENT TO ABIDE BY BUSINESS RULES AND OPERATING RULES.....	1
1.4 COMPLIANCE WITH REQUIREMENTS.....	1
1.5 TERMINATION AND SUSPENSION.....	1
1.5.1 <i>Voluntary</i>	2
1.5.2 <i>Involuntary</i>	2
1.6 ENFORCEMENT.....	2
1.6.1 <i>Dispute Resolution</i>	2
1.6.2 <i>GSA Investigation</i>	2
1.6.3 <i>Recourse</i>	3
1.7 LEGAL TERMS.....	3
1.7.1 <i>Confidentiality and Non-Disclosure</i>	3
1.7.2 <i>Limitation of Liability</i>	3
1.7.3 <i>Governing Law</i>	3
1.7.4 <i>Order of Precedence</i>	4
1.7.5 <i>Assignment, Succession and Bankruptcy</i>	4
1.7.6 <i>Severability</i>	4
1.7.7 <i>Grant of License</i>	5
1.7.8 <i>Ownership of Intellectual Property</i>	5
1.7.9 <i>Publicity</i>	5
1.7.10 <i>Waiver</i>	5
1.7.11 <i>Survival</i>	5
1.7.12 <i>Amendment</i>	6
1.7.13 <i>Responsibility For Taxes, Expenses</i>	6
1.7.14 <i>Force Majeure</i>	6
1.7.15 <i>Business Rules and Operating Rules Freeze</i>	6
1.8 SIGNATURES	6
2 E-AUTHENTICATION FEDERATION RELYING PARTY PARTICIPATION AGREEMENT	7
2.1 SCOPE AND APPLICATION	7
2.2 PARTIES AND CONTACT PERSON.....	7
2.3 AGREEMENT TO ABIDE BY BUSINESS RULES AND OPERATING RULES.....	7
2.4 COMPLIANCE WITH REQUIREMENTS.....	7
2.5 TERMINATION AND SUSPENSION.....	7
2.5.1 <i>Voluntary</i>	8
2.5.2 <i>Involuntary</i>	8
2.6 ENFORCEMENT.....	8
2.6.1 <i>Dispute Resolution</i>	8
2.6.2 <i>GSA Investigation</i>	8
2.6.3 <i>Recourse</i>	9

2.7	LEGAL TERMS.....	9
2.7.1	<i>Governing Law</i>	9
2.7.2	<i>Grant of License</i>	9
2.7.3	<i>Ownership of Intellectual Property</i>	9
2.7.4	<i>Survival</i>	10
2.7.5	<i>Confidentiality and Non-Disclosure</i>	10
2.7.6	<i>Order of Precedence</i>	10
2.7.7	<i>Severability</i>	10
2.7.8	<i>Amendment</i>	10
2.7.9	<i>Publicity</i>	11
2.7.10	<i>Waiver</i>	11
2.7.11	<i>Force Majeure</i>	11
2.7.12	<i>Assignment and Succession</i>	11
2.7.13	<i>Business Rules and Operating Rules Freeze</i>	11
2.8	SIGNATURES	12
3	E-AUTHENTICATION FEDERATION INTERIM BUSINESS RULES	13
3.1	TITLE	13
3.2	SCOPE	13
3.2.1	<i>Scope of Rules</i>	13
3.2.2	<i>Agreements and Conduct Outside Scope of Rules</i>	13
3.2.3	<i>Rules Appearing in Multiple Documents</i>	13
3.3	PARTICIPATION	14
3.3.1	<i>Eligibility</i>	14
3.3.2	<i>Participation Requirements</i>	14
3.3.2.1	Relying Parties.....	14
3.3.2.2	CSPs.....	14
3.3.2.3	End-Users	15
3.3.3	<i>GSA Role and Obligations</i>	15
3.3.3.1	Operating Authorization	15
3.3.3.2	Promulgation and Amendment of Business Rules, Operating Rules and Other Documents.....	15
3.3.3.3	Relying Party and CSP Approval.....	16
3.3.3.4	Service Offerings	16
3.3.3.5	Contact Information	17
3.3.4	<i>Relying Party Role and Obligations</i>	17
3.3.4.1	Relying Party Boarding Process, Operational Readiness Review and Participation Agreement.....	17
3.3.4.2	Interface Specifications, Approved Software Use and Upgrade	17
3.3.4.3	Security and Privacy Compliance	17
3.3.4.4	Reasonable Reliance on Credential.....	18
3.3.5	<i>CSP Role and Obligations</i>	18
3.3.5.1	CSP Boarding Process, Operational Readiness Review and Participation Agreement	18
3.3.5.2	CSP Continuing Audit Requirement	18
3.3.5.3	Material Change to CSP, Credential Services or Credential	18
3.3.5.4	Technical Architecture and Interface Specification	19
3.3.5.5	Designated Financial Agents.....	19
3.3.6	<i>General Obligations</i>	19
3.3.6.1	Federation Security and Reliability.....	19
3.3.6.2	Federation Interoperability.....	19
3.3.6.3	Operational and Ongoing Requirements	20
3.3.6.4	End-User Consent and Notice	20
3.3.6.5	Additional Transactions	21
4	E-AUTHENTICATION FEDERATION INTERIM OPERATING RULES.....	22
4.1	INTRODUCTION	22
4.1.1	<i>Purpose</i>	22
4.1.2	<i>Document Organization</i>	22

4.2	PRIVACY	24
4.3	LOGS.....	25
4.4	REPORTING	26
4.5	MONITORING	28
4.6	PERFORMANCE REQUIREMENTS.....	30
4.7	STYLE GUIDELINES, NARRATIVE ELEMENTS, BRANDING AND LOGOS.....	31
4.8	SECURITY REQUIREMENTS.....	34
4.9	INCIDENT RESPONSE	39
4.10	METADATA.....	43
4.11	CONFIGURATION MANAGEMENT	44
4.12	OPTIONAL ATTRIBUTES	45
4.13	ADD-ON SERVICES	46
4.14	TIME SYNCHRONIZATION.....	47
4.15	END-USER SERVICE	48
4.16	POINTS OF CONTACT.....	49
4.17	GSA ARCHITECTURE COMPONENTS	50
4.18	DOCUMENT MANAGEMENT	51
4.19	AUTHORITATIVE DOCUMENTS	52
4.20	OFFICIAL WAIVER(S).....	53
	APPENDIX A: GLOSSARY	54
	APPENDIX B: ACRONYMS	65
	APPENDIX C: MONITORING TEST TYPES	67
	APPENDIX D: PERFORMANCE TESTING	68
	AVAILABILITY TESTING CRITERIA	68
	AVERAGE RESPONSE TIME.....	69
	<i>Testing</i>	69
	MINIMAL ACCEPTABLE RESPONSE TIME.....	69
	<i>Testing</i>	69
	MEASUREMENTS	71
	<i>Availability Test</i>	71
	<i>Average Response Time Test</i>	72
	<i>Minimal Acceptable Response Time Test</i>	73
	APPENDIX E: FEDERATION GOVERNANCE	74
	APPENDIX F: FEDERATION CHANGE MANAGEMENT POLICY	77
	CHANGE CLASSIFICATION.....	78
	CHANGE CATEGORY	78
	CHANGE TYPE.....	78
	IMPACT	79
	MAGNITUDE.....	79
	CHANGE POLICIES.....	80
	RELEASE RULES	80
	CHANGE MANAGEMENT POLICIES	80
	POLICIES FOR CHANGE CATEGORIES.....	81
	CHANGE REVIEW AND IMPLEMENTATION PROCESS	82
	END NOTES	83

1 E-AUTHENTICATION FEDERATION CSP PARTICIPATION AGREEMENT

1.1 Scope and Application

This Participation Agreement constitutes the legal basis for an organization becoming a Credential Service Provider (CSP) within the E-Authentication Federation. Signatories agree that the signed Participation Agreement, Business Rules, and Operating Rules, including the Binding Documents referenced in Section 3.3.3.2 of the Business Rules, govern participation in the E-Authentication Federation. Final approval by the GSA is necessary for a CSP to participate in the E-Authentication Federation. Such GSA approval is contingent upon the CSP successfully completing the Boarding Process and Operational Readiness Review. Signatories agree to abide by all applicable laws and regulations, including those relating to privacy, and record keeping.

1.2 Parties and Contact Person

The parties to this Participation Agreement are the General Services Administration of the United States Federal Government (GSA) and _____ (CSP). Each party shall designate one or more contact persons for purposes of notices and other communications under the Business Rules, Operating Rules and this Participation Agreement.

1.3 Agreement to Abide by Business Rules and Operating Rules

By signing this Participation Agreement, the CSP agrees to abide by the E-Authentication Federation Business Rules and Operating Rules as in effect during the period of CSP participation in the E-Authentication Federation, and which are expressly incorporated into and made a part of this Agreement.

1.4 Compliance With Requirements

CSP agrees that compliance with the Credential Assessment Framework (CAF), including security requirements specified in the Operating Rules, is a prerequisite to participation in the E-Authentication Federation and must be finalized before approval for inclusion in the E-Authentication Federation. CSP agrees to maintain continuing compliance with CAF and other terms contained in the Business Rules and Operating Rules.

1.5 Termination and Suspension

The terms of this Participation Agreement cease to apply to any CSP as of the effective date of termination of participation in the E-Authentication Federation, except surviving terms, according to Section 1.7.11.

1.5.1 Voluntary

This CSP Participation Agreement may be terminated at the discretion of the CSP, upon written notice to GSA or by mutual agreement between GSA and the CSP, reflected in a signed writing, provided that in the event of any such voluntary termination each party remains responsible to the extent practicable for an orderly wind down of activities or services in progress and for the maintenance of the records of such activities and services.

1.5.2 Involuntary

GSA may terminate or suspend the participation of a CSP in the E-Authentication Federation, at any time, under extraordinary circumstances necessary to prevent or cease serious harm to the E-Authentication Federation, or for breach by the CSP of the terms of this Participation Agreement, the Business Rules or the Operating Rules, that the CSP is unable to cure within 30 days after receiving notice from GSA regarding such breach. Termination shall be in writing and shall be effective no less than 30 days from time notice is given, unless a shorter period or immediate termination is required in the reasonable judgement of GSA. Suspension may occur at any time, as the needs and circumstances may reasonably require, with notice to the CSP as soon as practicable.

1.6 Enforcement

CSP and GSA agree that the following provisions are related to enforcement, recognizing that such provisions are incorporated into the Participation Agreements executed by all Approved Parties.

1.6.1 Dispute Resolution

Every Approved Party or its authorized agent agrees to attempt in a timely manner to resolve any dispute arising out of or related to the application of the Business Rules, the Operating Rules or the Participation Agreement executed by that Approved Party in good faith with the other disputants and parties related to the dispute. In the event the parties are unable to resolve the matter, then each such dispute, the date of attempted resolutions, including proposed changes in policy, practices or technology implementation, shall be reported to the GSA in a timely manner.

In the event parties to a dispute are unable, despite their best good faith efforts, to resolve a dispute among themselves, any party may request GSA to investigate the dispute and may propose resolution or mediate at the request of the parties. Each such request must be accompanied by a full report of all the relevant information related to the dispute.

1.6.2 GSA Investigation

GSA shall respond to every request to investigate a dispute in a timely manner. GSA may request additional information from one or more parties to the dispute.

GSA may initiate an investigation based upon the request of any Approved Party in the E-Authentication Federation, or may initiate an investigation whenever it deems appropriate based on any information it regards as relevant and credible. Without

limitation, such information may include a reasonable determination that an Approved Party is not in compliance with continuing obligations required under this Participation Agreement, the Business Rules or the Operating Rules. An Approved Party shall be notified in a timely manner by GSA if it becomes the subject of an investigation.

1.6.3 Recourse

Based upon the results of its investigation, and only under extraordinary circumstances necessary to prevent or limit serious harm to the E-Authentication Federation, the GSA may suspend participation of any Approved Party in the E-Authentication Federation or render inaccessible any Architectural Component of the E-Authentication Federation by one or more Approved Parties. An Approved Party has the right to appeal any proposed suspension, including being provided adequate notice and an opportunity to be heard. If the result of an investigation indicates that an Approved Party is not in compliance with any requirement included directly or by reference under these Business Rules or the Operating Rules, GSA may require such additional audit, re-approval or approval at different Level(s) of Assurance, to the extent necessary to prevent or limit serious harm to the E-Authentication Federation.

1.7 Legal Terms

1.7.1 Confidentiality and Non-Disclosure

GSA agrees not to unreasonably withhold assent to industry standard confidentiality and/or non-disclosure agreements with the CSP that may be required as a condition of accepting Approved Credentials of that CSP and according to the Business Rules and Operating Rules. GSA further agrees to require consent to the relevant terms of such agreements by any Relying Party to whom the terms may apply.

1.7.2 Limitation of Liability

Liability against the United States for damage caused by negligence of the Government is controlled by the Federal Tort Claims Act, 28 USC Section 1346 et seq. A non-governmental Approved CSP operating in accordance with the terms of this CSP Participation Agreement, the Business Rules and the Operating Rules, may assert the Government contractor defense to tort claims arising out of or related to participation in the E-Authentication Federation.

There shall be no liability against any Approved Party under any theory of liability for any claim arising out of or in relation to this Agreement or to the use of or reliance upon an Approved Credential or participation in the E-Authentication Federation, beyond the recourse available under the Federal Tort Claims Act, unless agreed by contract among the relevant parties.

1.7.3 Governing Law

This Participation Agreement, the Business Rules and the Operating Rules and any related materials governing the E-Authentication Federation shall be construed and

adjudicated according to the statutes, regulations and judicial decisions of the United States of America.

1.7.4 Order of Precedence

The parties agree to interpret the provisions of all E-Authentication documents to be consistent, to the maximum extent reasonable and practicable. However, in the event of a conflict between the terms of various E-Authentication Federation related documents, documents shall be accorded the following order of priority: This CSP Participation Agreement shall be construed to prevail over the terms of any other document in the E-Authentication Legal Suite, followed in order of precedence by the terms of the E-Authentication Federation Business Rules, followed by the terms of the Operating Rules, followed by the terms of any Binding Document referenced in Section 3.3.3.2 of the Business Rules, followed by any other policies, agreements or other materials formally promulgated for the purpose of documenting legal terms governing participation in the E-Authentication Federation.

1.7.5 Assignment, Succession and Bankruptcy

CSP agrees it may not sell, rent, lease, sublicense, assign, grant a security interest in or otherwise transfer any right and/or obligation contained in this CSP Participation Agreement, the E-Authentication Federation Business Rules or the Operating Rules except as permitted herein. CSP may request of GSA permission for assignment or succession to a different party, of part or all of the rights and/or obligations contained in this CSP Participation Agreement, the E-Authentication Federation Business Rules or the Operating Rules. Nothing in this paragraph shall be construed as to prevent the Department of the Treasury from Designating Financial Agents to carry out its obligations under this agreement, in accord with the terms of Section 3.3.5.5 of the Business Rules, or to prohibit such agents from the use of contractors, affiliates or other third parties. Any prohibited assignment shall be null and void.

CSP or an agent thereof may engage its affiliates and/or third parties to perform certain of its obligations contained in this CSP Participation Agreement, the E-Authentication Federation Business Rules or the Operating Rules. For purposes of this Agreement, Affiliate shall mean any entity directly or indirectly Controlling, Controlled by or under common Control with a CSP. For purposes of this provision, Control means an ownership interest of 50 percent or more.

1.7.6 Severability

If any provision, set of provisions or part of a provision of this Participation Agreement, the Business Rules or the Operating Rules is held to be unenforceable or otherwise invalid in whole or in part, the remaining provisions shall remain in full force and effect and shall be construed to the maximum extent practicable as a consistent and reasonable entire agreement.

1.7.7 *Grant of License*

For the term of this Participation Agreement, CSP is hereby granted a perpetual, non-exclusive, royalty free, non-transferable license to use the Architectural Component known as the Portal required for participation in the E-Authentication Federation, including the right to access and grant access to other authorized parties to such components and to Systems and applications of Approved Relying Parties.

1.7.8 *Ownership of Intellectual Property*

Ownership and control of all databases, records, and data transmission systems remains solely with the CSP. CSP hereby grants all Approved Parties of the E-Authentication Federation a perpetual, royalty-free, non-exclusive, non-transferable license to use any methods or other intellectual property of the CSP solely for use within the E-Authentication Federation and in accordance with the E-Authentication Federation Business Rules and Operating Rules (the “Approved Purpose”). Such license includes the right to practice, solely for the Approved purpose, under claims in any United States patent granted to CSP and its affiliates. Usage of this license by any Approved Parties will require a reciprocal, perpetual, royalty-free non-exclusive, non-transferable license to CSP from any other Approved Parties in connection with CSP’s participation.

1.7.9 *Publicity*

No Signatory may make any public claims regarding any other Signatory without that party's prior written approval, including use of the name of a CSP by GSA or a Relying Party or any suggestion of endorsement of a CSP by GSA or any Relying Party. The foregoing limitation shall not apply to use of the name of a CSP on the Trusted Credential Service Provider List or in any other way authorized under these Business Rules or Operating Rules and other Binding Documents referenced in Section 3.3.3.2.

1.7.10 *Waiver*

Neither party's failure to enforce strict performance of any provision of this Participation Agreement, the Business Rules or the Operating Rules will constitute a waiver of a right to subsequently enforce such a provision. No written waiver shall constitute, or be construed as, a waiver of any other obligation or condition of this Participation Agreement, the Business Rules or the Operating Rules.

1.7.11 *Survival*

Any termination or suspension of CSP's participation in the E-Authentication Federation shall not affect any accrued rights or liabilities of any party nor shall it affect the coming into force or the continuance in force of any provision of this Participation Agreement which is expressly or by implication intended to come into force or continue in force on or after such termination or suspension.

1.7.12 Amendment

This Participation Agreement may be amended by agreement of the parties, reflected by a signed writing.

1.7.13 Responsibility For Taxes, Expenses

Each party agrees that each are solely responsible for the payment of taxes or expenses incurred by that party arising out of or related to participation in the E-Authentication Federation, unless otherwise agreed by a signed writing.

1.7.14 Force Majeure

Neither party shall be considered in default hereunder due to any failure in performance of its obligations under this Participation Agreement, the Business Rules or the Operating Rules, including any Binding Document referenced in Section 3.3.3.2, should such failure arise out of causes beyond its reasonable control and without its fault or negligence.

1.7.15 Business Rules and Operating Rules Freeze

The parties agree that, unless otherwise agreed to in writing, the Business Rules or the Operating Rules are not intended to be, and shall not be amended for a period of one year from the date of execution of this Participation Agreement or before October 31, 2006, whichever date shall precede the other.

1.8 Signatures

The undersigned represent and warrant that they have the requisite power and authority to execute this Participation Agreement on behalf of their respective organizations (the Parties), including authority to legally bind their respective organizations to the Binding Documents referenced in Section 3.3.3.2 of the Business Rules.

CSP

GSA

2 E-AUTHENTICATION FEDERATION RELYING PARTY PARTICIPATION AGREEMENT

2.1 Scope and Application

This Relying Party Participation Agreement constitutes the legal basis for an organization becoming a Relying Party within the E-Authentication Federation. Signatories agree that the signed Participation Agreement, Business Rules and the Operating Rules, including the Binding Documents referenced in Section 3.3.3.2 of the Business Rules, govern participation in the E-Authentication Federation. Final approval by the GSA is necessary for a Relying Party to participate in the E-Authentication Federation. Such GSA approval is contingent upon the Relying Party successfully completing the Boarding Process and Operational Readiness Review. Signatories agree to abide by all applicable laws and regulations, including those relating to privacy, and record keeping.

2.2 Parties and Contact Person

The parties to this Participation Agreement are the General Services Administration of the United States Federal Government (GSA) and _____ (Relying Party). Each party shall designate one or more contact persons for purposes of notices and other communications under the Business Rules, Operating Rules and this Participation Agreement.

2.3 Agreement to Abide by Business Rules and Operating Rules

By signing this Participation Agreement, the Relying Party agrees to abide by the E-Authentication Federation Business Rules and Operating Rules, as in effect during the period of participation in the E-Authentication Federation, and which are expressly incorporated into and made a part of this Agreement.

2.4 Compliance With Requirements

Relying Party agrees that compliance with NIST SP 800-53 and the security requirements specified in the Operating Rules, are prerequisites to participation in the E-Authentication Federation and must be finalized before approval for inclusion in the E-Authentication Federation. Relying Party agrees to maintain continuing compliance with NIST SP 800-53 and other terms contained in the Business Rules and Operating Rules.

2.5 Termination and Suspension

The terms of this Participation Agreement, the Business Rules and the Operating Rules cease to apply to any Relying Party as of the effective date of termination of participation in the E-Authentication Federation except for the surviving terms, according to Section 2.7.4.

2.5.1 Voluntary

Participation in the E-Authentication Federation may be terminated by Relying Party through written notice to GSA, to avoid the imminent effect of amended language to the Business Rules or Operating Rules. Such termination shall be effective no less than 30 calendar days from the date of receipt by GSA. Relying Party may terminate its participation in the E-Authentication Federation, without cause, upon 60 days prior written notice to GSA. In the event of extraordinary emergency circumstances for which relief is not possible in the context of continued participation, a Relying Party may terminate participation immediately, provided that both parties remains responsible to the extent practicable for an orderly wind down of activities or services in progress and for the maintenance of the records of such activities and services. Participation in the E-Authentication Federation may also be terminated at any time for any reason by mutual agreement between the GSA and Relying Party.

2.5.2 Involuntary

GSA may suspend the participation of any Relying Party in the E-Authentication Federation, and only under extraordinary circumstances necessary to prevent or cease serious harm to the E-Authentication Federation.

2.6 Enforcement

Relying Party and GSA agree that the following provisions are related to enforcement, recognizing that such provisions are incorporated into the Participation Agreements executed by all Approved Parties.

2.6.1 Dispute Resolution

Every Approved Party agrees to attempt in a timely manner to resolve any dispute arising out of or related to the application of the Business Rules, the Operating Rules or the Participation Agreement executed by that Approved Party in good faith with the other disputants and parties related to the dispute. In the event the parties are unable to resolve the matter, then each such dispute, the date of attempted resolutions, including proposed changes in policy, practices or technology implementation, shall be reported to the GSA in a timely manner.

In the event parties to a dispute are unable, despite their best good faith efforts, to resolve a dispute among themselves, any party may request GSA to investigate the dispute and may propose resolution or mediate at the request of the parties. Each such request must be accompanied by a full report of all the relevant information related to the dispute.

2.6.2 GSA Investigation

GSA shall respond to every request to investigate a dispute in a timely manner. GSA may request additional information from one or more parties to the dispute.

GSA may initiate an investigation based upon the request of any Approved Party in the E-Authentication Federation, or may initiate an investigation whenever it deems



appropriate based on any information it regards as relevant and credible. Without limitation, such information may include a reasonable determination that an Approved Party is not in compliance with continuing obligations required under this Participation Agreement, the Business Rules or the Operating Rules. An Approved Party shall be notified in a timely manner by GSA if it becomes the subject of an investigation.

2.6.3 Recourse

Based upon the results of its investigation, and only under extraordinary circumstances necessary to prevent or limit serious harm to the E-Authentication Federation, the GSA may suspend participation of any Approved Party in the E-Authentication Federation or render inaccessible any Architectural Component of the E-Authentication Federation by one or more Approved Parties. An Approved Party has the right to appeal any proposed suspension, including being provided adequate notice and an opportunity to be heard. If the result of an investigation indicates that an Approved Party is not in compliance with any requirement included directly or by reference under these Business Rules or the Operating Rules, GSA may require such additional audit, re-approval or approval at different Level(s) of Assurance, to the extent necessary to prevent or limit serious harm to the E-Authentication Federation.

2.7 Legal Terms

2.7.1 Governing Law

This Participation Agreement, the Business Rules and the Operating Rules and any related materials governing the E-Authentication Federation shall be construed and adjudicated according to the statutes, regulations and judicial decisions of the United States of America.

2.7.2 Grant of License

For the term of this Participation Agreement, Relying Party is hereby granted a perpetual, non-exclusive, royalty free, non-transferable license to use the Architectural Component known as the Portal required for participation in the E-Authentication Federation, including the right to access and grant access to other authorized parties to such components and to Systems and applications of Approved Relying Parties.

2.7.3 Ownership of Intellectual Property

Ownership and control of all databases, records, and data transmission systems remains solely with the Relying Party. Relying Party hereby grants all Approved Parties of the E-Authentication Federation a perpetual, royalty-free, non-exclusive, non-transferable license to use any methods or other intellectual property of the Relying Party solely for use within the E-Authentication Federation and in accordance with the E-Authentication Federation Business Rules and Operating Rules (the “Approved Purpose”). Such license includes the right to practice, solely for the Approved purpose, under claims in any United States patent granted to the Relying Party and its affiliates. Usage of this license by any Approved Parties will require a reciprocal, perpetual, royalty-free non-exclusive,

non-transferable license to the Relying Party from any other Approved Parties in connection with Relying Party's participation.

2.7.4 *Survival*

Any termination or suspension of Relying Party's participation in the E-Authentication Federation shall not affect any accrued rights or liabilities of either party nor shall it affect the coming into force or the continuance in force of any provision of this Participation Agreement which is expressly or by implication intended to come into force or continue in force on or after such termination or suspension.

2.7.5 *Confidentiality and Non-Disclosure*

Relying Party agrees not to unreasonably withhold assent to industry standard confidentiality and/or non-disclosure agreements participating CSPs may require as a condition of accepting Credentials of that CSP and according to the Business Rules and Operating Rules.

2.7.6 *Order of Precedence*

The parties agree to interpret the provisions of all E-Authentication documents to be consistent, to the maximum extent reasonable and practicable. However, in the event of a conflict between the terms of various E-Authentication Federation related documents, documents shall be accorded the following order of priority: This Relying Party Participation Agreement shall be construed to prevail over the terms of any other document in the E-Authentication Legal Suite, followed in order of precedence by the terms of the E-Authentication Federation Business Rules, followed by the terms of the Operating Rules, followed by the terms of any Binding Document referenced in Section 3.3.3.2 of the Business Rules, followed by any other policies, agreements or other materials formally promulgated for the purpose of documenting legal terms governing participation in the E-Authentication Federation.

2.7.7 *Severability*

If any provision, set of provisions or part of a provision of this Participation Agreement, the Business Rules or the Operating Rules is held to be unenforceable or otherwise invalid in whole or in part, the remaining provisions shall remain in full force and effect and shall be construed to the maximum extent practicable as a consistent and reasonable entire agreement.

2.7.8 *Amendment*

This Participation Agreement may be amended by agreement of the parties, reflected by a signed writing.

2.7.9 Publicity

No Signatory may make any public claims regarding any other Signatory without that party's prior written approval, including use of the name of a Relying Party by GSA or a CSP or any suggestion of endorsement of a Relying Party by GSA or any CSP. The foregoing limitation shall not apply to use of the name of a Relying Party in any other way authorized under these Business Rules or Operating Rules and other Binding Documents referenced in Section 3.3.3.2.

2.7.10 Waiver

Neither party's failure to enforce strict performance of any provision of this Participation Agreement, the Business Rules or the Operating Rules will constitute a waiver of a right to subsequently enforce such a provision. No written waiver shall constitute, or be construed as, a waiver of any other obligation or condition of this Participation Agreement, the Business Rules or the Operating Rules.

2.7.11 Force Majeure

Neither party shall be considered in default hereunder due to any failure in performance of its obligations under this Participation Agreement, the Business Rules or the Operating Rules, including any Binding Document referenced in Section 3.3.3.2 should such failure arise out of causes beyond its reasonable control and without its fault or negligence.

2.7.12 Assignment and Succession

Relying Party may not sell, rent, lease, sublicense, assign, grant a security interest in or otherwise transfer any right and/or obligation contained in this Participation Agreement, the Business Rules or the Operating Rules, except as permitted herein. Relying Party may request of GSA permission, which permission shall not be unreasonably withheld, for assignment or succession to a different party of part or all of the rights and/or obligations contained or referenced in this Participation Agreement, the Business Rules or the Operating Rules.

2.7.13 Business Rules and Operating Rules Freeze

The parties agree that the Business Rules or the Operating Rules are not intended to be, and shall not be amended for a period of one year from the date of execution of this Participation Agreement or before October 31, 2006, whichever date shall precede the other. However, by signed amendment to this Participation Agreement, the parties may modify this term as circumstances require.

2.8 Signatures

The undersigned represent and warrant that they have the requisite power and authority to execute this Participation Agreement on behalf of their respective organizations (the Parties), including authority to legally bind their respective organizations to the Binding Documents referenced in Section 3.3.3.2 of the Business Rules.

Relying Party

GSA

3 E-AUTHENTICATION FEDERATION INTERIM BUSINESS RULES

3.1 Title

This document shall be known and may be cited as the “E-Authentication Federation Interim Business Rules”, or, as referenced herein, as “Business Rules”.

3.2 Scope

3.2.1 Scope of Rules

Signatories agree that their signed Participation Agreement, these Business Rules, the Operating Rules and the Binding Documents referenced in Section 3.3.3.2 herein, govern participation in the E-Authentication Federation, administered by the General Services Administration of the United States Federal Government (GSA). The GSA, or its authorized agent, shall approve Credential Services (CSs) of a Credential Service Provider (CSP). Approved Credentials of a GSA Approved CSP must be accepted, validated and relied upon by GSA Approved Relying Parties (RPs). Such acceptance, validation or reliance does not require the use of any additional contract between an Approved CSP and an Approved RP.

3.2.2 Agreements and Conduct Outside Scope of Rules

Nothing in these Business Rules or the Operating Rules shall be construed to prevent Approved CSPs and RPs from executing such additional agreements among themselves as they see fit, including agreements covering the use of services, transactions or Credentials, including identity assertions or parts of such assertions. Any activity covered by other contract arrangements, other than the Participation Agreement, these Business Rules, the Operating Rules or other Binding Documents referenced in Section 3.3.3.2 herein, is subject to the terms of such other contract arrangements, and is outside the scope of these Business Rules. These Business Rules and the Operating Rules are incorporated by reference into the signed Participation Agreements and thereby applicable to the Signatories.

3.2.3 Rules Appearing in Multiple Documents

Any provision of these Business Rules or the Operating Rules that duplicates or emphasizes identical or similar provisions of other Binding Documents referenced in Section 3.3.3.2 governing the E-Authentication Federation shall not be construed as to lessen the enforceability of any other provisions that have not been duplicated or emphasized.

3.3 Participation

3.3.1 Eligibility

A department, Agency, Government sponsored corporation, or other instrumentality, or any State or Local Government is eligible to become a RP within the E-Authentication Federation, provided the requirements set forth in these Business Rules and the Operating Rules are satisfied.

A department, Agency, Government sponsored corporation, or other instrumentality, including a Designated Financial Agent of the United States Federal Government, or any State or Local Government is eligible to become a CSP within the E-Authentication Federation, provided the requirements set forth in these Business Rules and the Operating Rules are satisfied.

A CSP that is part of the United States Federal Government has the right to choose not to provide Credential Services to a RP that is not part of the United States Federal, State, or Local Government.

In addition, any legal entity, including a non-governmental organization, is eligible to become a CSP within the E-Authentication Federation provided the requirements set forth in these Business Rules and the Operating Rules are satisfied.

Any Signatory must continue to abide by the terms of their signed Participation Agreement to remain eligible to participate in the E-Authentication Federation.

3.3.2 Participation Requirements

3.3.2.1 Relying Parties

Approval by the GSA is necessary for a RP to participate in the E-Authentication Federation. A RP must be a Signatory as a prerequisite to approval by the GSA. A party becomes a Signatory RP by executing the Relying Party Participation Agreement with GSA. Each such Relying Party Participation Agreement includes obligations whereby these Business Rules and the Operating Rules, as periodically Approved in writing and amended in accordance with the change control process, are incorporated by reference. Final approval by the GSA is contingent upon the Signatory successfully completing the Boarding Process and Operational Readiness Review.

A Signatory RP must also be Approved according to terms of the Binding Documents referenced in 3.3.3.2, and comply with National Institute of Standards and Technology (NIST) SP 800-53 and the security requirements specified in the Operating Rules.

3.3.2.2 CSPs

Approval by the GSA is necessary for a CSP to participate in the E-Authentication Federation. A party becomes a Signatory CSP by executing the CSP Participation Agreement with GSA. A CSP Participation Agreement may be executed directly with the GSA, or as part of a formal solicitation and procurement process the GSA may

require. Each such CSP Participation Agreement includes obligations whereby these Business Rules and the Operating Rules, as periodically Approved in writing and amended, are incorporated by reference.

A Signatory CSP must also have one or more CSs Approved according to the terms of the Binding Documents referenced in Section 3.3.3.2, herein, including the Credential Assessment Framework Suite (CAF), and be added to the E-Authentication Federation Trusted Credential Service Provider List as a prerequisite to be Approved by GSA to participate in the E-Authentication Federation.

3.3.2.3 End-Users

Any party participating in the E-Authentication Federation as an End-User must have an agreement with an Approved CSP or an entity acting under an agreement, or chain of agreements, with an Approved CSP. Such agreement must contain such minimum terms as are required under these Business Rules and the CSP Participation Agreement. An End-User may be a natural person or any other legal entity, including a corporation. End-Users are Participants in the E-Authentication Federation, but are not Signatories.

3.3.3 GSA Role and Obligations

The GSA is the party responsible for policy and operations related to the E-Authentication Federation. The GSA is responsible for facilitating the roles, relationships and mutual obligations among parties operating in the E-Authentication Federation. The GSA uses Business Rules, Operating Rules and Participation Agreements as a method of documenting these roles, relationships and obligations in a formal and, as needed, enforceable manner. The GSA shall provide processes for determining qualification of any party in the E-Authentication Federation. In the course of such activities, as well as ongoing oversight of Approved Parties and System performance, the GSA shall act as coordinator and policy enforcement body for the E-Authentication Federation. Any GSA approvals or other determinations required by or arising under these Business Rules and the Operating Rules shall not be unreasonably withheld. The GSA may designate offices, departments or other organizational units within the GSA or otherwise within the United States Federal Government to exercise such rights or obligations defined under these Business Rules and the Operating Rules.

3.3.3.1 Operating Authorization

GSA actions in administering the E-Authentication Federation support the authentication component of the United States Federal Enterprise Architecture. The President's Management Agenda of 2001 directed GSA to lead the operation of the E-Authentication Federation, which implements Office of Management and Budget (OMB) M04-04 and NIST SP 800-63.

3.3.3.2 Promulgation and Amendment of Business Rules, Operating Rules and Other Documents

GSA shall formalize the initial set of these Business Rules and the Operating Rules pursuant to its duty to administer and manage the E-Authentication Federation. Amendments to these Business Rules and the Operating Rules must comply with the E-Authentication Federation Change Management Policy. In addition to these Business Rules, the following materials are also formal Binding Documents defining rights, obligations, processes and other binding statements relative to the E-Authentication Federation: the CSP Participation Agreement, the Operating Rules, the Relying Party Participation Agreement, the Credential Assessment Framework (CAF), the Technical Architecture, and the Interface Specification.

3.3.3.3 Relying Party and CSP Approval

The GSA is responsible for determining whether to approve a RP for participation in the E-Authentication Federation, and shall formalize and may amend periodically the requirements for RP approval. The GSA is responsible for determining whether to approve a CSP for participation in the E-Authentication Federation, and shall formalize and may amend periodically the requirements for CSP approval.

3.3.3.4 Service Offerings

To promote use of the E-Authentication Federation, the GSA will facilitate policies for business relationship management, Business Rules, Operating Rules, Participation Agreements and other offerings, and will provide access to or make available various Architectural Components.

3.3.3.4.1 Architectural Components

GSA may implement and make available to Approved Parties Architectural Components to facilitate use of the E-Authentication Federation, including the E-Authentication Portal identified in the Technical Architecture, Step-Down Translator(s), Schema Translator(s) and Validation Services. The GSA may incorporate additional components.

3.3.3.4.2 Interoperability Requirements

The GSA shall operate an interoperability laboratory for the purpose of testing interoperability of products, software, communication specifications and other relevant aspects of current and potential future enhancements to the E-Authentication Federation. Each Signatory CSP and RP shall be responsible for the completion of their own testing in such laboratory in accordance with Section 3.3.6.2 of these Business Rules.

3.3.3.4.3 Federation Operations Center

The GSA shall operate a Federation Operations Center.

3.3.3.4.4 Trusted Credential Service Provider List

The GSA shall formalize, maintain and update as needed a Trusted Credential Service Provider List of Approved CSPs participating in the E-Authentication Federation. This

list shall be a public document and include, at a minimum, the names of each CSP that has been successfully Approved, and the Assurance Level of each Approved CS of that CSP. The GSA shall determine what continuing audit and other compliance requirements shall satisfy maintenance of approval and the terms of these Business Rules and the Operating Rules.

3.3.3.5 Contact Information

For current information related to the E-Authentication Federation and these Business Rules, contact the E-Authentication Program Director of the General Services Administration of the United States Federal Government or see <http://www.cio.gov/eauthentication/>.

3.3.4 Relying Party Role and Obligations

3.3.4.1 Relying Party Boarding Process, Operational Readiness Review and Participation Agreement

As a prerequisite to be Approved to participate in the E-Authentication Federation, a RP is obliged to successfully complete the Boarding Process and Operational Readiness Review, and to execute a Relying Party Participation Agreement with the GSA, thereby agreeing to abide by these Business Rules, the Operating Rules and other Binding Documents referenced in Section 3.3.3.2 of the Business Rules. The Relying Party Participation Agreement incorporates these Business Rules and the Operating Rules by reference.

3.3.4.2 Interface Specifications, Approved Software Use and Upgrade

A RP is obliged to comply with and use the E-Authentication Interface Specification to participate in, communicate through or connect with the E-Authentication Federation. A RP is obliged to use software on The Approved Technology Provider List or interface software otherwise Approved by GSA. In order to maintain approval to participate in the Federation, each RP is obliged to follow requirements set by GSA to stay current with the software on The Approved Technology Provider List.

3.3.4.3 Security and Privacy Compliance

The following Rules apply to any information System supporting the Agency Application (AA) of the RP that is part of the United States Federal Government. An Approved RP is obliged to comply with OMB Circular No. A-130 including Appendix III to OMB Circular No. A-130, with respect to any information technology System of the RP.

An Approved RP is obliged to comply with the Privacy Act of 1974 and OMB M-03-22, including where required, performing a Privacy Impact Assessment (PIA) with respect to the handling of Personally Identifiable Information (PII) of an End-User.

An Approved RP that is not part of the United States Federal Government must prove to the GSA that it is in compliance with equivalent safeguards and relevant requirements. GSA, in its discretion, shall determine whether such approval is sufficient.

3.3.4.4 Reasonable Reliance on Credential

A RP is obliged to reasonably determine for itself whether to rely on the authentication status of an End-User and whether to authorize usage of the AA. In order to determine the authentication status of an End-User, a RP must determine for itself, either through a published Activation process or other procedures, the level of AA Risk, and therefore the needed Assurance Level, as per the guidance in OMB M-04-04 and NIST SP 800-63, using the GSA-provided Electronic Risk and Requirements Assessment (E-RA) tool or any other method it deems acceptable.

3.3.5 *CSP Role and Obligations*

3.3.5.1 CSP Boarding Process, Operational Readiness Review and Participation Agreement

To be an Approved CSP, a CSP must successfully complete the Boarding Process and Operational Readiness Review, including being added to the Trusted Credential Service Provider List. A CSP is also obliged to execute a CSP Participation Agreement with the GSA as a prerequisite to being an Approved CSP for participation in the E-Authentication Federation, thereby agreeing to abide by these Business Rules, the Operating Rules and other Binding Documents referenced in Section 3.3.3.2 of these Business Rules. The CSP Participation Agreement incorporates these Business Rules and the Operating Rules by reference.

3.3.5.2 CSP Continuing Audit Requirement

An Approved CSP is obliged to undergo an audit, no less than annually, confirming compliance with continuing requirements arising out of approval and with the obligations and other relevant terms of these Business Rules, the Operating Rules and the CAF. An audit planned or undergone by a CSP unrelated to the E-Authentication Federation, including an internal audit, may be sufficient to meet this requirement in whole or in part, in the discretion of the GSA. The scope of an audit shall be limited to a CSP's conformance with the Business Rules, Operating Rules, and other Binding Documents. An Approved CSP must report to GSA in a timely manner any negative finding by an auditor that is material to compliance with requirements under any Binding Document referenced in Section 3.3.3.2.

3.3.5.3 Material Change to CSP, Credential Services or Credential

An Approved CSP may be required by the GSA to undergo an additional approval in whole or in part, to re-approve one or more CSs at the same or different Levels of Assurance or to accept suspension or termination of approval and participation in the E-Authentication Federation when audit results indicate material changes in the CSP, the

Approved CSs or in the Credentials it issues or other relevant changes that bring the CSP out of material compliance with continuing requirements.

3.3.5.4 Technical Architecture and Interface Specification

To participate in, communicate through or connect with the E-Authentication Federation, a CSP is obliged to comply with, implement and use the E-Authentication Technical Architecture, the E-Authentication Interface Specification, and all other applicable technical requirements identified in any Binding Document referenced in Section 3.3.3.2 of the Business Rules.

3.3.5.5 Designated Financial Agents

Notwithstanding any prohibition on assignment of rights contained in any Binding Document referenced in Section 3.3.3.2 of these Business Rules, the Department of the Treasury, in its role as a CSP, may designate one or more entities to act as its agent, provided that each such agent is fully subject to all Rules, rights, obligations contained within the CSP Participation Agreement, these Business Rules, the Operating Rules, any other Binding Document referenced in Section 3.3.3.2 of these Business Rules and any other relevant document, practice or procedure of the E-Authentication Federation applicable to an Approved CSP.

CSPs whether principals or agents for CSPs shall be held individually accountable for compliance with Business and Operating Rules.

3.3.6 General Obligations

Every Approved Party is obliged to comply with the following Rules.

3.3.6.1 Federation Security and Reliability

Every Approved Party agrees to coordinate with the GSA in safeguarding the security and reliability of the E-Authentication Federation. GSA may render inaccessible any Node or Architectural Component of the E-Authentication Federation to prevent or cease serious harm to the Federation. Every Approved Party may disable their connection to any Node or Architectural Component of the E-Authentication Federation to prevent or cease serious harm to their Systems or to the Federation. Every Signatory agrees to provide notice to the counter-party Signatory of their Participation Agreement of any such emergency suspension of service prior to, if practicable, or as soon after as reasonably possible. Participation by any Approved Party in the E-Authentication Federation may be suspended under extraordinary circumstances necessary to prevent or cease serious harm to the E-Authentication Federation.

3.3.6.2 Federation Interoperability

To assure the efficacy and operation of the E-Authentication Federation, every Approved Party must demonstrate to the GSA that its interactions and communications through the Federation comply with the E-Authentication Technical Architecture and will

interoperate with the Architectural Components of the Federation. To this end, every Approved Party must conduct tests of its planned Federation interactions and communications in the Interoperability Lab, or through such other process GSA may designate, to demonstrate compliance and interoperability requirements for the Federation have been met.

3.3.6.3 Operational and Ongoing Requirements

Every Approved Party is obliged to comply with application, testing, piloting, production and continuing maintenance requirements set forth by the GSA. These ongoing requirements include continued compliance with the provisions of the CAF, NIST SP 800-53, the security requirements specified in the Operating Rules, and with applicable requirements documents defining operational sufficiency for participation in the E-Authentication Federation. Nothing in this section, however, shall be construed to prevent any Approved Party from extending, adding to or otherwise applying other technologies or services in accordance with Section 3.2.2 of these Business Rules.

3.3.6.4 End-User Consent and Notice

Every Approved Party is obliged to assure that each End-User that is an individual natural person has provided Informed Consent to the sharing of any PII related to such End-User by the Approved Party with any other party operating within the E-Authentication Federation, including any PII contained in a certificate or other identity assertion as included in the Interface Specification. Under these Business Rules, no Approved CSP or Approved RP is permitted to share PII about any such End-User beyond the information provided for in the Interface Specification. Nothing in this section authorizes the sharing of PII about such End-User for purposes of sending commercial solicitations to that user, including marketing or advertising messages.

Every Approved CSP must inform each of its End-Users, prior to the End-User's participation in the E-Authentication Federation, that the End-User must maintain the security of their Approved Credential, including any Token housing their Credential, and must report to the CSP any known or reasonably suspected compromise of such Credential or Token.

In accordance with the Right to Financial Privacy Act, any financial institution providing CSP services must inform each End-User of the categories of information that will be disclosed (name, date of birth, etc.) and obtain the consent of the End-User to disclose that information to the Government. This requirement applies regardless of whether the financial institution is acting on its own or on behalf of a Government Agency.

Every Approved CSP must obtain the affirmative manifestation of assent by each End-User to the foregoing terms, prior to End-User participation in the E-Authentication Federation.

In the case of organizational End-Users, all relevant rights and obligations, including notice requirements and requirements for Informed Consent, must pass through to each natural person acting on behalf of End-User within the E-Authentication Federation.

To the extent that information identified as part of the Dispute Resolution processes described in the Participation Agreements constitutes PII within a System of Records under the Privacy Act of 1974, nothing in those agreements shall be construed to authorize or permit the communication of such information about an End-User who is an individual natural person without that End-User's Informed Consent.

3.3.6.5 Additional Transactions

Approved Parties may conduct transactions and communicate data in conjunction with the E-Authentication Federation in addition to the authentication of an End-User. These additional transactions may be conducted in conjunction with the E-Authentication Federation, but will not be deemed to be within the scope but shall conform with the spirit of the Business Rules and the Operating Rules.

Acceptance of data by an Approved Party shall constitute an agreement for purposes of this subsection.

Notwithstanding the above, the following subsection applies to any such additional transaction.

3.3.6.5.1 Transaction Privacy

Any additional transaction data transferred from an Approved CSP to an Approved RP shall be used solely for the purpose of the agreed transaction and related application and for resolving issues which may arise in the execution of that service. Such data shall not be used or forwarded to any other Government Agency or other party without the written approval of the Approved CSP. Such data shall also be kept only as long as required to perform the defined service, or unless required by applicable laws or other regulations. The Approved RP shall only store and maintain such data in their record keeping Systems once the End-User has verified the information and affirmatively manifested assent, in accordance with any applicable processes and policies of the Approved RP.

4 **E-AUTHENTICATION FEDERATION INTERIM OPERATING RULES**

4.1 **Introduction**

Public trust in the security of information exchanged over the Internet plays a vital role in the E-Gov transformation. The General Services Administration (GSA) makes that trust possible. As part of the President's Management Agenda, the E-Authentication Federation will ultimately enable trust and confidence in E-Government transactions through the establishment of an integrated policy and technical infrastructure for electronic authentication. Through the Federation, citizens and businesses will have simpler access to multiple Agency Applications (AAs) through the re-use of Credentials and established identities. Furthermore, GSA will establish a Federation comprised of Relying Parties (RPs) and Credential Services (CSs).

The E-Authentication concept is best described through the trust relationships among AAs, Credential Service Providers (CSPs) and End-Users. CSPs are commercial or Government entities authorized by GSA to provide Credentials (e.g., Personal Identification Numbers (PINs), Passwords, Digital Certificates) to potential End-Users for access to Government Systems. AAs are Government applications, Systems or services that rely on (or trust) the authentication/ CS of CSPs. End-Users are people or organizations that have Credentials issued by a CSP and desire to use that Credential to conduct business with an AA. It is the management of trust among these entities (AA, CSPs and End-Users), that is the essence of the Federation.

4.1.1 **Purpose**

This document defines operational requirements for Federation Members. The Operating Rules defined herein ensure that the best interests of the Federation, specifically the Integrity of the operating environment, are maintained. Operating Rules are in addition to requirements specified in various documents that are identified within the body of this document. Where necessary, these documents are referenced and several of the documents are included as an appendix to this document.

The Operating Rules described herein are ***mandatory*** except for those that explicitly grant latitude or subjective judgment or where official waiver is granted by GSA. Federation Members are required to formally agree to these Operating Rules. End-User requirements are to be provided by Federation Members and are not within the scope of this document.

4.1.2 **Document Organization**

This document provides specific areas that a Federation Member must implement. The document is organized according specific Operating Rules and is subsequently broken down into specific requirements for each area. Where necessary, additional requirements are identified by reference and the appropriate document is listed. This document also

contains several appendices that provide supporting information or references that are defined within the body of the Rules.

4.2 Privacy

End-User privacy is a high priority for GSA. Federation Members must strive to protect End-User privacy at all times. The following Rules apply:

Reference Number	Privacy
4.2.1	PII may be provided to RPs for establishing End-User identity; no other use of this information is permitted unless: <ol style="list-style-type: none">1. The CS provides written consent to the RP, and2. The End-User provides explicit permission to the CS.
4.2.2	Federation Members must comply with all privacy laws and regulations as applicable, whether or not referenced specifically by Federation Rules and guidance.
4.2.3	Federation Members must comply with the Privacy Act of 1974 to the extent applicable.

4.3 Logs

Federation Member Systems and applications will need to produce particular log records. To maintain a level of security and consistency across the Federation, the following Rules apply:

Reference Number	Logs
4.3.1	Assertion-based RPs must log transaction identifier (TID) ¹ , CS identifier (CSID), End-User identifier (UID), assertionid, Assurance Level, and subject name (commonName) for every assertion received.
4.3.2	Assertion-based RPs should log artifacts and every element in the assertion ² .
4.3.3	CSs sending Security Assertion Markup Language (SAML) assertions must log assertionid, UID, and TID for every assertion.
4.3.4	Assertion-based Federation Members must have the ability to correlate local session identifiers with associated authenticated transactions.
4.3.5	CSs sending SAML Assertions should log artifacts and all assertion elements.
4.3.6	Certificate-based RPs must log the End-User certificate and relevant validation activities.
4.3.7	RPs must be able to track the activity of End-Users from the receipt of external authentication through the end of the Business Transaction ³ .
4.3.8	Federation Members must have processes and controls that ensure that System Log Files can be used as persuasive evidence in a court of law ⁴ .
4.3.9	The Federation Portal will record TID, CS selected, and AA selected at the Portal.
4.3.10	All logs relevant to these Rules must include a date and timestamp for every log entry.
4.3.11	CSPs must keep the logs defined in these Rules in accordance with Federal, State, Local and regulatory requirements or a minimum of 3 years.
4.3.12	RPs must keep related logs of transactions in accordance with Federal, State, Local and regulatory requirements or a minimum of 3 years.
4.3.13	Production environment logs required by these Rules must be backed up, including the use of on offsite storage location that has appropriate environmental and security controls.

4.4 Reporting

Communication amongst Federation Members is a key component of the operations of the Federation. GSA may share information required in this section with Connected Members. The following reporting Rules apply:

Reference Number	Reporting
4.4.1	<p>RPs must provide a monthly report containing each authenticated session, which should be ASCII-encoded text in comma-separated values format. Contents are as follows:</p> <ol style="list-style-type: none"> 1. Timestamp - Must include date and time. Time should be specified in Greenwich Mean Time (GMT) and include hours, minutes, and seconds. Will have the format mmddyyyy:hh:mm:ss . 2. TID - Will have the format P-mmddyyyy-{luid}. The luid is a base64 encoded representation of 64 bits that is unique to a transaction. 3. AAID - As published in the Federation Metadata. 4. CSID - As published in the Federation Metadata; if a certificate is used, the contents of this element should consist of the issuer of the certificate presented by the user. 5. Assertion Validation (success/failure) - Should represent the successful receipt of an assertion or successful validation of the presented end-user's certificate. Values: 0 = Failure & 1 = Success.
4.4.2	<p>CSPs must provide a monthly report containing each authenticated session, which should be ASCII-encoded text in comma-separated values format. Contents are as follows:</p> <ol style="list-style-type: none"> 1. Timestamp - Must include date and time. Time should be specified in GMT and include hours, minutes, and seconds. Will have the format mmddyyyy:hh:mm:ss. 2. TID - Will have the format P-mmddyyyy-{luid}. The luid is a base64 encoded representation of 64 bits that is unique to a transaction. 3. AAID - As published in the Federation Metadata. 4. CSID - As published in the Federation Metadata. 5. Assertion Validation (success/failure) - Should represent the successful, completed transmission of an assertion. Assertions that are not fully transmitted must be considered to have failed. Values: 0 = Failure & 1 = Success.
4.4.3	<p>GSA will publish reports on the Federation Portal traffic to the Federation every month via means accessible only to active Federation Members in good standing. Reports will include the number of page views and the number of transactions initiated.</p>

4.4.4	GSA will provide Federation activity reports to Federation Members every month via means accessible only to active Federation Members in good standing. Reports will include the total number of Federation authenticated sessions.
4.4.5	All reports will be a signed and encrypted Secure/Multipurpose Internet Mail Extension (S/MIME) email using digital certificates that are trusted by the Federation ⁵ until the email is incapable of handling the data (i.e. size).

4.5 Monitoring

To ensure that the System maintains a level of security, Integrity and Availability, a certain level of monitoring must occur. The following Rules provide a minimum set of requirements for achieving the level of monitoring necessary to maintain the Federation. The following Rules apply:

Reference Number	Monitoring
4.5.1	GSA will publish monitoring service information, such as IP address, location, and contact information, at least two (2) weeks in advance of the start of monitoring or the implementation of changes in monitoring service.
4.5.2	GSA, or its designated representative, will monitor the Availability of the Federation Member's web-based E-Authentication-enabled applications during the agreed upon hours of operation, to ensure that the services are being delivered to end-users according to the standards contained in Section 4.9 and Appendix D.
4.5.3	Federation Members must monitor the Availability of their own web-based E-Authentication-enabled applications in accordance with Section 4.9 and Appendix D.
4.5.4	GSA reserves the right to use third parties to run tests and to change monitoring tools at its sole discretion, provided the scope of such tests be mutually agreed between Federation Members and GSA and subject to the terms of this agreement.
4.5.5	All tests must be targeted at "top level" load balancing Uniform Resource Locators (URLs) and URLs will be selected based on the criticality of functionality to the Federation Portal and will be designed to exercise components of Federation's infrastructure involved in delivery of the services provided by Federation RPs ⁶ .
4.5.6	Compliance with the terms of Section 4.9 and Appendix D will be evaluated based on the Availability of the services provided by Federation RPs and CSs.
4.5.7	Data collected from all tests will be evaluated using three different methods: Availability, minimum acceptable response time, and average response time (see Appendix D).
4.5.8	GSA's measurements of performance and Availability compliance data will be available to Connected Members ⁷ .
4.5.9	On a monthly basis, all testing evaluation methods must pass to be considered in compliance, based on the criteria in Appendix D and the measurements made by GSA.

4.5.10	If measurements made by GSA leads to a determination of non-compliance (fail), a joint analysis will be conducted to determine the source of the situation. The Federation Member and GSA will work to resolve the situation if it is in either's control. Otherwise the Federation Member will be deemed compliant. This joint determination will be made prior to disseminating or publishing compliance and Availability information to Connected Members.
4.5.11	Federation Members do not need to pass every periodic test for every window in order to pass on a monthly basis (see Appendix D).
4.5.12	A failure to pass any of the three testing evaluation methods on a monthly basis will constitute non-compliance for the month.
4.5.13	Tests will be run at five-minute intervals and tests may be run from monitors located within GSA hosting sites or from external monitors.
4.5.14	For external monitors, tests will be run from at least three domestic locations.
4.5.15	Certain time frames, testing locations or URLs may be exempt from calculation for a variety of reasons: testing location unavailable, tech window, change window, mutually agreed scheduled maintenance windows, etc., or Internet problems beyond the reasonable control of either party.
4.5.16	Exempt items will be excluded from the Availability and performance compliance calculations.

4.6 Performance Requirements

Availability of the Federation is critical and this section provides Federation Member performance requirements. Appendix D also provides test and measurement criteria that Federation Members should use as a guide when implementing performance requirements. Performance degradation will be treated as an incident described in Section 4.9. The following Rules apply:

Reference Number	Performance
4.6.1	All Federation Member services must achieve 99% Availability during scheduled up time as defined by the Federation Member.
4.6.2	Federation Members must ensure routine maintenance requiring downtime must not be scheduled 6 a.m. to 9 p.m. (Eastern Time (ET)) Monday through Friday.
4.6.3	Federation Members must provide planned up time and downtime schedules to GSA, and GSA will provide them to the Connected Members.
4.6.4	Federation Members must monitor their own sites for Availability and response time.
4.6.5	Federation Members must notify GSA of any unscheduled downtime as soon as detected in compliance with escalation policies defined in Section 4.9.
4.6.6	Response time will include Domain Name System (DNS) resolution, connect (i.e., TCP 3-way handshake), and 1 st byte transferred.
4.6.7	Federation Members will be monitored by GSA to ensure Availability and adequate response times ⁸ .
4.6.8	GSA will conduct tests using the test criteria listed in Appendix D.
4.6.9	GSA shall ensure the Federation Portal is available 99.9% of the time, 24x7.
4.6.10	GSA shall ensure that E-Governance Certificate Authority (E-GCA) revocation data is available 99.9% of the time, 24x7.
4.6.11	Federation Members will display down pages during planned or unplanned service unavailability.

4.7 Style Guidelines, Narrative Elements, Branding and Logos

GSA will establish, provide, and maintain Federation Style Guidelines, which will include Approved content for use on Federation Member sites. Use of Federation Member branding and logos is subject to the intellectual property terms defined in Section 1.7.8 (CSPs) and 2.7.3 (RPs). This section provides requirements for Web sites linking to the Federation Portal in terms of presenting visual and narrative elements that identify those sites as Members of the Federation. The following Rules apply:

Reference Number	Style Guide and Narrative Elements
4.7.1	<p>Federation Member sites must contain language that describes and explains E-Authentication in a manner consistent with the language loaded on to the Federation Portal page.</p> <ol style="list-style-type: none">1. GSA will provide an “E-Authentication Primer,” which Federation Members may display in whole or in part from their sites.2. This Primer must be accessed via a clear link that leads to:<ol style="list-style-type: none">a. A page within the Federation Member’s site; orb. A pop-up window off the Federation Member’s site; orc. The Federation Portal in a separate window.
4.7.2	<p>Federation Member sites must contain language that describes and explains E-Authentication in a manner consistent with the language loaded on to the Federation Portal page.</p> <ol style="list-style-type: none">1. GSA will provide an “E-Authentication Frequently Asked Question (FAQ),” which Federation Members may display in whole or in part from their sites.2. This FAQs must be accessed via a clear link that leads to:<ol style="list-style-type: none">a. A page within the Federation Member’s site; orb. A pop-up window off the Federation Member’s site; orc. The Federation Portal in a separate window.

Reference Number	Style Guide and Narrative Elements
4.7.3	<p>Federation Member sites must provide explanatory / educational references to the Federation Portal and related processes at site pages that link directly to the Portal.</p> <ol style="list-style-type: none">1. In the case of RPs, this means at a minimum the page from which the user is sent to the Federation Portal to select a CS.2. In the case of the CSP, this means at a minimum the page from which a user is sent to the Federation Portal to select Government service, or RP, from which to access services.3. GSA will provide Federation Members a copy of the pages that will be used as appropriate in whole or in part.

Reference Number	Branding and Logos
4.7.4	Federation Members must display the Federation logo.
4.7.5	<p>Only those sites explicitly authorized by GSA may display the Federation logo.</p> <ol style="list-style-type: none">1. All Federation Member Websites.2. Non-Federation Member sites may also be authorized at the discretion of GSA.3. GSA will provide electronic files containing the logo to authorized parties.
4.7.6	The logo must be displayed unmodified, unless modification is explicitly Approved by GSA.
4.7.7	The logo must be displayed on each page of the Federation Member's site that links directly to the Federation Portal.
4.7.8	The logo must be displayed on each page within the Federation Member site that lists partner or affiliate Web sites / services. The logo must not be conveyed by a Federation Member site to any partner or affiliate Web site / service, even if that site is also a Federation Member.
4.7.9	The logo will be made available in .jpg and .gif format.
4.7.10	Maximum size specification for use at the Federation Member site is: <ul style="list-style-type: none">• Width: 140 pixels• Height: 40 pixels

Reference Number	Branding and Logos
4.7.11	Federation Member logos will be made available to GSA in .jpg and .gif format.
4.7.12	Maximum size specification of the Federation Member logo is: <ul style="list-style-type: none">• Width: 140 pixels.• Height: 40 pixels.
4.7.13	Federation Members must provide GSA with branding information, including logos, solely for use in the Federation Portal. This material will be provided and used unaltered.
4.7.14	Federation Members must use Federation branding information only as allowed in these Federation Style Guidelines.
4.7.15	Federation Members must not use other Federation Members branding information without explicit written permission from the Federation Member.

4.8 Security Requirements

The security requirements are intended to protect and secure Federation Member information assets and application Systems from threats, whether internal or external, deliberate or accidental. They aim to ensure the Availability, Integrity, and Confidentiality of information to the extent required by GSA. The objectives of the requirements are:

- To ensure that GSA information assets such as Federation Member and transaction information are pragmatically protected on a cost-effective basis and to a level that allows the Federation to fulfill its mission and operate within acceptable levels of Risk to information assets.
- To provide an indication of the mandatory provisions that should be adhered to.
- To establish standards for the means by which information exchanged with Federation Approved Parties will be controlled and safeguarded.

This section defines the minimum-security requirements throughout the Federation System and provides a template for consistent application of these requirements. The security requirements are organized by area. The following Rules apply:

Reference Number	General
4.8.1	CSPs must comply with the requirements of the Credential Assessment Framework (CAF) Suite.
4.8.2	RPs must attest to compliance with National Institute of Standards and Technology (NIST) SP 800-53 as required by Federal Information Security Management Act (FISMA).
4.8.3	Security requirements for protocols and messaging are included in the E-Authentication Interface Specifications. Federation Members must comply with the requirements of the interface specifications.
4.8.4	Federation components operated by GSA must abide by the FISMA and GSA Information Technology (IT) Security Policy, CIO HB 2100.1A.

Reference Number	Confidential Information and Electronic Messaging
4.8.5	All confidential information shall be marked as confidential by the data/information owner, and the receiver shall protect it as such unless otherwise specified by these Operating Rules.

Reference Number	Confidential Information and Electronic Messaging
4.8.6	For the purposes of these Rules, confidential information will be defined as whatever is marked as confidential by the information owner.
4.8.7	All Federation Member personnel who have access to, or are authorized to work on Systems/devices processing or storing, End-User data and/or confidential information must participate in a suitable background evaluation that includes financial and criminal record checks.
4.8.8	Federation Members must employ security measures to safeguard confidential information that is being stored, processed, transported, or disposed. These measures must apply to paper files, tape backups, call logs, mail messages and other media.

Reference Number	Security Policies and Procedures
4.8.9	<p>GSA, or its authorized representatives, will have the right to perform a review of Federation Member's relevant security, business continuity, data center and operations controls (at GSA's own expense) in response to a security incident.</p> <ol style="list-style-type: none">1. Federation Members must grant GSA and its representatives reasonable access, subject to the Federation Member's standard security policies, during normal business hours and upon two (2) weeks notice, to the relevant portion of the Federation Member's records and facilities as they relate to their Participation Agreement.2. Federation Members must provide GSA, or its authorized representatives, such information and assistance as reasonably requested in order to perform such a review.

Reference Number	Security Policies and Procedures
4.8.10	<p>Federation Members must allow GSA, or its designee to perform regular reasonable Network, security vulnerability assessments on any of the Federation Member's Internet accessible Systems and servers utilized by the Federation Member that host Federation confidential information in order to measure vulnerability of the Network to external cyber attack. A list of externally facing Systems must be provided to GSA and updated as changes occur.</p> <ol style="list-style-type: none"> 1. GSA and the Federation Member will work to establish mutual agreement on date and time of security scans. 2. Two (2) weeks prior to performing the assessment, GSA will provide the Federation Member with the following information: <ul style="list-style-type: none"> • Date, time, and duration of security scan; • IP address performing the test; and • Name, phone number and pager of person performing the scan. 3. No destructive or intrusive testing (brute force or denial-of-service (DOS)) will be performed. 4. As the servers utilized by the Federation Member are Internet accessible, any user on the Internet can perform these tests, so long as the tests will not have a negative impact on the Federation Member's Network or data center. 5. GSA will have support available to address any negative consequences as a result of the assessment.
4.8.11	<p>GSA will provide each Federation Member access to the security reports produced as part of the review of that Federation Member's security controls and the security vulnerability assessments, and the Federation Member agrees to take commercially reasonable steps to address the concerns contained in such reports within timeframes mutually agreed to by the Federation Member and GSA. Federation Members must track the actions taken to address any concerns contained in the security reports to ensure the agreed upon changes are implemented as agreed to and must report the progress of such actions to GSA.</p>
4.8.12	<p>Federation Members must mitigate against known vulnerabilities on Systems providing services to the Federation. Acceptable mitigation may consist of active remediation (e.g., patches, coded updates, firewall changes, etc.).</p>
4.8.13	<p>GSA must be notified of any proposed modifications that may materially impact a Federation Member's overall security posture at least ten (10) business days prior to implementation.</p>

Reference Number	Security Policies and Procedures
4.8.14	Federation components operated by GSA must comply with GSA security policies and procedures, including Certification and Accreditation (C&A).

Reference Number	System Security
4.8.15	Federation Members, their contractors, and their agents must ensure that all sensitive and confidential information is secured against unauthorized access.
4.8.16	When outside a firewall and attempting to access a Federation System root, strong authentication procedures (i.e., two-factor authentication, such as use of Password & hard Token or a passcode & biometric System) are required.
4.8.17	Federation Members will ensure that Systems Passwords are sufficiently complex (e.g., length, construction, frequency of change, etc.) to reduce the likelihood of System Password compromise.
4.8.18	All System access will be configured by the Federation Member to prevent an intruder from gaining access to the System.
4.8.19	All transaction requests denied access must not reveal detailed information about the Federation Member's hardware/software configuration.
4.8.20	All user input and data, including URL name-value arguments, will be checked for its appropriateness based on its format, size and validity and any inputs not conforming to those parameters must be rejected.
4.8.21	The servers utilized by Federation Members will not have the ability to remotely execute arbitrary outside requests, except for remote management performed over an encrypted, authenticated channel.
4.8.22	For Internet exposed Systems providing services to the Federation, the following Rules apply: <ol style="list-style-type: none">1. All routers used within Federation Member Systems are to be segmented to provide a Federation Member's Network traffic in isolation of other Network traffic; the Federation Member's segment contains a packet filter which has been configured to disallow access to all protocols.2. When a protocol (such as http and https) is allowed to call into the Federation Member System, that protocol must be explicitly exceptioned into the firewall infrastructure.
4.8.23	Monitoring procedures of the firewall and supporting Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) will promptly inform Federation Members of any unauthorized access or otherwise suspicious attempts to access secured portions of the System across the Network.

Reference Number	System Security
4.8.24	Federation Member's Systems must have logging enabled and sufficient information must be captured in the logs to provide for individual accountability of all access to, or attempts to access, the data stores that contain confidential information.
4.8.25	Systems storing or processing sensitive and confidential information must be stripped and be configured with only enabled services and must have unnecessary and unused services disabled. It is recommended that unneeded services be removed.

Reference Number	Physical Access Control
4.8.26	Federation Members must implement physical Access Controls to secure access to the location, computer room(s), computer equipment and confidential information, including those locations managed by third party data centers.
4.8.27	Sensitive areas, such as data centers, must be monitored 24x7.
4.8.28	Systems storing or processing confidential information must be physically isolated and access must be granted to only authorized personnel.
4.8.29	Access must be removed from terminated and transferred employees prior to or upon termination or transfer.
4.8.30	All access to such areas storing or processing confidential information must be logged for audit purposes and made available to GSA during the conduction of security inspections.
4.8.31	Unauthorized access or access attempts, or other significant security incidents, resulting in breaches of the Federation Member's physical Access Controls must be reported to GSA after a Federation Member obtains knowledge of such events in accordance with the time frame set forth for severity one incidents (See Section 4.9).
4.8.32	Federation Members must use commercially reasonable efforts to terminate any breaches of its physical Access Controls immediately after detection.

4.9 Incident Response

This section defines the requirements for managing an incident. An incident is an event that has a material adverse affect on a Federation Member System or service including but not limited to the following:

- Unwanted disruption or denial of service;
- Unacceptable site performance or Availability;
- The unauthorized use of a System for the processing or storage of data; or
- Unauthorized changes to System hardware, firmware, or software characteristics.

Incidents can take many forms and the following Rules apply:

Reference Number	Incident Response
4.9.1	All Federation Members are responsible for reporting any known security incident promptly to GSA according to the escalation procedures that will be published periodically.
4.9.2	For any significant security incident that has led to a breach or compromise of sensitive and confidential information. Federation Members must present GSA with documentation of the cause of the security incident, remedial steps, and future plans to prevent a recurrence of the security incident.
4.9.3	When GSA initially detects a problem or a CSP or RP reports a problem or incident, GSA in consultation with the Federation Member, will first classify the problem or incident according to its severity and nature in accordance with the severity table located in this section.
4.9.4	When GSA becomes aware of an error or problem, either on its own accord or following notification made by a Federation Member, GSA will respond using the criteria listed in this section.
4.9.5	GSA will use commercially reasonable efforts to contact the Federation Member's technical contacts via telephone, pager, and email whenever an incident occurs.
4.9.6	GSA will provide the escalation contacts in regards to outages or change management in accordance with the Federation Change Management Policy.
4.9.7	Contact information must be provided to GSA, who may provide it to Connected Members.
4.9.8	For any incident, including dispute resolution, occurring in the last six (6) weeks, Federation Members must be capable of accessing relevant logs for forensic analyses within 24 hours.

Reference Number	Incident Response
4.9.9	For any incident that is six (6) weeks or older, Federation Members must be capable of accessing relevant logs for forensic analyses within 72 hours.
4.9.10	<p>Escalation procedures for responding to security incidents that affect, or could reasonably be expected to affect, Federation's confidential information or any Systems on which the information is stored or processed, are set forth in these Operating Rules.</p> <ol style="list-style-type: none">1. Without limiting the forgoing, Federation Members must notify GSA of any significant security incident (significant security incidents must be deemed to include, without limitation, any known attacks on or improper disclosure of Personally Identifiable Information (PII), Personal Health Information or any other personally identifiable End-User data) that breaches, compromises or threatens the Confidentiality, Integrity and/or Availability of GSA confidential information within the time frame set forth for Severity One incidents.2. Federation Members must use reasonable business efforts to respond to security incidents and keep GSA informed of the incident, actions taken to respond to it and measures taken to correct it in accordance with the incident management procedures set forth in this section.3. At no time must the Federation Member allow any security breach or compromise to persist for any amount of time in order to determine the identity of the perpetrator or for any reason, except as required by law or as deemed necessary to stop the compromise.
4.9.11	<p>For any significant security incident that has led to a breach or compromise of the Federation's sensitive information, Federation Members must present GSA with documentation of the cause of the security incident, remedial steps, and future plans to prevent a recurrence of the security incident in accordance with the incident management procedures set forth in these Operating Rules.</p> <p>If a Federation Member's proposed measures are not deemed acceptable, based on GSA's reasonable judgment, Federation Members must, upon receipt of written request from GSA, enter into good faith negotiations to address the differences and provide security fix within the time frames for providing solutions set forth in these Operating Rules.</p>

The following classification scheme will be used to categorize problems:

Classification	Criteria
Severity One:	Business Critical Failures <ul style="list-style-type: none">• Issues that result in the outage of the entire service provided by GSA under this Agreement to the End-Users.• Any situation that prevents new End-Users from accessing or using the applicable Customized Pages or the Tools, or existing End-Users from receiving their End-User data.• Issues or software defects that result in a significant security exposure (i.e., disclosure to unauthorized third parties of personally identifiable health information of End-Users or other personally identifiable End-User data).• Significant End-User data quality issue (missing, incomplete or incorrect End-User data with significant impact on End-User experience or on the Integrity of End-User data).• Outage, significant slowdown, etc. (caused by failures related to the Tools or otherwise within GSA's reasonable control) which materially impacts or disables major functions from being performed and for which no workaround is available.
Severity Two:	Business Defect with Workaround <ul style="list-style-type: none">• Any problem that impacts the user's ability to use a major feature or function included in the Tools or the Customized Pages but does not prevent all useful work from being performed or does not disable major functions.• Minor End-User data quality issue• Software defects that result in unrecoverable End-User data loss or corruption but for which a work around exists.
Severity Three	Non-material Error <ul style="list-style-type: none">• Errors or non-conformity to specifications that have a minor impact on service performance.• A defect that affects the user's ability to use minor features/functionality included in the Tools or the Customized Pages.

Reference Number	Severity One Incident Response Rules
4.9.12	For severity one incidents, GSA and effected Federation Members will make best efforts to provide telephone acknowledgement of report of error, or problem, within 15 minutes (or as promptly as possible thereafter), provided that such telephone acknowledgement shall in all cases be provided within 30 minutes. Incident updates should be provided on an hourly basis.
4.9.13	For severity one incidents, Federation Members and GSA will assign dedicated resources immediately and continually work the problem until it is resolved.

Reference Number	Severity Two Incident Response Rules
4.9.14	For severity two incidents, Federation Members and GSA will provide telephone acknowledgement of report of error, or problem, within 60 minutes. Incident updates will be provided every two hours.
4.9.15	For severity two incidents, Federation Members and GSA determine a problem correction plan by the end of next business day.

Reference Number	Severity Three Incident Response Rules
4.9.16	For severity three incidents, Federation Members and GSA will provide telephone or email acknowledgement of report of error or problem within 24 hours. Incident updates will be provided on a daily basis.
4.9.17	For severity three incidents, Federation Members and GSA will determine a problem correction plan within five (5) business days.

4.10 Metadata

Metadata will be shared between Federation Members. The following Rules apply:

Reference Number	Metadata
4.10.1	Federation Members must make all Metadata ⁹ available to GSA who will share it with Connected Members and configure the Portal accordingly.
4.10.2	Federation Members must notify GSA of any planned Metadata changes no less than 6 weeks in advance of the changes.
4.10.3	Federation Members must respond to changes in other Federation Members' Metadata within 45 days of notification by GSA.
4.10.4	Federation Members must confirm receipt of Metadata change notices upon receipt.
4.10.5	GSA shall determine, issue, publish, and track AAID and CSID values as defined in the Technical Suite.
4.10.6	GSA shall maintain an up to date record of Federation Metadata and provide relevant excerpts to Federation Members as appropriate.

4.11 Configuration Management

The following Configuration Management Rules apply:

Reference Number	System Changes
4.11.1	GSA must be notified in advance of any substantial changes that affect other Federation Member Systems.

Reference Number	Change Management
4.11.2	Federation Members must comply with Federation Change Management Policy (see Appendix F).
4.11.3	Assertion-based CSs must establish a SAML connection with new Compatible RPs of the Federation within 90 days of the new Federation Member completing the Federation Boarding Process. CSs may delay these new connections so that no more than three (3) new RP connections are established in any given 90 day period.
4.11.4	Assertion-based RPs must establish a SAML connection with new Compatible CSs in the Federation within 90 days of the new Federation Member completing the Federation Boarding Process. Assertion-based RPs may delay these new connections so that no more than three (3) new CS connections are established in any given 90 day period.
4.11.5	GSA will publish Federation Member candidate status, including expected boarding completion date and Federation Member compatibility ¹⁰ .

4.12 Optional Attributes

The technical suite references some attributes of the assertion that are optional. The following Rules apply:

Reference Number	Optional Attributes
4.12.1	Assertion-based Federation Members may elect not to receive optional attributes.
4.12.2	Assertion-based RPs must notify GSA if any restrictions on optional attributes exist before going live.
4.12.3	Before going live, CSs sending SAML Assertions must notify GSA of which attributes they are willing and able to assert.
4.12.4	CSs sending SAML Assertions must not send attributes that RPs are prohibited from receiving.
4.12.5	GSA shall maintain records of the capabilities and restrictions related to optional attributes in the Federation. <ol style="list-style-type: none">1. These capabilities and restrictions must be incorporated into rollout planning as new Federation Members join the Federation.2. GSA will notify Federation Members of these capabilities and restrictions for all Connected Members.
4.12.6	Federation Members must notify GSA in the event of any changes in capabilities or restrictions.

4.13 Add-on Services

The technical suite provides a mechanism for additional services to be added to the trust relationship established between Federation Members¹¹. The following Rules apply for any of these additional services:

Reference Number	Requirement
4.13.1	Federation Members must notify GSA of the existence and nature of these services.
4.13.2	GSA will assist in the issuance of the service specification throughout the Federation if desired by the Federation Members. If requested by Federation Members, GSA will document the technical specification of how add-ons operate as part of the framework. Specifications will include explanations of data used in add-on services.
4.13.3	Add-on services are considered equal in their treatment of the E-Authentication architecture and Operating Rules. They will also adhere to the same laws and policies governing the architecture.
4.13.4	Add-on services will not require a separate agreement between a CSP/Letter of Designation (LoD) and the RP.

4.14 Time Synchronization

For security and operational purposes, it is important that each Federation System have time synchronization. The following Rules apply:

Reference Number	Requirement
4.14.1	Federation Member Systems must run time synchronization software such as using NIST or Global Positioning Systems (GPS) servers.

4.15 End-User Service

The following End-User service Rules apply:

Reference Number	Requirement
4.15.1	Federation Members must make customer service contact information available to GSA.
4.15.2	Federation Members are entitled to use standardized customer service materials provided by GSA.
4.15.3	GSA shall provide telephone support from 8:00 a.m. to 8:00 p.m. (ET) to assist in identifying and resolving service problems and in answering questions related to the operational use of the services.
4.15.4	GSA shall make technical support personnel available from Monday through Friday 6:00 a.m. to 9:00 p.m. (ET) to assist identifying and resolving problems.
4.15.5	GSA shall provide emergency support on a 24x7 basis to solve problems which render the Federation inoperable to users or impair their functionality significantly (See Section 4.9 for Severity Levels).
4.15.6	As part of emergency support, GSA shall provide, and update, as needed, a list of individuals to be paged in resolution of such emergencies.

4.16 Points of Contact

As mentioned in an earlier section of the Rules, communication is a key element to the operation of the Federation. As such, the following Rules apply:

Reference Number	Requirement
4.16.1	All Federation Members must establish a principal point of contact (PPOC) for Federation communications that is available during their normal business hours. Alternatives must be established during vacation or travel.
4.16.2	The PPOC must be reachable during their normal business hours.
4.16.3	Each Federation Member must provide contact information for 2 secondary points of contact (SPOC) in the event the PPOC cannot be reached.
4.16.4	The PPOC and SPOC must be able to reach policy, technical, security, and operational representatives for their organization as needed to meet the requirements of these Rules.
4.16.5	GSA shall maintain a contact list with these point of contacts (POCs) and facilitate coordination and collaboration as needed and appropriate.
4.16.6	Each Federation Member must provide information on customer service channels to GSA for use in End-User assistance.
4.16.7	GSA shall maintain a customer service contact list for Federation Members and provide relevant information to Federation Members.
4.16.8	Federation Members must have on-call personnel available after normal business hours that are capable of acting as PPOC for emergency situations.
4.16.9	GSA will maintain an email address that will allow Federation Members to submit reports.

4.17 GSA Architecture Components

GSA shall provide the following in regard to architecture components:

Reference Number	Requirement
4.17.1	GSA shall make available the Federation Portal as defined in the Technical Suite.
4.17.2	GSA shall make available a Governing Authority Certification Authority as defined in the Technical Suite.
4.17.3	GSA shall make available one (1) or more Step Down Translators (SDTs) as defined in the Technical Suite.
4.17.4	GSA shall make available facilities needed for interoperability testing, including product testing and Federation Member acceptance testing.
4.17.5	GSA shall make test portals available for Federation Member integration testing as needed.
4.17.6	GSA shall maintain technical interface specifications.
4.17.7	GSA will provide, either directly or via a third-party, physical support of the GSA Systems 24x7, including support of power, air conditioning, physical security, and physical changes to existing Systems.

4.18 Document Management

The following document management Rules apply:

Reference Number	Requirement
4.18.1	<p>GSA shall establish positive document control on all documentation distributed to the Federation.</p> <ol style="list-style-type: none">1. Each document will be assigned a configuration item number and a version number.2. Any updates to those documents will trigger a notification to the user group.

4.19 Authoritative Documents

The following documents, as amended from time-to-time, are included by reference and are considered authoritative:

Reference Number	Requirement
4.19.1	The CAF Suite.
4.19.2	The Technical Suite.

4.20 Official Waiver(s)

While it is mandatory that each Federation Member sign a Participation Agreement (CSP or RP) stating they will adhere to the requirements set forth in the Federation Business and Operating Rules, there may be times when a Federation Member will be unable to satisfy certain requirements due to technical or operational limitations. In the event that a Federation Member may need a waiver, the process for issuing the waiver will be governed by the following guidelines:

Reference Number	Official Waiver(s)
4.20.1	Only the GSA Manager of the Federation can approve waivers. Any disputes will be resolved by the GSA Program Executive (PE) or the GSA Deputy Program Manager. In the event of disputes that cannot be resolved by the PE or Deputy, the “court of last resort” for waiver disputes will be a standing committee of the GSA Executive Steering Committee (ESC), populated by at least two representatives from Agencies that are Federation Members and in good standing with the Federation.
4.20.2	The GSA Manager of the Federation shall ensure that no waiver materially effects the security and operational Integrity of the Federation. In addition, there will be no permanent waivers.
4.20.3	Waivers and supporting material will be shared among connected Federation Members.
4.20.4	Applications for waivers must be submitted using the Waiver Request Form, which will be available from GSA.

APPENDIX A: GLOSSARY

Term	Definition
Access Control	Mechanisms and policies that restrict access to computer resources and/or facilities.
Activation	Activation is the process of mapping information contained in either the SAML Assertion or the public key certificate with the Agency Application's own database of users.
Agency	A Government owned corporation, which is considered a RP or CSP in regard to the Federation.
Agency Application (AA)	E-Government applications that perform some business function online. If an E-Government application has multiple interfaces (e.g., administration and service application), each interface with distinct authentication requirements is considered a stand-alone AA. AAs manage all Business Transactions and all End-User authorization decisions.
Approved	Acceptance by the GSA to participate in the E-Authentication Federation, or other inclusion or use in the E-Authentication Federation.
Approved Credential	A Credential issued to an End-User by an Approved Credential Service of an Approved Credential Service Provider
Approved Credential Service Provider	A Credential Service Provider or authorized agent that has been Approved by the GSA to participate in the E-Authentication Federation.
Approved Party	An Approved Relying Party, Credential Service Provider, or authorized agent.
Approved Relying Party	A Relying Party or authorized agent that has been approved by the GSA to participate in the E-Authentication Federation.
Assurance Level	<p>Level of trust, as defined by the OMB Guidance for E-Authentication. This guidance describes four identity authentication Assurance Levels for E-Government transactions. Each Assurance Level describes the Agency's degree of certainty that the user has presented an identifier (a Credential in this context) that refers to his or her identity. In this context, assurance is defined as 1) the degree of confidence in the <i>vetting process</i> used to establish the identity of the individual to whom the Credential was issued, and 2) the degree of confidence that the individual who uses the Credential is the individual to whom the Credential was issued. The four levels of assurance are:</p> <ul style="list-style-type: none"> Level 1: Little or no confidence in the asserted identity's validity. Level 2: Some confidence in the asserted identity's validity. Level 3: High confidence in the asserted identity's validity. Level 4: Very high confidence in the asserted identity's validity.

Term	Definition
Authentication Service Component (ASC)	A federated architecture that leverages Credentials from multiple domains through certifications, guidelines, standards adoption and policies. The ASC accommodates assertion-based authentication (i.e., authentication of PINs and Passwords) and certificate-based authentication (i.e., public key certificates) within the same environment. Over time, the architecture will leverage multiple emerging schemes such as the SAML and Liberty Alliance, and will not be built around a single scheme or commercial product. In this light, the ASC is more precisely defined as an architectural framework.
Authorization To Operate	Occurs when management authorizes a System based on an assessment of management, operational and technical controls. By authorizing processing in a System the management official accepts the Risk associated with it.
Availability	State of usability and functionality to provide operational effectiveness.
Binding Documents	E-Authentication Federation documents, in addition to the Participation Agreements, Business Rules and Operating Rules, that RPs and CSPs are required to adhere to and comply with.
Boarding Process	Includes all the activities involved in converting a Federation member candidate into an official Federation member. It includes an assessment to verify all applicable agreements and rules have been complied with (or waived), acceptance testing to ensure interface specification compliance, change control board (CCB) approval of member system integration, and CCB recommendation of the member candidate's request for a production E-GCA certificate.
Business Transaction	Business Transaction refers to the functionality of an Agency Application that was the basis of that applications Risk Assessment.
Business Rules	Core E-Authentication Federation principles (i.e., interoperability, auditing, and privacy) that RPs and CSPs must comply with.

Term	Definition
Certification and Accreditation (C&A)	<p>Security Certification and Accreditation are important activities that support a Risk management process and are an integral part of an Agency's information security program.</p> <p>Security accreditation is the official management decision given by a senior Agency official to authorize operation of an information System and to explicitly accept the Risk to Agency operations, Agency assets, or individuals based on the implementation of an agreed-upon set of security controls. Required by OMB Circular A-130, Appendix III, security accreditation provides a form of quality control and challenges managers and technical staffs at all levels to implement the most effective security controls possible in an information System, given mission requirements, technical constraints, operational constraints, and cost/schedule constraints. By accrediting an information System, an Agency official accepts responsibility for the security of the System and is fully accountable for any adverse impacts to the Agency if a breach of security occurs. Thus, responsibility and accountability are core principals that characterize security accreditation.</p>
Chain of Custody	A set of procedure(s)/document(s) to account for the Integrity of an object by tracking its handling and storage from point of instantiation through the current or final disposition of the object.
Compatible	<p>Two Federation Members are considered Compatible if:</p> <ol style="list-style-type: none"> <li data-bbox="589 1100 1400 1142">1. the CS has an equal or higher Assurance Level than the RP, <li data-bbox="589 1163 1400 1248">2. the CS is willing and able to provide all optional attributes required by the RP, <li data-bbox="589 1269 1400 1353">3. and the Federation Members are currently using the same interface specification version.
Confidentiality	System and data Confidentiality refers to the protection of information from unauthorized disclosure. The impact of unauthorized disclosure of confidential information can range from the jeopardizing of national security to the disclosure of Privacy Act data. Unauthorized, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the organization.
Configuration Management (CM)	<p>CM is conducted using the two interrelated functions:</p> <ul style="list-style-type: none"> <li data-bbox="665 1628 992 1670">• Configuration control <li data-bbox="665 1670 1008 1712">• Baseline management <p>Configuration control addresses CM policy and procedures, while baseline management is used to record changes over the life cycle.</p>

Term	Definition
Connected Members	Connected Members are Federation Members that have directly connected their Systems to allow SAML exchanges. Every Member of the Federation is not connected to every other Federation Member, for example CSs are not connected to other CSs, higher Risk AAs are not connected to lower assurance CSs, etc.
Contractor	Person or entity that is under contract to provide the Federal Government with services, supplies, or other needs.
Credential	Digital documents used in authentication that bind an identity or an attribute to a subscriber's Token. Note that this document uses "Credential" broadly, referring to both electronic Credentials and Tokens.
Credential Service (CS)	System that authenticates an End-User who has a PIN or Password based identity Credential. The Credential Service then issues an identity assertion to the relying party. A Credential Service is a Verifier.
Credential Service Provider (CSP)	An organization that offers one or more Approved Credential Services.
Cryptography	The discipline which embodies principles, means and methods for the transformation of data to hide its information content, prevent its undetected modification, prevent its unauthorized use or a combination thereof. [ANSI X9.31] Cryptography deals with the transformation of ordinary text (plaintext) into coded form (ciphertext) by encryption and transformation of ciphertext into plaintext by decryption. [NIST SP 800-2]
Data Integrity	The property that data has not been altered by an unauthorized entity.
E-Authentication Federation (Federation)	An identity federation, whereby Government agencies can rely on Credentials issued and managed by other organizations – within and outside the Federal Government. The Federation is driven by supply and demand. The demand is for online services, which will be fulfilled by leveraging an existing supply of trusted Credentials that are already available and in use by the American public. The Federation includes policy and standards, Business Rules, an architectural framework, Credential Services, Agency Applications, service delivery and acquisition, and a financial model.
E-Governance Certificate Authority (E-GCA)	Established by the Government to issue certificates that allow Agency Applications to retrieve SAML Assertions from Credential Services over a client and server authenticated SSL channel, effectively controlling which entities can participate.

Term	Definition
Electronic Risk and Requirements Assessment, or E-RA (E-RA)	A risk-based approach to authentication requirements. This approach identifies the Risks associated with insufficient authentication of users, and it forms the basis for the definition of authentication requirements.
End-User	Any citizen, Government employee, contractor, or business that authenticates to an AA using a Credential issued by a CS.
Federation Change Management	Policies and processes agreed to by Federation Members to review, approve, and roll out architecture changes to production.
Federation Member	A Relying Party or Credential Service Provider that has successfully completed the preparation phase and the boarding phase. A Federation Member's System (Agency Application or Credential Service) is integrated into the production Authentication Service Component in the third and final phase of joining the Federation – the rollout phase.
Federation Operations Center	Organization within the PMO that operates and maintains the ASC production environment, and manages integration of Member Systems into the production ASC.
Federation Portal (Portal)	A website that helps End-Users locate the CSs and AAs they need to complete their transactions. The Portal also maintains information about CSs and AAs referred to as Metadata, which includes technical interface data as well as descriptive information. When the End-User opts into single sign-on, the Portal assigns a session cookie.
Federation Style Guide	Guidelines pertaining to Federation Member use of E-Authentication logos, branding, and providing E-Authentication instructions and information to End-Users via Federation Member System web pages.
Designated Financial Agent	Selected by a RP or CSP to provide financial related services in regard to the E-Authentication Federation.
Forensics	Process of gathering, processing, and interpreting digital and other evidence to conclusively solve a problem and/or derive a conclusion.
Hosted ASC Components	GSA Preferred hosting of ASC components. Unisys to host ASC components in the same facility, environment, and infrastructure. Each hosted component will be operated with the same direct management control. In addition, Unisys will support all hardware, operating Systems, and basic Network connectivity. Accordingly, Hosted ASC components are considered a single System.
Impact	The magnitude of harm that could be caused by a threat's exercise of a vulnerability.

Term	Definition
Informed Consent	Consent voluntarily signified by an End-User who is competent and who understands the terms of the consent and who has been provided in a clear statement with the appropriate knowledge needed to freely decide without the intervention of any element of force, fraud, deceit, duress, over-reaching or other ulterior form of constraint or coercion. Informed Consent may be signified by any method, including electronically, in a form or otherwise as provided by the party requesting the consent.
Integrity	Integrity refers to the requirement that information be protected from improper modification. Integrity is lost if unauthorized changes are made to the data or IT System by either intentional or accidental acts. If the loss of System or Data Integrity is not corrected, continued use of the contaminated System or corrupted data could result in inaccuracy, fraud, or erroneous decisions. Also, violation of Integrity may be the first step in a successful attack against System Availability or Confidentiality. For all these reasons, loss of Integrity reduces the assurance of an IT System.
Log File	Audit trail of actions and/or exceptions.
Memo of Understanding	Executing an MOU begins the process of joining the E-Authentication Federation, and formally establishes an ongoing working relationship with the Initiative for an Agency. The MOU covers your commitments as an Agency, as well as the Initiative's commitment to your Agency.
Metadata	<p>Information necessary for Nodes (Federation Member Systems) to technically interoperate. Metadata encompasses:</p> <ul style="list-style-type: none"> <li data-bbox="600 1248 1421 1431">• E-Authentication specific information— scheme independent information pertaining to E-Authentication Federation Members (e.g., AA identifiers and CS identifiers) and E-Authentication policies (e.g., Assurance Levels, issuers, client/server certificates) <li data-bbox="600 1438 1421 1579">• Scheme specific information – information that directly supports technical interoperability for this scheme. Some or all of the Metadata for this scheme may not be used for a different E-Authentication scheme. <p>A Node must be configured with both E-Authentication specific Metadata and scheme specific Metadata. Failure to completely and correctly configure Metadata can preclude technical interoperation, or result in unexpected consequences or negative impacts to any number of Nodes. Metadata is not considered secret information.</p>

Term	Definition
National Archives and Records Administration (NARA)	<p>The National Archives and Records Administration Act of 1984 amended the records management statutes to divide records management responsibilities between the National Archives and Records Administration (NARA) and the General Services Administration (GSA). Under the Act, NARA is responsible for adequacy of documentation and records disposition and GSA is responsible for economy and efficiency in records management.</p> <p>Section 3101 of title 44 U.S.C. requires the head of each Federal Agency to make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures and essential transactions of the Agency and designed to furnish the information necessary to protect the legal and financial rights of the Government and of persons directly affected by the Agency's activities.</p>
Network	An open communications medium, typically the Internet, that is used to transport messages between the claimant and other parties. Unless otherwise stated no assumptions are made about the security of the Network; it is assumed to be open and subject to active (e.g., impersonation, man-in-the-middle, session hijacking...) and passive (e.g., eavesdropping) attack at any point between the parties (claimant, verifier, CSP or relying party).
Node	Synonym for “Federation Member System” in context of rolling out the System to or operating the System in the production Authentication Service Component (ASC) federated Network of interconnected Systems (Nodes).
Node Information Form	Form to be filled out by the Agency that documents essential information about the Agency’s Node. Essential information includes Metadata values, assertion engine information, and E-GCA production certificate information.
Operating Rules	Day to day practices and policies Federation Members agree to in order to ensure Federation security, consistency, and service standards.
Operational Readiness Review	Federation Operations Center conducts an operational readiness review to determine whether the Federation member candidate’s system is ready to be integrated into the production ASC. It includes final verification of the readiness of: Security, metadata, servers, node configuration, production scripts, capacity plans, escalation plans, Help desk, contact information, monitoring, training readiness, user support, documentation of testing, participation agreements, and production date coordination.
Participant	An End-User of the Federation.

Term	Definition
Password	A secret that a claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings. See also PIN.
Personal Identification Number (PIN)	A Password consisting only of decimal digits.
Personally Identifiable Information (PII)	Any information that identifies or can be used to identify, contact, or locate the person to whom such information pertains. This includes information that is used in a way that is personally identifiable, including linking it with identifiable information from other sources, or from which other Personally Identifiable Information can easily be derived, including, but not limited to, name, address, phone number, fax number, email address, financial profiles, and social security number, and credit card information.
Privacy Impact Assessment (PIA)	Privacy Impact Assessments are required by the E-Government Act of 2002 whenever “developing or procuring information technology . . . or initiating a new collection of information . . . in an identifiable form . . .” The purpose of a Privacy Impact Assessment is to ensure there is no collection, storage, access, use or dissemination of identifiable personal information (and for some organizations business information) that is not both needed and permitted.
Program Management Office (PMO)	Established by the Government to issue certificates that allow Agency Applications to retrieve SAML Assertions from Credential Services over a client and server authenticated SSL channel, effectively controlling which entities can participate.
Public Key Certificate	A digital document issued and digitally signed by the private key of a Certification Authority that binds the name of a subscriber to a public key. The certificate indicates that the subscriber identified in the certificate has sole control and access to the private key. See also [RFC 3280].
Relying Party	A Federal Agency that relies upon the End-User’s Credentials, typically to process a transaction or grant access to information or a System.
Risk	Risk is a function of the likelihood of a given threat-source’s exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization.
Risk Assessment	Risk Assessment is the first process in the Risk management methodology, used to determine the extent of the potential threat and the Risk associated with an IT System throughout its Software Development Life Cycle (SDLC). The output of this process helps to identify appropriate controls for reducing or eliminating Risk during the Risk mitigation process.

Term	Definition
Rule	A term or condition of participation manifested as an Operating Rule or Business Rule.
Rules of Behavior	Rules that have been established and implemented concerning use of, security in, and acceptable level of Risk for the System. Rules will clearly delineate responsibilities and expected behavior of all individuals with access to the System. Rules should cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of Federal Government equipment, the assignment and limitation of System privileges, and individual accountability.
SAML Artifact	A SAML Artifact of “small” bounded size is carried as part of a URL query string such that, when the artifact is conveyed to the source site, the artifact unambiguously references an assertion. The artifact is conveyed via redirection to the destination site, which then acquires the referenced assertion by some further steps. Typically, this involves the use of a registered SAML protocol binding. This technique is used in the browser/artifact profile of SAML.
SAML Assertion	A statement from a verifier to a relying party that contains identity information about a subscriber. Assertions may also contain verified attributes. Assertions may be digitally signed objects or they may be obtained from a trusted source by a secure protocol.
Section 508	In 1998, Congress amended the Rehabilitation Act to require Federal agencies to make their electronic and information technology accessible to people with disabilities. The purpose of this part is to implement Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d). Section 508 requires that when Federal agencies develop, procure, maintain, or use electronic and information technology, Federal employees with disabilities have access to and use of information and data that is comparable to the access and use by Federal employees who are not individuals with disabilities, unless an undue burden would be imposed on the Agency. Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal Agency, have access to and use of information and data that is comparable to that provided to the public who are not individuals with disabilities, unless an undue burden would be imposed on the Agency.
Security Assertion Markup Language (SAML)	XML-based framework for ensuring that transmitted communications are secure. SAML defines mechanisms to exchange authentication, authorization and nonrepudiation information, allowing single sign-on capabilities for Web services.
Sensitive Information	Information that must be protected due to the risk of loss or harm resulting from disclosure, alteration, or destruction.

Term	Definition
Service Level Agreement	Stipulates and commits a Federation Member to a required level of service. It also specifies, as appropriate, enforcement or penalty provisions for services not provided, a guaranteed level of System performance as relates to downtime or uptime, a specified level of customer support and what software or hardware will be used.
Session Identifier (SID)	Mechanism for indicating to the AA that there is prefill or data transfer available.
Session Reset	A request by an AA to re-authenticate an End-User already authenticated, resulting in a hand-off of the End-User to the CS. This request derives from the AA's Agency session policy.
Signatory	An Approved Party and the GSA who signs and is bound by the terms and conditions of this document.
System	System is a generic term used for brevity to mean either a major application or a general support System.
System of Records Notice	<p>The Privacy Act of 1974 (5 U.S.C. § 552a, the Act) requires agencies to inform the public of the existence of Systems of Records containing personal information, to give individuals access to records about themselves in a System of Records, and to manage those records in a way to ensure fairness to individuals in Agency programs.</p> <p>For the Privacy Act to work effectively, it is imperative that each Agency properly maintain its Systems of Records and ensure that the public is adequately informed about the Systems of Records the Agency maintains and the uses that are being made of the records in those Systems. Therefore, agencies must periodically review their Systems of Records and the published notices that describe them to ensure that they are accurate and complete. OMB Circular A-130, "Management of Federal Information Resources," (61 Fed. Reg. 6428, Feb. 20, 1996) requires agencies to conduct periodic reviews, and this memorandum satisfies that requirement for calendar year FY 1999. Agencies should continue to conduct reviews in accordance with the schedule in Appendix I of the Circular.</p>
The Approved Technology Provider List	A list of software products that have demonstrated basic interoperability in the E-Authentication Interoperability Lab and are approved by the E-Authentication Initiative for use in the Federation.
Token	Something that the claimant (End-User) possesses and controls (typically a key or Password) used to authenticate the claimant's identity.

Term	Definition
Transaction Identifier (TID)	Mechanism for tracking transactions across various components in the architecture. TIDs will be generated by the Portal, and will be passed with the End-User, via query string, as they are redirected from (1) the Portal to CSs, (2) from CSs to AAs, and, (3) once generated by the Portal, to the Portal by AAs or CSs. TID is expected in Architecture 1.1.
Trust List	List of Certification Authorities that an application trusts.

APPENDIX B: ACRONYMS

Acronym	Definition
AA	Agency Application
AAID	Agency Application Identifier
ASC	Authentication Service Component
CAF	Credential Assessment Framework
CMWG	Configuration Management Working Group
CS	Credential Service
CSID	Credential Service Identifier
CSP	Credential Service Provider
DNS	Domain Name System
DOS	Denial of Service
E-GCA	E-Governance Certificate Authority
E-RA	Electronic Risk and Requirements Assessment
ESC	Executive Steering Committee
ET	Eastern Time
FAQ	Frequently Asked Question
FCMP	Federation Change Management Policies
FISMA	Federation Information Security Management Act
FOC	Federal Operations Center
GMT	Greenwich Mean Time
GPS	Global Positioning System
GSA	General Services Administration
ID	Identifier
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
LoD	Letter of Designation
NIST	National Institute of Science and Technology
OMB	Office of Management and Budget
PII	Personally Identifiable Information
PIN	Personal Identification Number
PMO	Program Management Office
POC	Point of Contact
PPOC	Principle Point of Contact
PE	Program Executive
RP	Relying Party

Acronym	Definition
SAML	Security Assertion Markup Language
SID	Session Identifier
S/MIME	Secure/Multipurpose Internet Mail Extension
SPOC	Secondary Points of Contact
SDT	Step Down Translator
TBD	To Be Determined
TID	Transaction Identifier
UID	End-User Identifier
URL	Uniform Resource Locator
XML	Extensible Markup Language

APPENDIX C: MONITORING TEST TYPES

Test Type	Frequency	Components Evaluated	Data Returned
Benchmark Test	12 times per hour	Full HTML/No images	DNS, Connect, Redirect, 1 st Byte, Content, Response Time
Transactional Test	12 times per hour	Full HTML/No images/ per page data	DNS, Connect, Redirect, 1 st Byte, Content, Response Time
Transactional Test	4 times per hour	Full HTML/No images/ per page data	DNS, Connect, Redirect, 1 st Byte, Content, Response Time
Full Page Download	1 time per hour	Full HTML/Images	DNS, Connect, Redirect, 1 st Byte, Content, Response Time

Note: Response Time (RT) equals DNS + Connect + Redirect + 1st Byte + Content

APPENDIX D: PERFORMANCE TESTING

Availability Testing Criteria

This test is designed to verify the reliability and Availability of the service provided by Federation Members. Testing is limited to those services that are part of the Federation. Availability and data quality is considered in this test. Overall response time is not considered during this test, unless the Availability threshold is exceeded. This test will be measured from external locations.

Definition	Default Threshold
Threshold Response Time	60 seconds
Periodic Availability Threshold (based on three external monitoring locations - two out of three must pass tests)	66.00%
Monthly Availability Threshold	99.00%

The Availability Test will be calculated as follows:

- The response time for each test in a five-minute window will be recorded for each test location.
- The response times for each test location within a five-minute window will then be evaluated versus the Threshold Response Time to determine which tests passed or failed. If Test Response Time is less than Threshold Response Time then the test passes, if not, the test fails.
- Based on the pass/fail status of each test location in a given window, a Periodic Pass Percentage will be calculated. (Number of Locations Passed / Total Number of Test Locations = Periodic Pass Percentage)
- The Periodic Pass Percentage will then be compared to the Periodic Availability Threshold to determine if the window is a Pass or a Fail. (If Periodic Pass Percentage is greater than Periodic Availability Threshold then the window passes, if not it fails)
- A Monthly Pass Percentage will be calculated based on the pass/fail status of all the windows in a given month. (Monthly Pass Percentage = Number of Window passes / Number of Windows for the Month)
- The Monthly Pass Percentage will then be compared to the Monthly Availability Threshold to determine if FOC passes or fails the test for the month. (If Monthly Pass Percentage is greater than or equal to the Monthly Availability Threshold then the month passes, if not it fails) If measurements made by CSP and FOC differ on whether a month has passed, CSP and FOC will work jointly to

determine whether the month has passed in accordance with the criteria set forth herein.

Average Response Time

Testing

This test is designed to ensure the service provided by Federation Members is, on average, delivered to the customer in a timely manner. Average response time, Availability and data quality are considered in this test. Tests will be measured over high-speed lines using a monitor that emulates the default behavior of the then-current version of Microsoft Internet Explorer. .

Definition	Default Threshold
Monthly Average Response Time Threshold	5 seconds

The Average Response Time Test will be calculated as follows:

- The total response time for each test in a five-minute window will be recorded for each test location. If there are multiple web pages in the test, the total response time for all pages will be divided by the number of pages in the test to calculate the Average Page Response time for each location.
- The Average Page Response Times for each test location within a five-minute window will then be averaged to calculate the Periodic Average Response Time. This process will be repeated for every given window throughout the month.
- The Periodic Average Response Times will be averaged together to calculate the Monthly Average Time Response Time.
- The Monthly Average Time will then be compared to the Monthly Average Response Time Threshold to determine if the Federation Member passes or fails the test for the month. (If the Monthly Average Response Time is less than or equal to the Monthly Average Response Time Threshold then the month passes, if not it fails)

Minimal Acceptable Response Time

Testing

This test is designed to ensure the service provided by the Federation Member is delivered to the customer in a timely manner. Response time, Availability and data quality are considered in this test. Average response time is not considered during this test. Tests will be measured over high-speed lines using a monitor that emulates the default behavior of the then-current version of Microsoft Internet Explorer.

Definition	Default Threshold
Threshold Response Time	10 seconds
Periodic Minimum Acceptable Response Time Threshold (based on three external monitoring locations - two out of three must pass tests)	66.00%
Monthly Minimum Acceptable Response Time Threshold	99.00%

The Minimum Acceptable Response Time Test will be calculated as follows

- The total response time for each test in a five-minute window will be recorded for each test location. If there are multiple web pages in the test, the total response time will be divided by the number of pages in the test to calculate the Average Page Response time for each location.
- The Average Page Response Times for each test location within a five-minute window will then be evaluated versus the Threshold Response Time to determine which tests passed or failed. (If Average Page Response Time is less than Threshold Response Time then the test passes, if not it fails)
- Based on the pass/fail status of each test location in a given window, a Periodic Pass Percentage will be calculated. (Number of Locations Passed / Total Number of Tests in a Window = Periodic Pass Percentage)
- The Periodic Pass Percentage will then be compared to the Periodic Minimum Acceptable Response Time Threshold to determine if the window is a Pass or a Fail. (If the Periodic Pass Percentage is greater than the Periodic Minimum Acceptable Response Time Threshold, then the window passes, if not it fails)
- A Monthly Pass Percentage will be calculated based on the pass/fail status of all the windows in a given month. (Monthly Pass Percentage = Number of Window passes / Number of Windows in the Month)
- The Monthly Pass Percentage will then be compared to the Monthly Minimum Acceptable Response Time Threshold to determine if the Federation Member passes or fails the test for the month. (If Monthly Pass Percentage is greater than or equal to the Monthly Minimum Acceptable Response Time Threshold then the month passes, if not it fails.)

Measurements

Availability Test

URL or object to be monitored	Test Type	Monitoring Frequency	Threshold Response Time	Periodic Availability Threshold	Monthly Availability Threshold
	Benchmark	12 per hour	60 seconds	66.00%	99.00%
	Transactional	12 per hour			
	Full Page Download	1 per hour			

Average Response Time Test

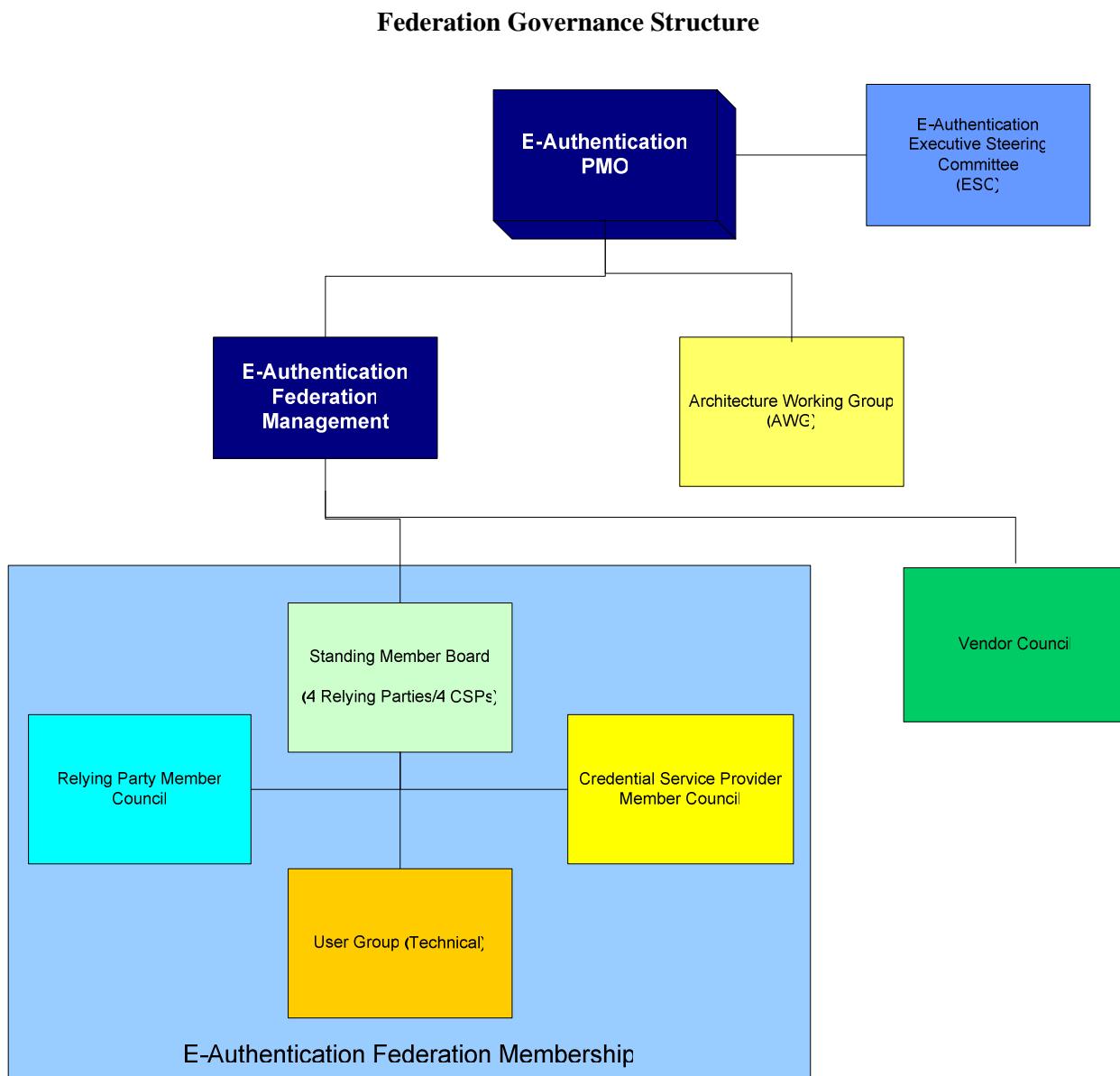
URL or object to be monitored	Test Type	Monitoring Frequency	Monthly Average Response Time Threshold
	Benchmark	12 per hour	5 seconds
	Transactional	12 per hour	
	Full Page Download	1 per hour	

Minimal Acceptable Response Time Test

URL or object to be monitored	Test Type	Monitoring Frequency	Threshold Response Time	Periodic Minimum Acceptable Response Time Threshold	Monthly Minimum Acceptable Response Time Threshold
	Benchmark	12 per hour	10 seconds	66.00%	99.00%
	Transactional	12 per hour			
	Full Page Download	1 per hour			

APPENDIX E: FEDERATION GOVERNANCE

The governance structure for the E-Authentication Federation is shown in the drawing below and is defined in the table that follows. The table indicates the lead or chair for each governing entity, a definition of the entity's membership, the role of the entity, and its decision-making authority, if any.



Federation Governing Entities

Entity	Chair	Membership	Role	Decision-Making
Executive Steering Committee (ESC)	Elected ESC Member	Cabinet-level Agency CIOs or CIO designee	Advisory and oversight responsibility for the E-Authentication Initiative including guidance on strategy and approval of the Initiative's business, spend, and funding plans.	Majority vote
Program Management Office (PMO)	Appointed by GSA	Program Executive, Deputy PM, and staff	Responsible for Federation Management, Operations, Management of Products/Services, and Acquisition Services, plus Project Management functions such as communications, reporting, budget, change management, and architecture. Required to raise issues to the ESC when requested by the SMB.	Program Executive
Federation Management	Deputy PM	Staff	Responsible for day to day Federation management and administration, outreach and recruitment of commercial CSPs and strategic E-Gov applications, relationship management of relying parties and CSPs, maintenance of the Business and Operating Rules and associated Federation documents, formation and management of Federation boards/groups/councils, change management, ensuring ongoing security and privacy of the Federation Network, and Federation membership compliance.	Deputy PM
Standing Member Board (SMB)	Elected by the membership, to rotate between a CSP and an RP	Four CSP representatives and four RP representatives, to include representation from both PKI and SAML relying parties, PKI and SAML CSPs, and gov't and commercial CSPs	Responsible for providing input and recommendations (either solicited or unsolicited) to Federation Management regarding issues that impact Federation membership. This Board will solicit input from the CSP Member Council, the RP Member Council, and the Federation User Group, as appropriate, and then will analyze, assess and compile recommendations to Federation Management.	Provides recommendations to Federation Management and the PMO, and can force the presentation of issues to the ESC.
Credential Service Provider (CSP) Member	Elected by the membership	One designated representative for each CSP Member of the Federation	Responsible for providing input and recommendations (either solicited or unsolicited) to the Standing Member Board regarding issues impacting CSPs including Federation Rules, E-Authentication architecture and	None. Provides input and recommendations to SMB on issues or changes.

Council			technical specifications, current or potential schemes, the Credential Assessment Framework, the Federation membership System and other business and operations policies. Subcommittees may be created as necessary to address specific issues or proposed changes.	May present issues/concerns directly to Federation Management (PMO) when deemed necessary/appropriate by Council membership.
Relying Party (RP) Member Council	Elected by the membership	One designated representative for each (RP) Member of the Federation	Responsible for providing input and recommendations (either solicited or unsolicited) to the Standing Member Board regarding issues impacting RPs including Federation Rules, E-Authentication architecture and technical specifications, current or potential schemes, the Relying Party Assessment Framework, the Federation membership System and other business and operations policies. Subcommittees may be created as necessary to address specific issues or proposed changes.	None. Provides input and recommendations to SMB on issues or changes. May present issues/concerns directly to Federation Management (PMO) when deemed necessary/appropriate by Council membership
Vendor Council	Appointed by the PMO	Representatives of vendors with Approved products within the E-Authentication architecture	Responsible for providing input and recommendations (either solicited or unsolicited) to Federation Management on issues impacting vendors and/or relative to commercial off-the-shelf electronic authentication products.	None. Provides input and recommendations to Federation Management
Federation User Group	Appointed by the Deputy PM	One or more representatives for each Member of the Federation	Responsible for providing input and recommendations (either solicited or unsolicited) to the Standing Member Board on issues impacting Federation Member users. Subcommittees may be created as necessary to address specific issues or proposed changes.	None. Provides input and recommendations to SMB on issues or changes
Architecture Working Group	E-Authentication Chief Architect (appointed by PMO)	Architectural subject matter experts (SMEs) recruited by the PMO	Responsible for making architectural and specification recommendations to the E-Authentication PMO at the request of the PMO or Chief Architect.	None. Provides input and recommendations to PMO relative to architectural issues and changes.

APPENDIX F: FEDERATION CHANGE MANAGEMENT POLICY

The purpose of this Appendix is to outline Federation Change Management Policies (FCMP). The PMO recognizes the need and importance of FCMP as part of the requirement for world-class operations. FCMP are complementary to the configuration or change management processes each Federation Member has established for itself.

FCMP is a framework within an overall Federation Change Management environment. FCMP is established to provide all Federation Members with:

1. Awareness and assurance that the Federation is operating appropriately,
2. Assurance that all changes are controlled, carefully reviewed and Approved, and
3. Assurance that Risks to service, reputation, and ongoing operations are identified, considered, and minimized.

The PMO has determined that the establishment of FCMP is critical. Therefore, the FCMP approach consists of several key steps to ensure consistency in communication, evaluation, and management, as well as to mitigate change-related Risks over time. This Appendix groups these steps into four major areas and addresses them in turn:

1. Change Classification
2. Change Evaluation
3. Approval
4. Compliance/Implementation

Each major area considers and/or is influenced by each change proposal profile. A change proposal profile is described in terms of four dimensions:

1. Category of change
2. Type of change
3. Impact of the change
4. Magnitude of the change

A change proposal profile influences required response times, change evaluation and approval time frames, and implementation and compliance time frames.

Change classification is considered the key initial step. It consists of determining the areas affected and magnitude. These decisions provide Federation Members with an evaluation frame of reference.

Change evaluation is the process by which the Federation's Standing Member Board (see Appendix E for a description of the Governance structure for the Federation), the Vendor Council, the Architecture Working Group (AWG), and other interested parties may assess the change according to the standard dimensions and to contribute feedback. Note that the Federation's Standing Member Board has the authority to leverage the Relying Party Member Council, the Credential Service Provider Member Council, and the Federation User Group (and its primarily technical membership) in order to obtain the appropriate level of analysis and input relative to potential changes. The change evaluation process and timeframes will be tailored appropriately according to the profile of the change in question. Changes bearing the same profile are expected to experience the same evaluation processes and timeframes.

Once a Federation change proposal is Approved, some or all Federation Members are required to implement the change. The timeframe to implement the change and to comply in the production environment is determined by the change proposal profile.

The final section of the document describes the change review process and the dispute resolution procedure.

Change Classification

As described, a key component FCMP is change classification. Change classification results in a change proposal profile, which consists of several dimensions to capture the essence of the change. Once a change has been classified, the appropriate process for the change can be engaged.

The following classification dimensions are described below in further detail:

1. Category
2. Type
3. Impact
4. Magnitude

Change Category

To be evaluated properly, changes must be categorized to provide guidance regarding Federation aspect(s) affected by the change. Understanding the affected aspect(s) allows Federation Members to evaluate the change in its correct context. It also allows Federation Members to better assess potential Impacts to the overall Federation and to individual Federation Members.

The following is a representative list of change categories:

1. Change in Federation membership
2. Update to Member System
3. Technical Specification changes
4. Scheme Introduction/Deprecation
5. Policies
6. Rules
7. Operational Requirements
8. ASC Component Changes

Change Type

The degree of change will vary depending upon the type of change proposed. Describing the range of the anticipated change using consistent terms provides Federation Members necessary information regarding the extent of the change. The following table defines change types:

Table 1: Change Types

Change Types	
Type	Description
<i>Evolutionary</i>	Evolutionary changes do not substantially alter the target of the change (e.g. clarifications).
<i>Revolutionary</i>	Revolutionary changes are anticipated to effect substantial change.
<i>Emergency</i>	Emergency changes are intended to address situations that place Federation Members in immediate jeopardy. These are of critical importance and extreme time sensitivity to Members of the Federation.

Impact

Impact refers to the breadth of the change with regards to the overall Federation, and is essential to evaluating proposed changes. The following table defines three levels of relative impact:

Table 2: Impacts

Impact	
Level	Description
<i>Isolated</i>	Small pockets of the Federation are affected.
<i>Limited</i>	Less than half of Federation Members are affected.
<i>Broad</i>	Most of the Federation is likely to be impacted or affected by the change.

Magnitude

Regardless of type, scope, or category, all changes inherently require some cost. Magnitude is intended to provide a measure of the relative cost to Federation Members to implement a change, including direct costs and indirect costs related to activities or resources. As a single measure determined by the Federation Approved Parties, magnitude is not intended to divulge the precise cost estimates for individual organizations. The following table defines magnitudes:

Table 3: Magnitudes

Magnitude	
Level	Description
<i>Low</i>	Will be defined by Federation membership, consistent with Federation Governance Structure (Appendix E).
<i>Medium</i>	Will be defined by Federation membership, consistent with Federation Governance Structure (Appendix E).
<i>High</i>	Will be defined by Federation membership, consistent with Federation Governance Structure (Appendix E).

Change Policies

Depending upon the change, rollout may consist of implementation or compliance. Rather than pre-define specific timeframes for implementation or compliance, the PMO recognizes that the period will depend heavily on the classification. Rollouts will be conducted by Federation Members and the PMO in accordance with the agreed-upon plan, as documented in the change proposal.

The E-Authentication architecture framework will be able to support multiple versions in order to account for varying life cycle needs, internal project management and prioritization and resource needs of Federation Members. The latest version of the architecture adopted will be downward compatible with prior versions supported. The earliest operating version of the architecture will be assigned a sunset date at which point it will no longer be supported. The sunset date will be 18-24 months after the implementation of the latest version. This will provide Federation Members ample lead time for the removal of a currently-supported version of the architecture. Emergency changes are not subject to the 18-24 month timeframe. However, it is expected that GSA's software development and quality assurance processes will ensure emergency changes introduced into the architecture framework will not adversely impact Federation Members.

Release Rules

The following table defines release rules:

Table 4: Release Rules

Release Rules	
Release	Description
<i>Emergency</i>	Emergency releases are done as needed.
<i>Minor</i>	Will be defined by Federation membership, consistent with Federation Governance Structure (Appendix E).
<i>Major</i>	Will be defined by Federation membership, consistent with Federation Governance Structure (Appendix E).

Change Management Policies

The basic FCMP policies are outlined based upon change type and category.

Table 5: Policies for Change Types

Policies for Change Types	
Evolutionary	
	Evolutionary changes will occur no more than two times annually.
	The Standing Member Board will have at least 30 days to review and respond to proposed evolutionary changes.
	Official approval by appropriate Federation Approved Parties of finalized

	evolutionary changes will be submitted within 5 business days.
Revolutionary	
	Revolutionary changes should be rolled out no more than two times annually.
	The Standing Member Board will have at least 45 days to review and respond to proposed evolutionary changes
	Official approval by appropriate Federation Approved Parties of finalized revolutionary changes will be submitted within 10 business days.
Emergency	
	Emergency changes will be rolled out on an as needed basis to protect the Federation and its Members.
	The Standing Member Board will have at least 48 hours to review and respond to proposed emergency changes.
	Emergency changes will be implemented within 7 days of approval.

Policies for Change Categories

The following table defines policies related to change categories:

Table 6: Policies for Change Categories

Policies for Change Categories	
Change in Federation Membership	
	New Federation Members must use Approved software or obtain a waiver.
	New Federation Members will be connected into the Federation incrementally.
	All new Federation Members must pass acceptance testing with the Interoperability Lab.
	Federation Member interaction must be confirmed by both parties before they are revealed by the Federation Portal.
Update to Member System	
	Updates to Federation Member Systems must be coordinated with the Federation Operations Center.
	Substantial changes to scheme implementation may require new acceptance testing.
	The Interoperability Lab will be made available to Federation Members for testing new releases upon request.
Technical Specification Changes	
	Substantial updates to the architecture will be vetted through the AWG.
	The Standing Member Board will have an opportunity to comment on proposed changes (30 days).
	The Vendor Council will have an opportunity to comment on proposed changes (30 days).
	All changes will include a rollout plan, provided to Federation Members for comments.
Scheme Introduction/Deprecation	

	New schemes will be adopted according to the policies/procedures in the technical approach.
	The rollout plan for scheme introduction or deprecation will follow the scheme adoption lifecycle as outlined in the <i>Technical Approach for the Authentication Service Component</i> .
	Federation Members will have at least 6 months notice before old schemes are abandoned.
Policies	
	The Standing Member Board will have 30 days to comment on proposed changes.
	Federation Members will have the time period to comply as determined during the change review process.
Rules	
	The Standing Member Board will have up to 30 days to review and comment.
	Federation Members have the time period to comply as determined during the change review process.
Operational Requirements	
	The Standing Member Board and the Vendor Council will have up to 30 days to review and comment.
	Federation Members have the time period to comply as determined during the change review process.
ASC Component Changes	
	The FOC will advise Federation Members of planned changes and provide a release plan.
	Changes to ASC components will follow the same guidelines as other Federation changes.
	The FOC will coordinate changes to ASC components with the user group.

Change Review and Implementation Process

Changes may originate from any source, but must be sponsored by either GSA, OMB, or a Federation Member to be considered. Changes are first submitted to the PMO. The PMO will then provide the change to the AWG and/or to Federation Management. For those changes assigned to Federation Management, Federation Management will review the changes, and as appropriate, provide them to the Standing Member Board for analysis and consideration by the CSP Council, the RP Council, and/or the Federation User Group. The Standing Member Board will then assess and compile resulting recommendations regarding the change and provide them to Federation Management, which will in turn provide them to the PMO. Recommendations regarding changes initiated or assessed by the AWG will also be provided to the PMO.

Implementation of the changes will occur according to the timelines indicated as part of the policies defined in Table 6 above.

End Notes

¹ See Appendix A for TID definition.

² See Appendix A for SAML Assertion definition.

³ See Appendix A for Business Transaction definition.

⁴ Additional information is available at <http://www.usdoj.gov/criminal/cybercrime/eprocess.htm>.

⁵ Those that are trusted by the Federation are provided at

<http://www.cio.gov/eauthentication/TCSPList.htm>.

⁶ Test account requirements are defined in the *E-Authentication Interface Specifications*.

⁷ See Appendix A for Connected Members definition.

⁸ Availability and response times are specified in Appendix D.

⁹ Metadata elements are defined in the *E-Authentication Interface Specifications*.

¹⁰ See Appendix A for Compatible definition.

¹¹ This is accomplished through the use of the session identifier (SID) field in the assertion.

Appendix C: Certification Authority Ratings and Trust Guidelines

Attachment 1: Final CARAT Guidelines

Attachment 2: Background Materials on the CARAT Guidelines

Attachment 3: IETF RFC 3627 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

CARAT Guidelines

**Guidelines for Constructing Policies Governing the Use of Identity-Based
Public Key Certificates**

January 14, 2000

**National Automated Clearing House
Association (NACHA)**

The Internet Council

Certification Authority Rating and Trust (CARAT) Task Force

Chairs

Daniel Greenwood

John Sabo

Authors

Alan Asay

C.J. Brandt

Bob Daniels,

Daniel Greenwood

Jane Larimer

Winchel “Todd” Vincent, III

Reporter

Winchel “Todd” Vincent, III

Contributors

Dwight Arthur

Jim Galvin

Ralph Tepper

Joe Vignaly

COPYRIGHT NOTICE

Copyright © 2000 by the National Automated Clearing House Association (NACHA). All rights reserved.

Permission to reproduce this document is hereby granted provided that the following limitations on this right are observed:

(1) all copies must clearly indicate that this work is published by and attributed to NACHA, *and* (2) all copies must include this notice of copyright.

ACKNOWLEDGEMENT

The CARAT Task Force has benefited from collaboration with other organizations that are working on developing standards for the use of public key certificates. In particular, the CARAT Task Force wishes to thank the American Bar Association's Information Security Committee, the ANSI X9F5 Work Group, and CommerceNet for their helpful suggestions throughout the drafting process of the Guidelines.

Note to Readers

NACHA welcomes all comments from interested parties on any aspect of the Guidelines. NACHA is especially interested in learning which portions of the Guidelines you found most useful, how you actually used them, and whether and to what extent you followed the PKIX 4 Framework.

TABLE OF CONTENTS

<u>TABLE OF CONTENTS</u>	<u>5</u>
<u>EXECUTIVE SUMMARY</u>	<u>12</u>
BACKGROUND	12
INTRODUCTION TO THE GUIDELINES	12
SUMMARY OF THE GUIDELINES	12
<u>PART A. INTRODUCTION</u>	<u>16</u>
<u>PART B. ORGANIZATION AND GOVERNANCE: GETTING STARTED</u>	<u>17</u>
B.1 INTRODUCTION TO PUBLIC KEY INFRASTRUCTURE	17
B.1.1 PKI SERVICE PROVIDERS ENABLE TRANSACTIONS AMONG END ENTITIES	17
B.1.2 PKI PARTIES, ROLES, AND FUNCTIONS	18
B.2 THE ROLE OF A POLICY AUTHORITY	19
B.2.1 POLICY AND BUSINESS: THE PARTIES AND THE TRANSACTIONS	19
B.2.1.1 Who are the Stakeholders?	20
B.2.1.2 What Underlying Transactions are to be Facilitated by PKI?	20
B.2.1.3 Certificate Policy Subject to Primary Business Drivers	20
B.2.2 PROMULGATION OF POLICY AS A FUNCTION OF GOVERNANCE	21
B.3 THE STRUCTURE OF GOVERNANCE	21
B.4 FORM OF THE POLICY AUTHORITY	23
B.4.1 EXAMPLE POLICY AUTHORITY CHOICES FROM CURRENT CERTIFICATE POLICY DRAFTS	23
B.4.1.1 U.S. Department of Defense	23
B.4.1.2 Government of Canada	23
B.4.1.3 NACHA	23
B.4.2 SINGLE PARTY POLICY AUTHORITY	24
B.4.3 MULTI-PARTY POLICY AUTHORITY	24
B.4.4 INHERITED GOVERNANCE STRUCTURES	25
B.4.5 CUSTOM GOVERNANCE STRUCTURE	25
<u>PART C. BUILDING A BUSINESS AND LEGAL MODEL</u>	<u>27</u>
C.1 BASIC CONCEPTUAL BUILDING BLOCKS	27

C.1.1 FUNCTIONS ALLOCATED TO ROLES	28
C.1.1.1 Considerations in Allocating Functions to Roles	30
C.1.1.2 Examples of Function-to-Role Allocations	31
C.1.1.2.1 A Four-Cornered Example	31
C.1.1.2.2 A Three-Cornered Example	31
C.1.2 FROM ROLES TO OBLIGATIONS AND PARTIES	32
C.1.2.1 Contracts and Accounts	33
C.1.2.1.1 Contract Formation	33
C.1.2.1.2 System Uniformity and Closure	35
C.1.2.1.3 Ongoing Relationships: Accounts	36
C.1.2.2 Certificates and the Problem of Certificate Meaning	37
C.1.3 FROM OBLIGATIONS TO LIABILITY AND LEGAL REMEDIES	37
C.1.3.1 Choosing a Forum	38
C.1.3.2 Remedies	38
C.1.3.3 Enforcing Remedies and Financial Responsibility	39
C.1.4 CONCLUSION ON MODEL BUILDING BLOCKS	40
C.2 A CLOSER LOOK AT THE FOUR-CORNERED MODEL	40
C.2.1 THREE CORNERS, FOUR, OR MORE?	40
C.2.2 ISSUER FUNCTIONS AND OBLIGATIONS	42
C.2.2.1 Issuer-Subscriber Functions and Obligations	42
C.2.2.2 Issuer-Relying Party Functions and Obligations	45
C.2.2.3 Other Issuer-Related Roles	46
C.2.2.3.1 Registrar	47
C.2.2.3.2 Certificate Manufacturer	49
C.2.2.3.3 Other Roles Assisting Issuers	50
C.2.3 SUBSCRIBER FUNCTIONS AND OBLIGATIONS	51
C.2.3.1 Subscriber-Issuer Functions and Obligations	51
C.2.3.2 Subscriber-Relying Party Functions and Obligations	52
C.2.4 RELYING PARTY FUNCTIONS AND OBLIGATIONS	54
Establishing Relying Party Obligations	54
C.2.4.2 Relying Party-Issuer Functions and Obligations	57
C.2.4.3 Relying Party-Subscriber Functions and Obligations	58
C.2.4.4 Relying Party-Repository Functions and Obligations	58
C.2.5 REPOSITORY FUNCTIONS AND OBLIGATIONS	59
C.2.5.1 Repository-Relying Party Functions and Obligations	59
C.2.5.2 Repository-Subscriber Functions and Obligations	59
C.2.5.2.1 Privacy and Other Information Rights	59
C.2.5.2.2 Account Statements	60
C.2.5.3 Repository-Issuer Functions and Obligations	60
C.2.6 CONCLUSION ON FOUR-CORNERED MODEL	60
PART D. IMPLEMENTING A BUSINESS AND LEGAL MODEL	62

D.1 TAILORING CERTIFICATE POLICY TO REFLECT AND SUPPORT UNDERLYING BUSINESS AND LEGAL CONDITIONS	62
D.1.1 PARTIES AND TRANSACTIONS TOGETHER DEFINE THE UNDERLYING BUSINESS STRUCTURE	63
D.1.1.1 Legal and Regulatory Conditions Related to Certain Parties	63
D.1.1.2 Legal and Regulatory Conditions Related to Certain Transactions	64
D.2 THE ROLE OF THE CERTIFICATE POLICY IN THE CONTEXT OF THE BUSINESS ENVIRONMENT	64
D.2.1 SOURCES OF POWER OR SOURCES OF AUTHORITY UNDERLYING CERTIFICATE POLICY MAKING PROCESS	64
D.2.1.1 Power Based on Position in Private Market	65
D.2.1.2 Authority Based on Provisions in Public Law	65
D.2.1.3 Agreement Based on Consent of the Parties	65
D.2.2 ORDER OF PRECEDENCE OF THE CERTIFICATE POLICY VIS-À-VIS OTHER DOCUMENTS	66
D.2.2.1 Higher Level "Controlling" Documents	66
D.2.2.2 Lower Level "Subordinate" Documents	66
D.2.2.3 Peer Level Documents	67
D.2.3 ANALOGOUS CONTRACTUALLY-BASED GOVERNANCE STRUCTURES	67
D.2.3.1 Several Analogous Structures Exist	67
D.2.3.2 Mini-Study: The VISA Model	68
D.2.4 THE RELATIONSHIP OF PKI MODELS TO THE CERTIFICATE POLICY IMPLEMENTATION	69
D.2.4.1 Underlying Business Conditions and Allocation of PKI Functions to Roles	69
Certification Authority Model	69
Relying Party Model	70
Electronic Court Filing Model	73
D.3 DETERMINING WHETHER AND HOW TO DRAFT A CERTIFICATE POLICY	74
D.3.1 CRITERIA FOR MAKING THE DETERMINATION	75
D.3.1.1 Does the use of a PKI involve certificates?	75
D.3.1.2 Is this a single party system?	75
D.3.1.3 Is the underlying transaction of low-value?	76
D.3.1.4 Is there already a Certificate Policy in play?	76
D.3.2 SCOPE AND DETAIL OF THE CERTIFICATE POLICY	76
D.3.2.1 Public and/or Private Parties in Contract Systems	76
D.3.2.1.1 Reference Model: Business to Government Procurement in a Bounded Contract System	76
D.3.2.1.2 Variations	77
PART E. DRAFTING A CERTIFICATE POLICY	79
E.1 THESE GUIDELINES FOLLOW THE IETF PKIX 4 FRAMEWORK	79
E.2 ORGANIZATION	79
INTRODUCTION	81
1.1 OVERVIEW	81

Drafting Instructions	81
Discussion	81
Cross-Reference	81
1.2 IDENTIFICATION	81
Drafting Instructions	81
Discussion	82
1.3 COMMUNITY AND APPLICABILITY	84
Drafting Instructions	84
Discussion	84
1.4 CONTACT DETAILS	85
Drafting Instructions	85
Discussion	86
2. GENERAL PROVISIONS	86
2.1 OBLIGATIONS	86
Drafting Instructions	86
Cross-Reference	86
2.2 LIABILITY	87
Drafting Instructions	87
Discussion	87
Cross-Reference	87
2.3 FINANCIAL RESPONSIBILITY	87
Drafting Instructions	87
Discussion	87
2.4 INTERPRETATION AND ENFORCEMENT	88
Drafting Instructions	88
2.4.1 GOVERNING LAW	88
Drafting Instructions	88
Discussion	88
2.4.2 SEVERABILITY, SURVIVAL, MERGER, NOTICE	89
Drafting Instructions	89
Discussion	89
2.4.3 DISPUTE RESOLUTION PROCEDURES	91
Drafting Instructions	91
Discussion	91
2.5 FEES	91
Drafting Instructions	91
Discussion	92
2.6 PUBLICATION AND REPOSITORY	92
Drafting Instructions	92
Discussion	92
Cross-Reference	93
2.7 COMPLIANCE AUDIT	93
Drafting Instructions	93

Discussion	93
2.8 CONFIDENTIALITY	94
Drafting Instructions	94
Discussion	94
Cross-Reference	96
2.9 INTELLECTUAL PROPERTY RIGHTS	96
Drafting Instructions	96
Discussion	96
3. IDENTIFICATION AND AUTHENTICATION	97
3.1 INITIAL REGISTRATION	97
Drafting Instructions	97
Discussion	97
3.1.1 TYPES OF NAMES	97
DRAFTING INSTRUCTIONS	97
Discussion	98
3.1.2 NEED FOR NAMES TO BE MEANINGFUL	98
Drafting Instructions	98
Discussion	98
3.1.3 RULES FOR INTERPRETING VARIOUS NAME FORMS	99
Drafting Instructions	99
Discussion	99
3.1.4 UNIQUENESS OF NAMES	99
Drafting Instructions	99
Discussion	99
3.1.7 METHOD TO PROVE POSSESSION OF PRIVATE KEY	100
Drafting Instructions	100
Discussion	100
3.1.8 AUTHENTICATION OF ORGANIZATION IDENTITY	100
Drafting Instructions	100
3.1.9 AUTHENTICATION OF INDIVIDUAL IDENTITY	100
Drafting Instructions	100
Discussion	100
3.2 ROUTINE REKEY [RENEWAL]	102
Drafting Instructions	102
Discussion	102
3.3 REKEY AFTER REVOCATION [RENEWAL AFTER REVOCATION]	102
<u>DRAFTING INSTRUCTIONS</u>	102
Discussion	102
3.4 REVOCATION REQUEST	102
Drafting Instructions	102

Discussion	103
------------	-----

<u>4. OPERATIONAL REQUIREMENTS</u>	104
---	------------

4.1 CERTIFICATE APPLICATION	104
Drafting Instructions	104
Discussion	104
Cross-Reference	104
4.2 CERTIFICATE ISSUANCE	104
Drafting Instructions	104
Discussion	105
Cross-Reference	105
4.3 CERTIFICATE ACCEPTANCE	105
Drafting Instructions	105
Discussion	105
4.4 <u>CERTIFICATE REVOCATION</u>	106
4.4.1 CIRCUMSTANCES FOR REVOCATION	106
Drafting Instructions	106
Discussion	106
Cross-Reference	107
4.4.2 WHO CAN REQUEST REVOCATION	107
Drafting Instructions	107
Discussion	107
Cross-Reference	107
4.4.3 PROCEDURE FOR REVOCATION REQUEST	108
Drafting Instructions	108
Discussion	108
4.4.4 REVOCATION REQUEST GRACE PERIOD	108
Drafting Instructions	108
Discussion	109
Cross-Reference	109
4.4.5 CIRCUMSTANCES FOR SUSPENSION	109
Drafting Instructions	109
Discussion	109
4.4.6 WHO CAN REQUEST SUSPENSION	109
4.4.7 PROCEDURE FOR SUSPENSION REQUEST	109
4.4.8 LIMITS ON SUSPENSION PERIOD	110
4.4.9 CRL ISSUANCE FREQUENCY (IF APPLICABLE)	110
Drafting Instructions	110
Discussion	110
Cross-Reference	110
4.4.10 CRL CHECKING REQUIREMENTS	111

Drafting Instructions	111
Discussion	111
4.4.11 ON-LINE REVOCATION/STATUS CHECKING AVAILABILITY	111
Drafting Instructions	111
Discussion	111
Cross-Reference	112
4.4.12 ON-LINE REVOCATION CHECKING REQUIREMENTS	112
Drafting Instructions	112
Discussion	112
Cross-Reference	112
4.4.13 OTHER FORMS OF REVOCATION ADVERTISEMENTS AVAILABLE	112
4.4.14 CHECKING REQUIREMENTS FOR OTHER FORMS OF REVOCATION ADVERTISEMENTS	112
4.4.15 SPECIAL REQUIREMENTS RE KEY COMPROMISE	112
4.5 SECURITY AUDIT PROCEDURES	113
Drafting Instructions	113
Discussion	113
4.6 RECORDS ARCHIVAL	115
Drafting Instructions	115
Discussion	115
4.7 KEY CHANGEOVER	116
Drafting Instructions	116
Discussion	116
4.8 COMPROMISE AND DISASTER RECOVERY	116
Drafting Instructions	116
Discussion	116
Cross-Reference	117
4.9 CA TERMINATION	117
Drafting Instructions	117
8. SPECIFICATION ADMINISTRATION	118
Drafting Instructions	118
Discussion	118
Cross-Reference	118
APPENDIX	119
IETF PKIX FRAMEWORK	119

EXECUTIVE SUMMARY

Background

State governments have actively pursued methods for creating non-legislative standards for the use of digital signatures verifiable through public key certificates. In May 1997, the National Association of State Information Resource Executives (NASIRE), the National Association of State Purchasing Officers (NASPO), the National Association of State Auditors, Comptrollers and Treasurers (NASACT), and several states, sought to create a forum to explore this issue in collaboration with private sector participants. Following a competitive solicitation of proposals, the National Automated Clearing House Association (NACHA) was selected to facilitate this effort. These Guidelines are a product of that effort.

Introduction to the Guidelines

These Guidelines are intended to help organizations create closed, but interoperable public key infrastructures (PKIs) that can be used to facilitate pilot projects employing public key technology. Such organizations, called *Policy Authorities* in this document, can use the Guidelines to analyze their particular needs and to construct a PKI that will meet those needs. One important product of that analysis is likely to be a *Certificate Policy*, which may be thought of as a charter for a particular PKI. A Certificate Policy defines who the parties are, the relationships and obligations of the parties to one another, and what uses are acceptable within the PKI. The last part of these Guidelines includes high-level drafting instructions for Certificate Policy writers. The Guidelines suggest that Policy Authorities use contracts to make the provisions of a Certificate Policy legally binding among the parties.

The Guidelines are a publication of NACHA and were developed under the auspices of The Internet Council, a NACHA-sponsored council. The Guidelines were drafted by the Certification Authority Rating and Trust (CARAT) Task Force of The Internet Council's Authentication and Network of Trust Work Group. The Guidelines are still in draft form and should not be regarded as a finished document. For this work to advance, interested parties are encouraged to provide comments to NACHA regarding the usefulness of this document. NACHA also encourages interested parties to use these Guidelines to draft Certificate Policies that pertain to their particular pilot's needs and to provide comment to NACHA. It is envisioned that a summary of the cumulative experience of interested parties will lead to a revised and improved version of these draft Guidelines.

Summary of the Guidelines

Part A, "Introduction" explains the history of this document.

Part B, "Organization and Governance – Getting Started," explains the concept of a *Policy Authority* and its role in imparting structure, form and organization to a PKI. The Policy Authority is distinguished from other stakeholders, who may be *End Entities* or *PKI Service Providers*. End Entities include the

parties to the underlying transactions – for example, buyers and sellers in a procurement setting. PKI Service Providers include parties that perform enabling functions to support the underlying transactions. Even though a PKI is created to enable certain transactions it should not be confused with the substance of the business being conducted by the End Entities.

Because public key technology is an enabling technology, any attempt to use it must start with an analysis of business drivers -- *i.e.*, the transactions that bring stakeholders together. This analysis should take into account the general business and legal environment surrounding the transactions. A deliberate look at the parties' needs is a critical first step in determining whether and how a PKI can help. The next step is to learn more about the functions that public key technology can perform and consider how they may be applied to the parties' needs.

In Part C, "Building a Business and Legal Model," the Guidelines describe a suite of *functions* derived from public key technology that might be performed in a PKI. The list, which is not exhaustive, includes: key generation and safekeeping; information acquisition and confirmation; certificate creation; certificate signing; certificate distribution; certificate revocation; claim and dispute resolution; and risk management. These functions can be thought of as building blocks with which to construct a PKI. Once the relevant functions are identified, they must be associated with roles. The Guidelines refer to this process as *allocating functions to roles*.

A number of possible *roles* are identified and named. They include PKI Service Provider roles such as *Issuer*, *Certificate Manufacturer*, *Registrar* and *Repository* and End Entity roles such as *Subscribers* and *Relying Parties*. Not all roles will be appropriate in every business model, and there may be other roles not identified here that a Policy Authority might wish to specify. In addition, one party could assume several roles within a given PKI, depending on the business and legal model employed. Nevertheless, all parties within a PKI must agree to perform certain roles, and the agreements should be embodied in legally enforceable contracts.

Various models for structuring the parties' relationships have been constructed over time. The Guidelines use a "four-cornered" model (Subscriber, Issuer, Repository and Relying Party) as a starting point from which to consider how the functions and obligations of the parties might be allocated in a closed but scalable and interoperable PKI. The CARAT Task Force is not recommending the four-cornered model as a preferred model, but presents it for illustrative purposes.

The four-cornered model is then analyzed in some detail by looking at the functions and obligations of each party to the other parties. For example, the functions assigned to the Issuer (*e.g.*, issue certificates, state information accurately, revoke certificates on request, publish certificates, confirm accuracy of information in the certificates; etc.) are analyzed in the context of the Issuer's obligations to the Subscribers, Repository, and Relying Party. A similar analysis is performed for each of the other three roles occupying the four corners of the model. In addition, other roles such as Certificate Manufacturer and Registrar are discussed. This section also introduces certain concepts, such as "implementing contracts," that are explored more fully in the next section.

In Part D, "Implementing a Business and Legal Model," the Guidelines address PKI governance issues, and includes a discussion of the documents that may be used to organize and implement a particular

PKI. This section discusses some of the factors that may affect whether or not a Certificate Policy is needed. It reiterates and elaborates on the need to bind parties to their respective roles through implementing contracts.

This section of the Guidelines reminds Policy Authorities that there are additional considerations that a Certificate Policy must include other than the underlying transactions and the available suite of PKI functions. These considerations include non-contractual governance structures, such as existing legal and regulatory conditions that may apply to certain transactions. Different business and legal models, such as the three-party, "Certificate Authority" model (Subscriber, Certificate Authority and Relying Party) envisioned by the American Bar Association's Digital Signature Guidelines, are briefly introduced. Readers are reminded that the Guidelines were written with certain assumptions, including reference to a general business environment in which public sector buyers engage in online interactions with private sector sellers. It is necessary for Policy Authorities to draft Certificate Policies that are tailored to their particular needs and business requirements and to view these Guidelines as informational, but not prescriptive.

The final part of the Guidelines, Part E, "Drafting a Certificate Policy," is intended to provide practical suggestions to Policy Authorities as they begin the task of drafting their own Certificate Policies. Unlike the previous parts of the Guidelines, Part E follows the organization of the Internet Engineering Task Force (IETF) PKIX 4 Framework. The Guidelines include Parts 1, 2, 3, 4, and 8 of the Framework. The Guidelines do not incorporate Parts 5, 6 and 7 because the technical nature of the latter sections is not appropriate for guidelines of this type. Except where noted, the document mirrors the numbering used in the PKIX Framework.

In each such section, the reader will find "Drafting Instructions" followed by a "Discussion." The Drafting Instructions include high-level suggestions regarding what ought to be included in a Certificate Policy. They use the terms "should" and "may" in recognition of the fact that these are guidelines and should not be regarded as prescriptive.

In Part 1 ("Introduction") of "Drafting a Certificate Policy," the Guidelines provide assistance to drafters in describing the scope and purpose of a Certificate Policy. Of central importance here is the description of community and applicability; *i.e.*, the parties to whom the Certificate Policy will apply and the uses that will be permitted within the PKI.

In Part 2 ("General Provisions"), drafters are instructed to address the obligations of the various parties to one another. The content of the provisions in this section will differ from one Certificate Policy to another, depending on the business and legal model constructed by the Policy Authority. This part also addresses matters related to enforcement of the parties' obligations, and to issues such as the fees that may be charged by PKI Service Providers, publication requirements, compliance audit requirements, and so forth.

Part 3 ("Identification and Authentication") addresses the central issue of confirmation of individual identity. This part of the Guidelines includes instructions regarding initial registration, the types of names that may be included in public key certificates, requests to renew expired or revoked certificates, and certain revocation requests.

Part 4 ("Operational Requirements") includes high-level instructions regarding certain operations that are likely to occur in a PKI. Some of the more critical operations addressed here include the issuance of certificates by Issuers and their acceptance by Subscribers, and certificate revocation. This part also includes guidelines for Relying Parties concerning the need to check a certificate's current validity.

Finally, Part 8 ("Specification Administration") provides instructions on the manner in which a Policy Authority may change its Certificate Policy and on how it should notify affected parties of those changes.

PART A. INTRODUCTION

The bright promise of electronic commerce is shaded by concerns about security. The very openness of the Internet that has led to its explosive growth has also given rise to an awareness of its security limitations. Government entities and private businesses that are obvious candidates for participating in electronic commerce are understandably cautious. They need assurance that the electronic messages they receive are authentic, have not been altered, and can be relied upon.

Technical means of establishing message authenticity and integrity have existed for some time. Public key technology, which has long been known in technical circles, seems to hold extraordinary promise, but its practical implementation is only beginning. Impeding implementation is the lack of policy that defines the business and legal expectations and the requirements of the parties.

Many states have sought to provide a measure of predictability in this arena by enacting laws regarding digital or electronic signatures. A few of these laws go so far as to construct major elements of a PKI within their jurisdictions. State laws are far from uniform, however, and it is unclear whether this lack of uniformity is itself an impediment to the further growth of electronic commerce. Nonetheless, in response to a perceived need for a more integrated approach, several national associations of state officials embarked on a collaborative effort to address their shared security concerns. In May 1997, the National Association of State Information Resource Executives (NASIRE), the National Association of State Purchasing Officers (NASPO), the National Association of State Auditors, Comptrollers and Treasurers (NASACT), and several states, sought to create a forum to explore this issue in collaboration with private sector participants. Following a competitive solicitation of proposals, the National Automated Clearing House Association (NACHA) was selected to facilitate this effort. These Guidelines are a product of that effort. They were drafted by the Certification Authority Rating and Trust (CARAT) Task Force of The Internet Council's Authentication and Network of Trust Work Group.

PART B. ORGANIZATION AND GOVERNANCE: GETTING STARTED

This part of the Guidelines introduces the concepts of a certificate-based Public Key Infrastructure, a Certificate Policy, and the Policy Authority that promulgates a Certificate Policy. Generally, a Certificate Policy is used to define the interrelated rights and obligations of stakeholders utilizing public key certificates to enable electronic commerce transactions. Although some implementations of public key cryptography can be used to directly signify the role or authority an individual possesses, these Guidelines deal only with public key certificates used to authenticate the identity of an individual. In addition, the Guidelines are intended for use within a business environment that is capable of technical interoperability, but that is legally bounded to include only certain parties and transactions. These Guidelines do not purport to support an open, global electronic commerce structure for "stranger to stranger" spontaneous transactions. Instead, these Guidelines are tailored for use within business and legal environments in which parties have a contractually based and legally bounded relationship.

B.1 Introduction to Public Key Infrastructure

B.1.1 PKI Service Providers Enable Transactions Among End Entities

A Public Key Infrastructure (PKI), literally, is a complex infrastructure of hardware, software, databases, networks, security procedures, and legal obligations. Public key technology is one of a number of "enabling technologies" that supports and implements actual transactions. PKI allows individuals and entities to identify each other as they transact business over computer networks such as the Internet. For example, in an electronic procurement system that allows government agencies to procure goods from private companies, the actual transaction is "procurement;" PKI is the enabling technology that allows electronic procurement to take place.

Building a PKI is not a trivial task. It requires the successful execution of a suite of PKI *functions*. "PKI Service Providers" are the *parties* -- the legal persons or entities -- that perform PKI functions. In some PKIs, one party will perform all PKI functions. In other PKIs, multiple parties will perform sets of functions. These Guidelines refer to "PKI Service Providers" as the *parties* that perform a full suite of PKI *functions*.

PKI Service Providers perform PKI functions for the benefit of *End Entities*. The parties that perform "End Entity" roles are the parties that engage in actual transactions.¹ If PKI Service Providers did not provide a PKI, End Entities would still transact business. However, they would simply use some other

¹ There are two types of End Entities: a Subscriber and a Relying Party. Subscribers are sometimes called Subjects. Subscribers are originators and signers of messages. Relying Parties are recipients of signed messages. In most applications, Subscribers will be Relying Parties and Relying Parties will be Subscribers as communication is almost always bi-directional. For example, if a Subscriber-Offeree originates and signs an offer which requires acceptance, the Relying Party-Offeree must also be a subscriber if it is to originate and sign an acceptance.

identification or security technology, such as biometrics or pen and ink, to conduct business. Stated another way, End Entities will always exist to conduct business, but PKI Service Providers will exist only as long as End Entities or their governing bodies deem PKI to be the best technology to facilitate transactions.

B.1.2 PKI Parties, Roles, and Functions

Early thinkers conceived of a *Certification Authority* as the single party responsible for performing all PKI functions. In the ABA's Digital Signature Guidelines, the ABA drafters refer to a Certification Authority as the one party responsible for performing a full suite of PKI functions. They recognized, however, that a Certification Authority might delegate a certain set of functions to a *Registration Authority*. In fact, there are other sets of functions that can be logically and conveniently grouped and delegated. In business models, such sets of functions are often outsourced or have some other heightened significance.

It is useful to continue the evolution of naming sets of functions. Indeed, PKI functions can be divided into several sets, where each set can represent a *role*. Roles can be named according to the nature of the functions in each set. By naming roles and associating functions with roles, these Guidelines do not suggest that functions will be divided in the same manner in every business model. Nor is it suggested that there will be one-to-one correlation between roles and parties. Indeed, it is envisioned that a *party* may perform one or more roles in a PKI. Evolving business models may change the way in which functions are logically grouped. It may, therefore, be necessary in the future to further evolve the naming of roles.²

The roles identified in these Guidelines follow:³

- PKI Service Providers
 - Policy Authority (to be described more fully below)
 - Issuer⁴

² It is important to understand that all business models are unique. In any given business model, the division of functions among parties will be different. Hence, the roles described in this document may be inadequate in describing some business models. That is, simply because the Task Force states that a party performing Role 1 will perform Functions 1, 2, 3, 4, and 5 does not mean that in all business models a PKI Service Provider responsible for Role 1 will perform Functions 1-5. It could happen that Function 5 is performed by a PKI Service Provider that is responsible for Role 2. Roles are named simply because a granular vocabulary makes the task of describing rights and responsibilities of parties easier. (It is difficult, for instance, to refer only to a Certification Authority and a Registration Authority when describing functions generally recognized as being performed by a Repository.) Accordingly, drafters are cautioned to develop and examine carefully how functions are actually mapped to roles and PKI Service Providers under a particular Certificate Policy.

³ There are additional roles that could be named. At this time, the Task Force does not find it useful to define additional roles.

⁴ Throughout these Guidelines, the Task Force assumes that a Certificate Manufacturer and a Registrar are closely related to an Issuer. That is, it is assumed that the functions performed by the Certificate Manufacturer and the Registrar are functions that are very often the responsibility of the Issuer. Indeed, in the four-cornered model used throughout this document, the Certificate

- Certificate Manufacturer
- Registrar (Registration Authority)
- Repository
- End Entities
 - Subscriber
 - Relying Party

An example of how functions are assigned to roles is more fully described in Part C.

B.2 The Role of a Policy Authority

These Guidelines refer to the authoritative party (or body) that formulates and adopts the Certificate Policy as the *Policy Authority*. The Policy Authority has the final authority and responsibility for specifying a Certificate Policy. Setting a Certificate Policy is a function of organizational governance. Governance is the manner in which an organization structures the roles, rights, and responsibilities of people who participate within a given system. The governing body, according to Black's Law Dictionary, means that body "which has ultimate power to determine its policies and control its activities."⁵ Thus, the governance of an organization must be viewed as broader than the mere promulgation of a Certificate Policy, although setting certificate policy is included in, and tightly related to, the overall duties of governance. The Policy Authority is charged with these broader governance functions.

B.2.1 Policy and Business: The Parties and The Transactions

The Policy Authority is responsible for ensuring that the activities of PKI Service Providers and End Entities are conducted in a sound and efficient manner. An issue for the Policy Authority to consider prior to drafting a Certificate Policy is the scope and depth of the underlying business context that has given rise to the need to use either secure or authenticated electronic communications or both. A Certificate Policy must fit the basic business needs of the parties, which will differ depending on the nature of the participants involved and the business transactions they seek to conduct. Before drafting a Certificate Policy, a Policy Authority will have to first make fundamental business and legal policy determinations. The following are questions the Policy Authority should ask.

Manufacturer and Registrar are generally considered sub-roles of an Issuer. As a result, where the term Issuer is used, drafters should realize that in some cases either Certificate Manufacturer or Registrar could be substituted.

⁵ BLACK'S LAW DICTIONARY, 6TH EDITION, 1990.

B.2.1.1 Who are the Stakeholders?

In addition to the Policy Authority, the stakeholders are End Entities and PKI Service Providers, if PKI is used to enable transactions among End Entities. Stakeholders could be drawn from any number of groups, such as citizens, consumers, business organizations, government entities, academic institutions, employees, politicians, or any number of other groups. Depending on the stakeholders, very different roles and functions within a PKI system may be appropriate and feasible.

B.2.1.2 What Underlying Transactions are to be Facilitated by PKI?

The transactions facilitated by use of PKI may include medical records or third party payor requests in the healthcare environment, stock trades, baseball card trades, or the trading of promises to work for a new employer. The same parties who engage in different transactions may require different policies for each transaction due to the variations in the underlying legal and economic systems related to each transaction. For the sake of efficiency, it would be convenient for the same parties to use the same certificates under the same Certificate Policy as part of every transaction that they conduct with each other. The regulatory requirements governing payment systems, however, are so different from the regulatory requirements governing submission of a bid for a public works project that the obligations and rights of the parties may well require different certificate policies. At some point in the distant future, a broader system may emerge that consolidates several secure communications policies together. For the foreseeable future, however, policies that define the rights, duties, and functions of parties are expected to be related to the underlying transactions and businesses involved.

B.2.1.3 Certificate Policy Subject to Primary Business Drivers

The Certificate Policy must be drafted to support and reflect the underlying business structure. The business mission of the stakeholders and the business drivers that give rise to the specific transactions should be of paramount importance to the Policy Authority. A Policy Authority that puts implementing PKI, or any enabling technology, ahead of the fundamental business mission of the organization may be neglecting its governance duties. When a Policy Authority is the same as an overall governing body for an organization, there will be fiduciary duties owed by each individual member to execute the mission of the organization above other goals. The form of an electronic commerce transaction will be a means to an end. In other words, choice of a PKI model and drafting the related Certificate Policy must be subject to the business needs of the organizations that are served by this enabling technology. Though several models for the use of PKI have been put forward by theorists, these Guidelines suggest that business people seeking to implement a PKI system do so in a manner consistent with their business rather than following a pre-conceived model of PKI. A detailed examination of several business conditions that may affect the Certificate Policy drafting process is presented in Part D, "Implementing a Business and Legal Model."

B.2.2 Promulgation of Policy as a Function of Governance

The Policy Authority, as the party charged with governance, is responsible for drafting the Certificate Policy. The Certificate Policy, itself, will contain sections bearing on governance, including the party responsible for the Policy and the manner in which the Policy may be amended.⁶

A Certificate Policy, not unlike any other important policy or business decision, will be set in the context of a complex and interrelated set of conditions affecting the rights, obligations and mission of an organization. At its core, a Certificate Policy describes how a Policy Authority governs the parties, scope of business, functional operations, and the obligations of PKI Service Providers and End Entities who engage in electronic transactions. Such matters are not driven by PKI implementations but are based upon the duty of a governing body to carry out the mission of its organization in a sound and prudent manner.

The assumption of these Guidelines is that organizations have business, government, or public interest missions and it is not the mission of an organization to use and promote PKI. Rather, the use of PKI will be for the purpose of securing and authenticating communications and data interchange that is of relatively high value, sensitive, or otherwise important to the mission of the organization. Thus the governance decisions regarding the content of a Certificate Policy will be subordinate to the interests of the underlying communications and transactions, especially with respect to the obligations between “users” or “End Entities.”

B.3 The Structure of Governance

The Policy Authority has ultimate responsibility for specifying the Certificate Policy. The Policy Authority can be described as the governing body, or the designee thereof, which is tasked with promulgating the Certificate Policy in a manner that supports and reflects the needs of the underlying relationships and transactions.⁷ Authoritative policy is promulgated by a policy-making entity. This entity derives its authority from the governance structure of the organization on whose behalf it sets policy. A governing body may delegate some authority to executive decision makers, but it does not typically delegate matters that are fundamental to the mission and existence of an organization.

It is customary for governing bodies to subdivide aspects of governance to such lesser groupings as Committees, Councils and Boards. It is often necessary that such lesser grouping be entirely or partially comprised of full members of the governing body. In a given organization, a governing body may

⁶ For example, Part E of these Guidelines, “Drafting a Certificate Policy,” incorporates provisions for the listing of “the name and mailing address of the authority that is responsible for the registration, maintenance, and interpretation of this certificate policy” (see Section 1.4) and for the listing of a “specification administration” organization that lists responsibility for procedures necessary to amend the policy, publications or notices and certain approval procedures for relevant documents (see Section 8).

⁷ Examples of governing bodies abound. For instance, in a corporation, the governing body is said to be the Board of Directors. Academic institutions often have a Board of Trustees as a governing body. Governmental entities at the state and federal levels are said to gain their power from the consent of the governed as expressed in the Constitution and implemented or interpreted by the Executive, Legislative, and Judicial branches, which comprise the governing bodies.

choose to have a Certificate Policy promulgated by an Information Technology Committee or an Electronic Commerce Board. A small organization may require a Certificate Policy to be set and approved by the full governing body. A larger organization may only require such policy to be approved by the governing body. Alternatively, a governing body may delegate authority to make such policy to an executive officer. In all cases, a governing body or its delegate makes this type of policy. .

For purposes of simplicity, these Guidelines assume that the exercise of governing authority necessary to promulgate a Certificate Policy is, in fact, performed by a governing body of some sort. In other words, the Policy Authority empowered to draft or select a Certificate Policy would be a governing body, at least with respect to the subject matter contained within that Certificate Policy.

In some situations, different parties may try to organize a new representative organization with an independent scope of authority and governance structure to make the business, legal, and technical decisions related to promulgating a Certificate Policy. In particular, organizations that are engaged in electronic commerce as a fundamental aspect of their mission may find that their Certificate Policy is of sufficient importance to warrant the formation of a consortium, or other legal body, to specify and maintain the policy. Electronic commerce implementations may require a 'web' of relationships that spans traditional organizational boundaries and jurisdictions. This, in turn, may require multi-party cooperation, new business partners, leveraging and consolidation of existing infrastructures, and, in some cases, evolved organizational structures. (See, for example, the section below on "Custom Governance Structure"). Generally, however, these Guidelines assume that parties will seek to use PKI to facilitate business within an existing governance structure so that the structure will not be materially changed in the short term as a result of using PKI.

Although a governing body is responsible for promulgating a Certificate Policy, some elements specified in such a policy should be resolved in the server room rather than the Board room. For example, Section 7.1.8 of the PKIX Framework, detailing the "policy qualifiers and syntax semantics" may be an important matter, but probably is not one requiring direct policy determinations at the governance level of an organization. Technical staff will probably specify highly technical issues.

Matters like determining the scope of community and applicability; obligations and liability of the parties; fees and financial responsibility; and the confirmation and identification of certificate applicants are fundamental policy issues that require decisions by those with responsibility to steer the organization. There is no clear delineation between important and trivial usage of PKI.⁸ The Guidelines assume that the value and relevance of the Certificate Policy is such that formal policy making channels are necessary and appropriate.

⁸ Those with responsibility must consider whether the Certificate Policy materially affects high-value, sensitive, or mission critical relationships and transactions. Alternatively, a risk, benefit and cost analysis can be performed to determine whether the systems governed by the Certificate Policy are of sufficient relevance and value to warrant formal, high-level oversight and approval. If so, then the role of Policy Authority should be performed by one or more members of the governing body or its delegate.

B.4 Form of the Policy Authority

The form of the Policy Authority as a governing body will be of critical importance to any given business system operating under a named Certificate Policy. The form of the Policy Authority, including whether it is constituted as a representative association of multiple-parties or as single party, also has significant, practical ramifications. In forming the Policy Authority, organizers should first consider the legal form of all parties that will constitute the Policy Authority.

B.4.1 Example Policy Authority Choices from Current Certificate Policy Drafts

The following examples illustrate how various organizations that have published draft Certificate Policies have approached the sections detailing the “Specification Administration Organization” listed in section 1.4 of the PKIX Framework.⁹

B.4.1.1 U.S. Department of Defense

"A Policy Management Authority (PMA) [whose membership is to be determined] to be determined [*sic*], is responsible for definition, revision and promulgation of this policy. Until the authority is established, the National Security Agency is responsible for definition, revision and promulgation of this policy. The organization to be contacted is . . . "

B.4.1.2 Government of Canada

Digital Signature and Confidentiality, Certificate Policies for the Government of Canada Public Key Infrastructure, V2.0. August 1998:

"This certificate policy is administered by the Government of Canada PKI Policy Management Authority, Treasury Board Secretariate, Ottawa, Ontario, Canada. The contact person is . . . "

[NOTE: this certificate policy includes a definition of Policy Management Authority that provides as follows: "A GoC body responsible for setting, implementing, and administering policy decisions regarding CPs and CPSs throughout the GoC PKI."]

B.4.1.3 NACHA

National Automated Clearing House Association, The Internet Council, Authentication and Network of Trust Pilot Program, Certificate Policy:

⁹ As shown in these examples, some policy drafters have opted to call this party a “Policy Management Authority.” These Guidelines use the shorter term “Policy Authority” for the sake of brevity and also because it is felt that management of a policy can be considered as a lesser included function of setting policy. Policy implementation and other management issues can be delegated or sub-contracted to a project management or other organization. The ultimate authority and responsibility for making fundamental policy, however, may be considered a non-delegable fiduciary duty of the Policy Authority as a governing body of an organization.

“This Policy is administered by the National Automated Clearing House Association.”

B.4.2 Single Party Policy Authority

The single party natural person is the simplest possible entity. This would be the case of a sole proprietor as Policy Authority. It is far more likely, however, that the party assuming the role of a Policy Authority will be a more complex legal entity. Any legal person may perform the role of a Policy Authority. Legal persons may include corporations, partnerships, trusts, unincorporated non-profit associations, government bodies, and other organizations. Although more than one natural person may play an active part on behalf of such an organization, legally they would still be considered a single party. Of the several characteristics that are associated with the term "legal entity" two that are critical for eligibility to conduct the business of a Policy Authority are (1) the capacity to form binding contracts and (2) the ability to sue and be sued.

B.4.3 Multi-Party Policy Authority

More complex than a single organization serving as a Policy Authority is the case of multiple organizations joining together to fulfill the functions of this role. Multi-party governance can be relatively informal, occurring through informal mechanisms, such as a memorandum of understanding or, slightly more formally, a memorandum of agreement. For example, the current practice for organizing multi-state procurement often involves only a short memorandum of understanding. (Of course, the underlying bid process, project awards and contracts are considerably more formal in nature.) There is no need, however, for more formal documentation of the intent to collaborate on multi-state procurements given the relationship of the parties as co-equal, large and sophisticated organizations with interdependent histories. Given the voluntary nature of such collaboration, oppressive or rigid governance mechanisms are usually unwise and unwelcome.

When separate organizations choose to approach policy specification of a PKI jointly, they would be advised to structure joint governance mechanisms. Such governance mechanisms as approval by a certain number of parties or the granting of limited veto rights could be afforded. The question arises: what would prevent any party from violating an understanding related to performing Policy Authority functions (e.g., by attempting to substitute different terms of a Certificate Policy from those that have been agreed upon or by agreeing to cross-certify a different PKI without abiding by some specified process)? To reach higher levels of assurance, it may be advisable to enter into formal contracts. Based upon contract law, one could compel conduct in compliance with the agreement or possibly prevent conduct in breach of the agreement, or potentially gain compensation for breach. In some cases, it may be advisable for disparate individual parties to form a new single legal entity for the purpose of jointly carrying out the functions of the PA. (See Section 4.5, Custom Governance Structure, below).

B.4.4 Inherited Governance Structures

Today, Internet usage, while enjoying exponential adoption rates, is just beginning to achieve the market penetration of more traditional commercial media (e.g., voice telephony, facsimile and document delivery by land and air). Even within electronic commerce, the number of public key applications in use to secure communications is minute and commercial implementations are still in their infancy. Organizations that begin using PKI to enable business transactions will already have a governance structure. Several questions will be relevant to organizations that seek to become PKI Service Providers, such as: What is possible and impossible under existing structures? How much room exists to amend? Is it possible to outsource the policy drafting and administration functions so as to achieve all aims through contract rather than amendment of by-laws? If change in legacy governance system is required, how well or poorly do the PKI roles assumed by the PKI Service Provider overlay to the existing governance?¹⁰

B.4.5 Custom Governance Structure

Customizing a governance structure to accommodate a PKI-facilitated electronic commerce community poses opportunities and challenges. Parties may seek to organize a new legal entity to act as the Policy Authority for any of the following reasons:

- More favorable tax treatment and relief from regulatory obstacles
- Structured method of collaboration that avoids anti-trust violations
- Limitations of some forms of liability exposure for participants
- Member rights and duties that are fair and predictable for large and small participants

When an organization determines that a new governance structure is required or desirable to function as a Policy Authority, it can exercise some creativity and latitude in structuring governance. Governance can be structured in a way that reflects and supports the underlying business conditions and that is tailored to the functions and roles associated with the use of PKI. One approach may be to include seats on a governing board for representatives of each role played in a given PKI.

For example, in the four-cornered model, seats on the governing body might be reserved for one or more parties playing the Issuer, Repository, Relying Party and Subscriber roles. If the issues surrounding governance are too sensitive to allow representation for some or all of these parties, then

¹⁰ An example of a proposal to amend a governing structure to facilitate the use of advanced information technologies within an academic institution occurred at UCLA. The UCLA proposal includes detailed recommendations on the IT Organization and Governance Structure (including a governance board and details of several new reporting relationships involved). The UCLA plan would interrelate existing governing bodies (such as offices of the Executive Vice Chancellor) with newer governing bodies, such as an Information Technology Planning Group. (the plan can be found at the following address: <http://www.aitb.ucla.edu/itplan/GenMgmt.htm>). As in case of UCLA proposal, there may be need to meld existing governance with new governance bodies in an organization that inherits a governing structure.

other governance mechanisms, such as associate non-voting status or membership on an advisory council could be created.

PART C. Building a Business and Legal Model

Once the Policy Authority is formed and active as described in Part B, one of its initial tasks is to formulate a conceptual model describing what the participants will do in the project or endeavor that is the Policy Authority's charge. Customs and general industry practices have not yet evolved to the point that the architecture of the business system to carry out the project can be assumed—there is no tried-and-true, textbook approach to organizing the participants in a public key project. Organization of the participants must provide not only profitability and general economic efficiency but also a solid legal footing and enforceability for the expectations of the parties.

This part considers how the Policy Authority can organize the participants and structure their interrelationships within a public key-enabled project. In other words, this part is about how to architect and conceptualize a business-legal model for a public key business application.

C.1 Basic Conceptual Building Blocks

Once a Policy Authority has determined the objectives of a project, it needs a means to realize them. Public key technology offers significant utility in securing and authenticating digital information, but it is entirely dependent on human actors doing certain things. In constructing an organizational model, those *functions* that people must perform in order for the technology to be useful and valuable must be assigned to *roles* in the model. The model must also envision a way for actual, real-world *parties* to take on those roles by forming legally binding *obligations*. More specifically, with the project objectives in mind, the Policy Authority's organizational model building more or less follows these steps:

- **Derive functions** from the operational requirements of the public key technology. For the technology to work, devices and the people or business entities that run those devices must do certain things. The list of *functions* or things that must be done for the technology to work valuably is the starting point for a business-legal framework for a public key business application. The derivation of functions from roles has much to do with how usefully the technology will perform in the project.
- **Allocate functions to roles.** The Certificate Policy assigns the functions that must be performed for public key technology to work to classes of participants. Those classes or *roles* should be labeled and their functions and qualifications described. Often, the labeling and describing occurs in defining role terminology, such as “Enrolled Subscriber” or “Authorized CA.” The allocation of functions to roles tends to determine how smoothly and economically the organization will run.
- **Engage parties into roles through binding obligations.** Persons interested in a project become actual, committed participants by becoming parties to contracts or by becoming subject to other legally binding requirements that impose enforceable duties. *Obligations* are legally binding commitments that could be enforced judicially in case of a failure to perform according to the commitment. *Parties* are the persons who are thus committed.

- **Resolve disputes if an obligation is breached.** In this part, *liability* refers to an obligation that an authoritative tribunal has determined to be unconditionally due and unsatisfied. The tribunal accordingly orders a *remedy* such as monetary damages to correct or compensate for the liability. The collection or other actual realization of a remedy depends on a tribunal's ability to gain jurisdiction to resolve the dispute, which ultimately rests on its power to have its orders enforced by coercion if necessary. The effectiveness of the remedy also depends as a practical matter on the financial responsibility of the person liable.

The next sections examine these steps in greater detail.

C.1.1 Functions Allocated to Roles

Functions, the tasks that devices or people must perform for a public key infrastructure to work effectively, derive from the limitations of public key technology, because certain events or conditions must occur for that technology to be useful. For example, public key technology makes possible verifiable message authenticity or confidentiality, but one of its chief limitations is that the cryptographic key pairs used are really only mathematically related numbers. Key pairs, in and of themselves, have no association with any person whose authentication or confidentiality would be valued. Public key certification overcomes this limitation by associating a person with a specified public key, and many functions derive from the needs implicit in effecting that association in valuable, meaningful ways.

In general, the functions necessary to make public key technology useful include:

- **Key generation and safekeeping:** Public keys and their corresponding private keys need to be generated before they can be used. The utility of public key technology depends heavily on the ability to attribute usage of a particular private key to a particular person or persons. This 'attribution' of private key usage is undermined by the ability of unknown or unauthorized persons to use the private key. To assure sound attributability, the private key needs to be generated and kept in a way that precludes to a reasonable¹¹ extent access by persons who are not authorized to hold that private key.
- **Information acquisition and confirmation:** Information to be listed in a certificate, such as information identifying the Subscriber, needs to be gathered from available sources and confirmed. "Confirmation" implies a level of investigation and inquiry into the accuracy of the information that is reasonable in light of the foreseeable need. Often, an applicable Certificate Policy or certificate will specify the level of confirmation more precisely.

¹¹ As used in these Guidelines and in several other legal publications such as the ABA Guidelines, "reasonableness" and "trustworthiness" imply a balancing of available security measures in relation to the foreseeable need for them. Information security is generally a matter of degree. As applied in a particular situation, the degree of security should take into account the business objectives and needs of a project, benefits that could be gained by further security, and the foreseeable cost including the risk of loss, as well as any other relevant factors. The risk depends on the probability of a loss-causing event, the seriousness or degree of harm the loss would foreseeably present, and the methods that would be available for averting or short-stopping a loss once it begins to accrue.

- **Certificate creation:** The information to be certified, such as name and address identifying the Subscriber and stating the public key corresponding to the Subscriber’s public key, needs to be expressed in a digital form usable by the intended users or applications. The generally accepted certificate form in current practice is specified in ITU X.509. The X.509 standard specifies certain data content and, in very broad categories, the meaning of that data. Nevertheless, there is a need to further clarify the data.
- **Certificate signing:** Once formed, a certificate must be digitally signed or secured in a way that makes it attributable to its Issuer and that makes subsequent alterations of it detectable.
- **Certificate distribution:** The persons who create certificates or who use the related private key are sometimes not the same as the persons who rely on certificates, or at least, their roles are distinct and separable from a business-legal perspective. Consequently, a need exists to distribute certificates to prospective Relying Parties.
- **Certificate revocation:** A certificate may become unreliable after it is issued or may be issued in error. For example, if the Subscriber listed in a certificate loses control of the related private key, a digital signature created by that private key will not be reliably attributable to the Subscriber as a matter of fact. (Attribution may nevertheless be permissible by legal rules until the Subscriber takes appropriate action.) Often revoking the certificate (*i.e.* invalidating the certificate from a specified time forward) is the best recourse for a lost private key or a certificate that is apparently effective, but is, nevertheless, unreliable.
- **Claims, dispute resolution, and risk management:** Errors in certification on an industrial scale are inevitable, and claims based on those errors are to be expected. Mishaps, losses, or other performance difficulties may lead to disputes that will need to be resolved through adjudication, arbitration, or a similar process. The prospect of losses amounts to a risk that will need to be minimized, but even the best risk minimization will not cost-effectively reduce the risk to zero. A residual risk will need to be financed through means such as insurance, reserves, pooling or other risk-spreading arrangements, or a combination of such means.¹²

The above list is just a broad outline of certification functions. Generally the Policy Authority spearheads the allocation process because the function-to-role allocation is effected in the Certificate Policy and its implementing contracts.

The allocation of technology-based functions to roles can occur in different ways. Multiple conceptualizations of functional roles in various public key infrastructures have been proposed, and more can be envisioned. Currently, no single, generally accepted formula for allocating functions to roles can be said to predominate over other alternatives, so the possibilities in designing roles are unconstrained by convention. Practical constraints exist, however, in addition to the objectives of a particular project, or perhaps, in furtherance of those objectives.

¹² Simply shifting the risk to a party not obligated to bear the risk could violate the basic premises of the business model supporting the public key application. An effective certificate policy and its implementing contracts will eliminate loopholes that permit parties to evade their obligations and shunt risk to others who, under the business model, do not expect to bear the risk.

C.1.1.1 Considerations in Allocating Functions to Roles

The practicality of a function-to-role allocation and its success in the marketplace will depend on factors such as:

- **Economic efficiency:** Generally, functions should be grouped together and allocated to the participant in a position to perform the function at the least cost.¹³ For example, functions that require proximity to remote Subscribers should be allocated to a role that can operate in a decentralized fashion. Where accumulation of information facilitates one-stop referencing, the opposite is true and centralization is advantageous. Centralization versus distribution, availability of necessary resources (such as evidence necessary for confirmation, financial or risk-bearing capacity, secure operational capacity, degree of sophistication, ability to bear costs, etc.), and other economically significant characteristics of the stakeholders in the project bear heavily on the overall economic efficiency of a function-to-role allocation.
- **Clear risk and loss allocations:** If a party cannot clearly and precisely ascertain its risk, it might, to be prudent, take steps to carry more risk than it actually bears. For example, it may take security measures to reduce the chance of an event that would cause a loss that, in actuality, someone else would suffer, or it may obtain insurance to cover such a loss. The consequence of carrying a risk that, due to fuzzy definition, one does not actually bear are economic inefficiency (incurring unnecessary costs) and confusion in allocating losses. That confusion leads to conflict and disputes.
- **Conflict avoidance and resolution:** Making clear distinctions between functions and forensically traceable hand-offs where functions interlock among roles can reduce the likelihood of conflict. Overlapping or splitting of a single function among multiple, excessively independent roles can make decision making complicated, deadlock and buck-passing more likely, and fault and loss more difficult to apportion fairly. If decision making is shared, however, in a group acting according to orderly and efficient procedures, the quality of decisions as well as the group's control over them may improve - without intolerable additional cost in time and resources.
- **Operational controls and failsafes:** Without splitting or confusing control and responsibility for performing a function, it may be possible to create control points and failsafes to prevent errors or trap them as they occur, or at least before they become harmful. Sometimes functional role relationships can be designed so that one role checks or backs up another. For example, process flows can often include multiple steps such as expect-to-receive, send-and-receive, and acknowledge-receipt, and employee tasks can be scheduled to create a desired level of redundancy. Controls and failsafes, like system security and other risk-minimization techniques, come at a cost. Whether the cost is acceptable ultimately depends on the Policy Authority's business objectives.

¹³ “Cost” is intended here in an abstract, economic sense, and not in the sense of a price in a purchasing context.

Many other considerations may be relevant in allocating functions to roles, including the needs and preferences of people involved in a particular situation, regulatory requirements, and cultural predilections.

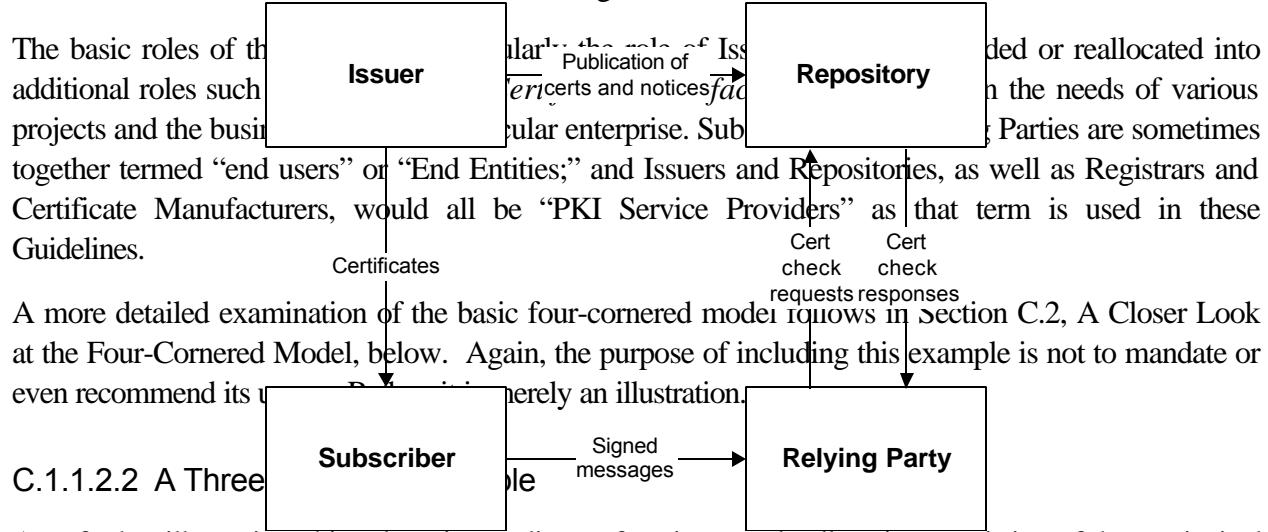
C.1.1.2 Examples of Function-to-Role Allocations

To illustrate how a Policy Authority can design an allocation of functions to roles, this subsection overviews two examples, one diagrammed with three corners and another with four. These examples are nothing more than illustrative possibilities, and these Guidelines make no recommendation regarding any function-to-role allocations.

C.1.1.2.1 A Four-Cornered Example

This example allocates functions such as issuance and revocation to the role termed *Issuer*. The person who the Issuer associates with a key pair, by means of the certificate, is the *Subscriber* of the certificate. A *Repository* disseminates certificates, notices of revocation, and related information to parties who may rely on the certificates. A Repository can also assist *Relying Parties* in other ways besides making information available, such as by helping them to observe the limitations of a certificate's trustworthiness or assurance or enabling them to obtain further assurance.

These roles and a few basic functions can be diagrammed as a Four-Cornered structure:



As a further illustration, this subsection outlines a function-to-role allocation consisting of three principal roles. It can be diagrammed as follows:

In this model, the roles designated “Issuer” and “Repository” comprise a single role designated “Issuer,” which serves both end-user roles of Subscribers and Relying Parties. More specifically, the Issuer creates certificates, signs them to their respective Subscribers, and disseminates them to their respective Relying Parties.

Compared to the four-cornered example, this three-cornered structure is simpler in structure, obligations, and information flows and hand-offs. The four-cornered model scales well for projects

involving a relatively large number of participants, a variety of transactions, and rather high values in play. For smaller-scale projects, however, the simplicity of the three-cornered approach can be a great advantage. Given they are in pilot or early in the life cycle of public key implementations, projects often center around a single or a few transactions and a relatively small group of cooperative participants. In such projects, the Policy Authority may well determine to do without differentiated roles for PKI Service Providers, and instead have a single service provider take care of all PKI functions.

Often, as in the case of the four-cornered model summarized above, the Issuer role, or other functions of a PKI Service Provider are modularized into several smaller roles, although keeping all the functions together in the same role provides simplicity, which could be desirable in a pilot, especially if its scale is small. Perhaps the most commonly employed smaller role is that of Registrar. Registrars obtain information from Subscribers for use in certificates, and may also perform other functions involving interaction with Subscribers, such as contract formation, receiving revocation requests, and customer service.

These multi-corner examples illustrate various ways for allocating into roles the basic functions that need to be accomplished for public key technology to be valuably employed. This function-to-role allocation is the initial step in the organizational engineering necessary to build a public key infrastructure into a project. Once functions are allocated to roles, the roles need to be accepted by actual parties and solidified in binding legal obligations.

C.1.2 From Roles to Obligations and Parties

Obligations are legally binding duties. The persons that obligations bind are termed “*parties*” in these Guidelines. (Parties may also be “*stakeholders*” if they have an interest in the project sufficient to make them constituents in, or members of, the Policy Authority.)

A Certificate Policy, as usually drafted, often does not name its participants, and it rarely commits them to perform their roles with binding legal force. By itself, a Certificate Policy is generally not legally binding, unless it is imposed by sovereign power such as through statutory enactment or regulatory adoption. Without sovereign imposition, the parties can bind themselves to obligations by agreeing contractually to be subject to the Certificate Policy. In the absence of contracts or sovereign enactments, the courts will extend generally applicable legal principles, called the “common law” in the Anglo-American tradition, to cover issues arising in public key applications.

All of these approaches toward achieving binding legal effect for a Certificate Policy are problematic. The common law doctrine most likely to be extended to cover public key applications relates to negligent misrepresentation. This doctrine is exceptionally vague, and varies greatly from state to state.¹⁴ Statutes and regulations are generally difficult to obtain, especially on the international level needed for the present, worldwide economy. Moreover, legislatures or regulatory agencies can fall short of the responsiveness needed to facilitate legitimate business objectives. Contracts must be formed in a

¹⁴ See Froomkin, The Essential Role of Trusted Third Parties in Electronic Commerce, 75 ORE. L. REV. 49, 96-103 (1996).

required way and on a party-by-party, one-by-one basis, and must fall within certain limitations (such as laws protecting consumers) to be valid and enforceable. Of all the means of achieving binding legal effect, the contractual alternative, is perhaps least disadvantaged and has the fewest drawbacks, particularly for private-sector projects of limited scale. These Guidelines assume, as a basic premise, a preference for contractual approaches toward achieving binding legal effect.¹⁵

C.1.2.1 Contracts and Accounts

A contract that gives binding legal effect to a Certificate Policy is termed an “*implementing contract*” in these Guidelines. As mentioned, contracts must be formed in a particular way. This section considers contract formation, the implications of the one-by-one approach required for contract formation, and the implications of the relationships that implementing contracts establish, beyond the mere incorporation of a project-wide Certificate Policy.

C.1.2.1.1 Contract Formation

In a common law legal system formation¹⁶ of a contract generally requires:

- **Parties:** Persons (including corporations, government agencies, or other legally recognized juridical entities) who have the legal capacity to contract (*i.e.* are not under the age of majority, adjudicated to be mentally incompetent, or subject to some other legal disability).¹⁷
- **Mutual assent:** The parties to the contract must come to an apparent¹⁸ agreement or “meeting of the minds” on the essential terms of the contract.¹⁹

¹⁵ Reliance on contracts to achieve binding legal effect does not rule out other approaches—the question of how to make a certificate policy legally binding is not an either-or question. It is possible to rely in the first instance on a contractual approach and also to rely on a statute such as Utah’s as a backup. One can also consider the common law outcome in the event that both the contract and statute fail to accomplish the requisite binding effect.

¹⁶ A contract, though formed according to these rules, may be rendered invalid or unenforceable by another rule. For example, statutes commonly termed “statutes of frauds” in the Anglo-American legal tradition forbid enforcement of contracts not expressed in a signed, written form. Consumer protection statutes, common law restrictions on the enforcement of illegal or unconscionable contracts, and other rules all limit the basic power to make effective contracts.

¹⁷ *Harrison v. Grobe*, 790 F. Supp. 443, 447 (S.D.N.Y. 1992); *Daniels v. Thomas, Dean & Hoskis, Inc.*, 804 P.2d 359, 363 (Mont. 1990); *see generally* RESTATEMENT (SECOND) OF CONTRACTS §§ 12, 16 (1991).

¹⁸ An actual, subjective agreement is not required, and the real content of any party’s mind at the time of contracting is irrelevant. What counts for contract formation is a *manifestation* of assent, and contract formation is judged by objective criteria. Thus, having evidence of the manifestation of assent is important but undertaking the difficult task of proving what was on anyone’s mind at the time the contract was made is unnecessary. *See Zeman v. Lufthansa German Airlines*, 699 P.2d 1274, 1281 (Alaska 1985); RESTATEMENT (SECOND) OF CONTRACTS § 17 cmt. c (1991).

¹⁹ *Federal Lumber Co. v. Wheeler*, 643 P.2d 31, 36 (Co. 1981).

- **Consideration:** In the Anglo-American legal tradition, a contract must rest on a bargain that is not wholly one-sided, and the law does not protect commitments that are entirely gratuitous.

These contract-formation requirements, other than the requirement of consideration, generally hold true in legal systems outside the Anglo-American tradition as well.

The mutual assent required for contract formation is often indicated by signing written agreements (either with ink or digital signatures), or can be accomplished suitably by another means of manifesting assent in a provable manner. A written or other clear, recorded expression of the agreement helps achieve clarity and precision in defining the parties' obligations, which in turn makes those obligations easier to perform. Besides a clear, provable expression of obligations, mutual assent requires expression of each party's intent to be obligated. That intention is customarily implied from a signature, but the person offering the contract may, within fair limits,²⁰ define it to be another act.

More concretely and assuming the four-cornered model, contract parties can indicate mutual assent and form contracts in the following ways, among others, depending on the needs of a particular project:

- **One-stop double enrollment:** When a person agrees with an Issuer to be a Subscriber, the person can also agree to be a Relying Party. Issuers, perhaps acting through Registrars, may well have direct, personal contact with their Subscriber customers, and signing a written contract in the traditional manner is not difficult in those circumstances. The Relying Party contract can also provide for use of the Repository, although an agency or another arrangement will be necessary if Repository services are provided by a party other than the Issuer.
- **Online, digitally signed contract:** If a person, particularly a prospective Relying Party, approaches a contract-based system online and has a digital signature capability, the person can use that digital signature to accept and sign an online offer from the Repository, presented via a Web page.
- **Clickwrap:** In some situations, contracts can be formed by clicking an on-screen button labeled "I agree" or by making a similar manifestation of assent by entirely electronic means.²¹ Optimally, the document proffering the contract and its agreement button should record evidence for subsequently proving that the contract-formation event occurred. Such evidence should include the system date on which the agreement button was clicked, the user's login identification, the user's network node name (*e.g.* current domain name) and address (*e.g.* current Internet protocol address), etc. The agreement process can also ask for user information and require a password, although confirmation of the information thus obtained will be problematic in an online, clickwrap setting.

²⁰ One would be party's power to treat some events as manifestations of assent is limited by fairness considerations. Generally, silence or inaction by one party do not indicate assent. Assent can be indicated by "acceptance of the benefit of offered services with reasonable opportunity to reject them and reason to know that they were offered with the expectation of compensation." See RESTATEMENT SECOND OF CONTRACTS § 69 (1981).

²¹ See generally T. Smedinghoff, ONLINE LAW 81-83 (1996).

Many variations of or alternatives to these examples are possible. The essential requirements for forming contracts require simply a manifestation of assent by suitable parties to a bargain, and online contracting opens needs and possibilities for creativity in making and documenting such manifestations.

C.1.2.1.2 System Uniformity and Closure

One implication of the contract-formation process just described is that contracts must be made one by one. They can have more than two parties, but all of the parties must complete the assent process for the contract to be validly formed. The greater the number of parties involved in a contract, the more difficult it is to amend or terminate it, or to resolve disputes.

The one-by-one nature of contracting makes it difficult to be certain that all participants in a project are bound by its rules, including mainly its Certificate Policy.²² Achieving assured closure of a system of participants is particularly difficult in the case of Relying Parties. In that regard, see Section C.2.4. Achieving a desirable level of system closure may necessitate a preclusion of reliance on certificates by prospective Relying Parties who cannot demonstrate that they have contracted for participation in the system. (See Section C.2.4. for more detail on these issues relating to Relying Parties and various means of precluding reliance.)

Making contracts one-by-one with all participants in a large system can also create challenges of scale. Large-scale contracting requires a tree-structured networking of the contract-formation process in order to reach the level of each individual party, and that networking will require management. One task of the contract manager will be to assure a sufficient degree of system-wide uniformity among the one-by-one contracts, so that they all add up to a coherent system of rights and obligations that is free of anomalies despite the capability for individual parties and contracts to include provisions inconsistent with the overall scheme.

Moreover, because contracts are made only between those parties assenting to a given instance of terms, making the contract's efficacy reach all of the parties that it needs to reach is a further challenge. Contracts generally apply only between the parties to them (a concept that lawyers call "privity"); this limitation on the scope of a contract's binding effect creates a difficulty in scaling contract systems.

Despite all these difficulties, bankcard, automatic teller, and clearinghouse systems demonstrate that large-scale webs of contracts are feasible. Generally, such systems have arisen after pilot projects and experience gathering, a stage similar to the stage of public key development as of this writing. From small beginnings, these systems have grown to be worldwide networks of privately made, legal rules. They demonstrate convincingly the ability of contract-based systems to traverse legal systems' boundaries in a cost-effective manner. The bankcard, automatic teller, and clearinghouse examples also demonstrate the need for a central coordinating body. The Policy Authority can fill that role, as can any other agent trusted by all participants in the project to supervise the contract infrastructure.

²² See generally Greenwood, Risk and Trust Management Techniques for an "Open But Bounded Public Key Infrastructure, 38 JURIMETRICS 277, 287-92 (1998).

Although a need to supervise contracting exists in order to establish a consistent and sufficiently extensive system of legal rights and obligations, the scope of that supervision and the limitations on contractual flexibility that it could impose need to be prudently bounded. Implementing contracts should incorporate the Certificate Policy and be consistent with it, but there is no reason to preclude implementing contracts from including additional provisions consistent with the policy to structure and govern the relationship between the parties. That relationship between a service provider and customer is the framework within which public key services will be obtained and provided, and the framework must have enough range and flexibility to achieve marketability and mutual economic advantage if public key services are to be commercially viable.

C.1.2.1.3 Ongoing Relationships: Accounts

As mentioned, an implementing contract essentially establishes a customer relationship. In conventional banking parlance, that customer relationship is termed an *account*.²³ In the four-cornered model, for example, a Subscriber's account is with an Issuer and a Relying Party's account is with its service provider, a Repository. Because an Issuer publishes its certificates into a Repository, it has a publisher's account (as distinct from a Relying Party account) with the Repository. Contractually established rights and duties between the Issuer and Relying Party are also necessary, and must be established either by the Repository acting on the Issuer's behalf or by the Issuer directly (as explained below in Section C.2.4).

Accounts establish ongoing, potentially long-term relationships. They thereby make possible the tracking of an account history, which can greatly enhance an Issuer's ability to confirm the accuracy of information in certificates, and accounts serve other functions as well. It is relatively easy to perpetrate a quick fraud on an Issuer, but it is considerably more difficult to maintain the fraud over time, through various transactions, and from one certificate through the next. Because certified information is most efficiently confirmed on a per account basis, any number of certificates containing that information can be issued for the account. A prudent Issuer will also manage its certification risk on a per account basis, accumulating the risk of all outstanding certificates for the Subscriber or account holder across the whole account.

Thus, to sum up the need for contracts and the account-relationships that result from them, the Policy Authority designing a business-legal model needs to provide a way to crystallize functional roles into legally binding and enforceable obligations and rights. Contracts are a means to that end, but the design of a management process to form all the necessary contracts and to manage that process of contract formation and the enforcement that flows from it. The management process should not, however, prevent vendors competing in the marketplace from developing commercially viable product offerings. Stifling creativity and innovation in customer relations among competing vendors will tend to hinder the effectiveness of the market in continuing the development of public key infrastructures.

²³ The “account” concept is common in the banking business, but other business traditions may well opt for other approaches to customer relationships. The description of the account concept here is not a recommendation.

C.1.2.2 Certificates and the Problem of Certificate Meaning

In addition to the implementing and account-establishing contracts, the certificates themselves have important legal significance and effect. Contracts are optimally made once per relationship. Amending or remaking them can be difficult, particularly in a large-scale system in which the contract-making network is large and widely distributed. Certificates issued in an account, on the other hand, are more current, and can more easily be tailored to the needs of a particular application or changing environment. Thus, contracts and the certificate policies they incorporate ideally are made only once, and in rather general terms, but certificates adapt those generalities to a particular customer's or project's present needs and circumstances.

The expressive capabilities of certificates in their fielded, standardized form, however, are extremely limited, so limited that it is not possible to know from the face of a certificate exactly what it means. Consequently, standardized certificates leave the rights and obligations of the parties, particularly of the Issuer and Relying Party, in substantial uncertainty. To solve this problem, a *certificate profile* (a specification of the fields, permissible content, and the range of permissible interpretation for those fields) for a particular certificate type can help make certificates understandable. In addition to, or in lieu of, a certificate profile, a *documentary version* of the certificate can place the certificate fields in a natural-language context and clarify their meaning. A documentary version of the certificate maps the certificate's fields into a documentary form, in which the declarative context implicit in the certificate is made explicit and clear.

An implementing contract must take into account the certificates to be issued pursuant to the contract and the interpretation to be given them. One way for the implementing contract to deal with the certificates to be issued is for the contract to provide for acceptance of those certificates (in the case of a Subscriber) or for reliance on those certificates (in the case of a Relying Party) in their documentary forms only. The contract thus becomes somewhat open ended, allowing certificates to vary by type, application, and other certificate-specific circumstances, while the certificates all fall under the legally-effectuating and perhaps long-term superstructure of the implementing contract and Certificate Policy.

These Guidelines envision that implementing contracts and the certificates issued under them (in their documentary renditions) are the instruments that give legal effect to certificate policies based on these Guidelines. In other words, implementing contracts and documentary certificates translate functional roles in an abstract architecture into binding obligations and enforceable rights. Enforcing those rights is the process of converting an obligation into a liability.

C.1.3 From Obligations to Liability and Legal Remedies

Legally, a significant difference exists between an obligation that is a mere promise, even if that promise is breached (*i.e.*, broken), and an obligation that has been adjudicated as due and immediately and unconditionally enforceable. This section terms the latter sort of adjudicated obligation a "liability," and uses "obligation" to refer to a simple promise that is as yet unadjudicated and perhaps also unbreached.

The previous section dealt with the process of converting the functional roles of an abstract design into obligations to give legal effect to the functional roles in a public key infrastructure. This section concerns

itself with the conversion of obligations into liabilities, a process in which the obligation becomes fixed and collectable and any issues or conditions about it are resolved. Converting an obligation into a liability requires a forum to conduct adjudication or a similar dispute-resolution process culminating in a judgment, order, or other award.

C.1.3.1 Choosing a Forum

In general, the parties, and often predominately the plaintiff, choose who will determine liability. The forum or tribunal can be judicial, in other words, the courts of a particular legal system. Which legal system and courts depends on where the party seeking enforcement (the plaintiff) can gain jurisdiction for the court over the defendant (the person against whom the claim of an unsatisfied obligation is asserted) or the defendant's assets. Within the United States, jurisdiction over a business enterprise can generally be established in any state where the enterprise has substantial business activity, and the courts of other states are obliged by the federal Constitution to give "full faith and credit" to the judgments of the courts in sister states. Internationally, jurisdiction is more difficult to obtain, and judgments are more difficult to enforce in foreign courts. Moreover, concerns about national or parochial favoritism or other issues might also lead to a preference for arbitration in resolving international disputes.

Arbitration is a process similar to adjudication, but it is performed by one or more non-governmental officers agreed upon by the parties. Often, arbitrators are more specialized and expert in the subject matter of their proceedings than are most judges. Arbitral proceedings are also somewhat less formal and time-consuming than are adjudications. However, to compel enforcement of an arbitral award, an arbitral award must be converted into a judicial order by suing on it in a court having jurisdiction, although court may not fully review or reconsider the arbitral award if the parties have agreed that the arbitration would be binding.

In addition to courts and arbitration, other forms of dispute resolution can be employed, but they are less common in commercial contexts.

C.1.3.2 Remedies

Whatever the forum the disputants choose to convert a breached obligation into a liability, the forum will have the task of devising an appropriate method of redressing or compensating for the liability of the party breaching its obligation. An adjudication of liability holds that the breach occurred and requires redress, but it is another matter to devise a remedy that fits the liability and achieves appropriate redress.

Generally in the Anglo-American legal tradition, monetary damages compensating for liability are preferred over other possible remedies like orders to perform or refrain from a specified act. Moreover, the monetary compensation generally covers only losses that the breaching party could reasonably foresee at the time it should have performed them.²⁴ Damages for an unforeseeable or

²⁴ See *Prutch v. Ford Motor Co.*, 618 P.2d 657, 661-62 (Colo. 1980); *Hadley v. Baxendale*, 156 Eng. Rep. 145 (Court of the Exchequer 1854); RESTATEMENT (SECOND) OF CONTRACTS § 351 (1981).

indirect harm, such as an inability to take advantage of a lost opportunity, the consequences of a business interruption, etc., are termed *consequential damages* and are generally not recoverable unless an agreement requires otherwise. Moreover, in cases where tort liability is determined for a defective product, damages are generally due under the law of most states in the United States only for bodily injuries, not for purely economic losses.²⁵

In considering the risk of nonperformance, it is important to consider not only whether an appropriate forum will conclude that liability exists for the nonperformance of an obligation but also what remedy that forum is likely to award. A delay in performing as obligated, for example, may clearly result in liability, but the foreseeable, direct harm caused by a minor business delay can be quite minimal, and therefore, the available remedy is also minimal.

Legal liability and a legally appropriate remedy are, however, only some of factors to consider in a dispute. Disputes have other costs, such as the cost of resolving them (including attorney and forum fees), as well as time, focus, and inconvenience. Conflict can also affect customer relations, especially if one side perceives that the other lacks merit. Each party needs to consider the overall business impact of each dispute in addition to its legal position.

C.1.3.3 Enforcing Remedies and Financial Responsibility

The breach of an obligation can be reduced to a liability for which a forum awards a remedy, but that remedy will not mean much if it cannot be collected or otherwise realized. An award of damages does not mean that the defendant has assets available to pay the damages, and the award, even though judicially ordered, can be discharged (*i.e.* be ordered unenforceable) in a bankruptcy case. The ability of a PKI Service Provider actually to make good its promises through real assets is an important factor to consider in evaluating the trustworthiness of the service provider and the significance of its promises.

Various indications of commercial security (as distinct from technical security), credit, or creditworthiness can firm up obligations with real financial assurance. Bonds, standby letters of credit,²⁶ balance sheets and asset reports, and other indications of financial capacity help assure that a PKI Service Provider is able to satisfy its liabilities and form the foundation of commercial-grade trust.

²⁵ See *Rockport Pharmacy, Inc. v. Digital Simplistics, Inc.*, 53 F.3d 195 (8th Cir. 1995); *Fireman's Fund Ins. v. SEC Donohue, Inc.*, 679 N.E.2d 1197, 1199 (Ill. 1997); *Clark v. International Harvester Co.*, 581 P.2d 784, 791 (Idaho 1978); see generally R.R. Fox and P. J. Loftus, *Riding the Choppy Waters of East River: Economic Loss Doctrine Ten Years Later*, 64 DEF. COUNS. J. 260 (1997).

²⁶ Bonds and standby letters of credit provide alternative sources of funding from which damages can be collected, and that fact, in turn, calls for a procedure for collecting the funds. A certificate policy requiring bonds or standby letters of credit should include an orderly process enabling multiple claimants to determine their respective priorities in the available funds.

C.1.4 Conclusion on Model Building Blocks

Putting public key technology to work requires not only technology that functions securely but also an organizational model or framework capable of using that technology for business purposes in a way that comports with applicable law. Developing an organizational model can consist of allocating technologically based tasks to roles, solidifying the roles into legally binding obligations, and enforcing the obligations as the need arises.

Many organizational models can be envisioned and have been suggested. Some have been outlined briefly in Section C.1.1.2 above. One illustrative organizational model outlined in that section is the four-cornered model, which the next section examines in greater detail.

C.2 A Closer Look at the Four-Cornered Model

These Guidelines do not require or recommend any particular model for the business-legal framework necessary for the public key aspects of a project. The purpose of examining a model in this section is to provide a case study illustrating how the functions of public key technology can be grouped together efficiently into roles, which in turn can be implemented contractually as obligations. While this case-study exercise may fit some actual business-legal models and certificate policies, it will not fit them all. Opinions vary quite widely, even within the Task Force authoring these Guidelines, about the optimal design of business-legal models for public key applications. Because current PKI projects are still in the pilot or early implementation stages, opinions tend to rest on theories that have not been validated by actual, wide-scale experience. It is simply too soon in the emerging public key industry to know from actual business experience which business-legal models work the best.

With that cautionary note, a detailed examination of the four-cornered business-legal model follows in this section, after brief consideration of the whole issue of how many corners.

C.2.1 Three Corners, Four, or More?

The examples briefly outlined in Section C.1.1.2 differ, not in the number of end-user roles, but rather in the number of separate roles broken out for PKI Service Providers. Particularly in early business-legal models, the Issuer and Repository functions were not differentiated, but a Registrar's role often was. In the ABA Guidelines and Utah Act, separate roles were defined for the Issuer (Certification Authority) and the Repository, but a separate role for the Registrar was hardly mentioned although the ABA Guidelines recognized the possibility for a variety of "ancillary services."²⁷ Since then, certificate manufacturing (i.e., outsourced operational services in support of an Issuer) and other service provider roles have gained attention. Clearly, there is nothing even an approaching a definitive or generally accepted division of roles for PKI Service Providers.

²⁷ ABA Guidelines § 1.2. (1995).

Examining all of the possible role divisions and models and weighing the merits of them all in relation to each other would exceed the scope of this introductory part, but an examination of how to go about building out a business-legal architecture would be too abstract if left at the highly conceptual level of the preceding sections. To illustrate an extensively elaborated business-legal architecture and stimulate thought about alternatives and variations, this section takes up the four-cornered model as a case study.

Compared to the four-cornered mode, the three-cornered model (summarized in Section C.1.1.2) has the advantage of greater simplicity, and it may be easier to implement in pilot projects or projects in which one PKI Service Provider will perform both Issuer and Repository functions for the term of the project. Combining the Issuer and Repository roles also eliminates the need for clear hand-offs between the two roles. The four-cornered model, with Issuer and Repository functions allocated to distinct roles (which nevertheless could be performed by the same person), has advantages such as these relative to the three-cornered model:

- **Customer focus:** For the most part, the Issuer serves the Subscriber as its customer (albeit with great consideration for the Relying Party), whereas the Repository serves the Relying Party. The difference between the Subscriber and Relying Party roles is conceptually thorough, and their needs differ almost entirely. Consequently, the basic business objectives of the Issuer and Repository are different.
- **Availability requirements:** Reliance happens more frequently than issuance, and the need for reliance support is therefore greater. It is also more difficult to predict or to constrain reliance within certain hours of the day in a particular time zone. Because reliance occurs frequently and around the clock, a Repository must generally be available 24 hours a day, seven days a week. The need to issue certificates at any time, however, is generally less than the need to rely on them at such times.
- **Online or offline:** Reliance requires online contact with the Repository over widely available communications channels. Issuance, however, need not be online, and is often performed offline for security reasons. A Repository is, therefore, an open, on-the-net service, whereas an Issuer provides service from a much less open, and often closed, information system.
- **Local or large and central:** An Issuer must generally have a presence local to the Subscriber, or at least with some direct contact with or proximity to the Subscriber, in order for the Issuer to confirm the accuracy of information about the Subscriber such as the Subscriber's identity. For example, an employer is often in an excellent position to identify its employees because of its familiarity with them. The proximity requirements of issuance and the much higher information quality obtained from primary, first-hand sources tends to make the centralizing and scaling of the Issuer role difficult. On the other hand, reliance on a certificate once issued is a global possibility, so a Repository needs to be ubiquitous. The need for efficiency will tend to give an advantage to centralization rather than distribution, in order to prevent moving around from one location to the next in search of the needed data. Moreover, the utility of a particular Repository increases in proportion to the size of its data inventory, so repositories have an incentive to be large as well as centralized.

- **Risk model:** The value of public key certificates lies in the assurance they provide to Relying Parties, and that assurance translates to a risk for the Issuer. If certificates are valuable, they provide significant assurance, and the Issuer undertakes a significant risk. Because of this risk, the expense side of the Issuer's business model will tend to resemble that of an insurance provider: a chance or probability of casualty losses plus operational expenses.²⁸ A Repository, on the other hand, bears little risk of fraud and the like. Instead, it has an operational risk, such as service interruptions, much like that of a public utility.
- **Revenue model:** Just as the expense side of an Issuer's business model resembles that of an insurance provider, so does its revenue side: In essence, the Issuer obtains revenue in return for taking on a risk, such as a fraud risk. In contrast, the Repository's revenue model for ongoing reliance support resembles that of a public utility.

Although distinguishing between Issuer and Repository has some advantages in the abstract, the distinction is just theoretical. The two roles can be, and often are, combined into a single role (as in the three-cornered model) and may in any event be performed by one party. To illustrate the development of a model, however, the remainder of this section assumes that Issuer and Repository are separate roles.

C.2.2 Issuer Functions and Obligations

In the four-cornered model elaborated here, the Issuer of a certificate (sometimes termed a Certification Authority) is viewed as having certain functions and owing certain obligations to Subscribers and Relying Parties. Generally, the Issuer's obligations with regard to a certificate remain inchoate, or any harm for breach of them is reversible, until the Issuer releases the certificate outside its organization. Usually the Issuer first releases the certificate to the Subscriber for the Subscriber's acceptance.

This section provides an overview of an Issuer's functions and obligations, many of which can be grouped differently than in this general collection or can be allocated to others.

C.2.2.1 Issuer-Subscriber Functions and Obligations

Broadly viewed within this example of a four-cornered model, an Issuer does the following for Subscribers:

²⁸ If certification risk is transaction-specific, it closely resembles other fraud risks that banks have long borne. For example, banks are familiar with the risk of paying an instrument over a forged endorsement, or making a wire transfer from an account based on fraudulent authorization. The nature of these risks is almost exactly the same as the risk of erroneously identifying the Subscriber of a certificate, except that a certificate may not be transaction-specific, unlike a commercial-paper instrument, for example. Many certificates may be relied upon in any number of transactions and by any number of Relying Parties. Thus, unlike forged instruments, which represent single points of risk, many certificates create vectors of risk that can be used in a wide range of transactions.

- **Issue certificates:** Perhaps the Issuer’s most fundamental commitment to a Subscriber is to issue certificates for the Subscriber’s account as requested by the Subscriber.²⁹ Once the information to be included in certificates has been confirmed and as long as the Subscriber’s account remains in good standing, a Subscriber may obtain certificates for its account by request, in accordance with rules (including the Certificate Policy) applicable to the account. The Issuer generates certificates listing its name in the **Issuer** field,³⁰ signs the certificates, and returns them to the Subscriber for acceptance.
- **State certified information accurately:** For Subscribers as well as for Relying Parties, the Issuer obligates itself to represent information in the certificate accurately according to a defined level of certainty or confirmation specified in the certificate and as of the date on which the certificate is issued.³¹
- **Notify the Subscriber of issuance:** Upon issuing a requested certificate, the Issuer informs the Subscriber of the issuance and provides a means for the Subscriber to review and accept the certificate before it is published or otherwise released to prospective Relying Parties.
- **Invalidate a certificate on request:** The Issuer also promises Subscribers that it will revoke or otherwise invalidate³² a certificate and give notice of the invalidation on receipt of a verifiably

²⁹ Illinois Electronic Commerce Security Act § 15-310(1) (effective July, 1, 1999) (hereinafter “Illinois Electronic Commerce Security Act”); Utah Code Ann. § 46-3-302(1)(a) (1996). Like all contractual undertakings, the obligation to issue on request is entered into voluntarily. Indeed, a certifier may well retain a right to determine whether it will issue on a certificate-by-certificate basis. Complete discretion in determining whether to issue any certificate at all, however, could make the contract rather one-sided and potentially empty, and could raise consideration issues in common law legal systems.

³⁰ The listing of the Issuer’s name in the **Issuer** field of the certificate is the defining act of the Issuer in the four-cornered model. All obligations other than this one can be reallocated by contract or the certificate policy, or delegated to others by the Issuer, but if an Issuer loses its identification as such in the certificate, it ceases to fit the definition of “Issuer.”

³¹ This obligation of accuracy does not apply in relation to the Subscriber if the Subscriber was the source of the information or is in a better position to know of its accuracy.

³² Revocation is final; a certificate, once revoked, is never again valid. The finality of revocation can sometimes make revocation a somewhat extreme remedy, particularly in cases of uncertainty or where the grounds for invalidation are not lasting. Suspension, the temporary invalidation of a certificate, better fits a situation in which the grounds to revoke are temporary, but, since suspension wholly invalidates the certificate, albeit only temporarily, it can be seen as an excessively black-or-white tool for dealing with uncertainty. It is also difficult to implement in some technological systems, and requires repeated checking for updates. Many public key systems have declined to provide for certificate suspension in practice.

In cases where full, permanent invalidation is unwarranted and the amounts at stake warrant significant attention, a Repository can pass through to a prospective Relying Party a message from the Subscriber advising the party of a difficulty that has arisen. Such a message can be much more informative than an either-or notation of temporary invalidity (suspension) because it can explain the situation and enable the Relying Party to arrive at a more informed decision whether to proceed to rely in a questionable situation or to forbear.

authentic request from the Subscriber of the certificate.³³ Contracts may also provide for other notices regarding certificate reliability.³⁴

- **Publish certificates:** The Issuer publishes certificates and notices of revocation in a Repository. The Repository may also provide other services to Subscribers in cooperation with the Issuer, in addition to serving the Subscribers in their possible role of Relying Parties.
- **Provide important information and customer support:** The Issuer may inform its Subscriber customers of important information necessary to perform the Subscriber's obligations, and may agree to provide additional customer service. Customer service commitments vary according to the contractually required level of service. Service can include advice regarding safekeeping of the Subscriber's private key and notification of serious system failures affecting the Subscribers, such as compromises of a key impairing the reliability of a certificate needed to verify the authenticity of a certificate issued to the Subscriber.
- **Observe agreed-upon confidentiality restrictions:** Information in a certificate is ordinarily not confidential, although the certificate may identify the Subscriber by a pseudonym that only the Issuer can associate with a real Subscriber³⁵ subject to limitations specified in the contract between the Issuer and Subscribers or as otherwise required by laws such as data protection or privacy statutes. The Issuer should generally keep information about the Subscriber that does not appear in the certificate confidential.³⁶ This information includes items such as evidence used to identify the Subscriber, billing and account history information.

Additional functions and obligations may be appropriate. For example, an Issuer could agree to assist the Subscribers with key generation or to keep a spare copy of a key used for decryption in case of accidental or improper use of an encryption capability.

³³ According to most certificate policies and implementing contracts employing the four-corner model, the Issuer may revoke a certificate regardless of whether the Subscriber requests or consents to revocation, but only for serious problems and with prompt notice to the Subscribers as well as to prospective Relying Parties. A serious problem that is the Subscriber's fault may also breach the contract between the Issuer and Subscribers, and may result in closure or other deactivation of the Subscriber's account with the Issuer.

³⁴ Suspension of certificates is a means of invalidating a certificate temporarily, short of permanent revocation. However, suspension can be somewhat difficult to implement, and is perhaps a rather crude means of dealing with uncertain or unauthenticated grounds for revocation. Rather than resorting to the harsh, all-or-nothing technique of suspension, the Repository may pass through a message from the Subscriber or other party permitted to give notice to Relying Parties. Such a message would not invalidate the certificate but could explain reason for caution or forbearance in relying on it or indicate what the author recommends, albeit in a non-mandatory way.

³⁵ Once the Issuer discloses the certificate-Subscriber association, it can become difficult to control the dissemination of that disclosure.

³⁶ The power of a service provider to keep information confidential is limited by the government's power to search. Banks, for example, have been required to open their files in response to search warrants against their customers, *see United States v. Miller*, 425 U.S. 435, 96 S. Ct. 1619 (1976) (subpoena requiring a bank to produce a customer's documents did not violate customer's Fourth Amendment rights); *see also* Bank Secrecy Act of 1970, 12 U.S.C. § 1829b (1997).

From the Subscriber's point of view, the objective of a certificate is ordinarily to enable the Subscriber to send authenticated messages to Relying Parties. The Subscriber's motivation to obtain a certificate, however, is often indirect and stems from the needs of Relying Parties. Relying Parties realize the most direct benefits from improved message security through public key certification, because the Relying Party takes the principal, direct risk of a forged message.

C.2.2.2 Issuer-Relying Party Functions and Obligations

Persons who receive and rely on digital messages take risks that include the inability (1) to attribute the message to its apparent signer, and (2) to demonstrate that the message is the same as the one signed, *i.e.*, that the integrity of the message is intact. Attribution of the message to the signer depends on the certificate linking the signing key pair to the signer. Demonstrating message integrity requires verification by the appropriate public key. By making provable attribution and message integrity possible, a certificate has the effect of transferring much of the risk of nonauthentic digital messages from the Relying Party to the certificate Issuer. In that risk transfer from the Relying Party to the Issuer lies the core value of certification, and that value is realized most directly by the Relying Party.

Thus, for Relying Parties, the value of certification is, in essence, the functions and obligations that the Issuer performs to reduce the Relying Party's risk of a nonauthentic message. In the four-cornered model, the functions and obligations are primarily:

- **Confirm accuracy:** The Issuer confirms³⁷ the accuracy of information to be listed in the certificate. Depending on the scope of the duty to confirm, it could include an obligation to state accurately all information that is foreseeably material to the reliability of the certificate.³⁸
- **Record certificate acceptance:** The Issuer obtains evidence indicating the Subscriber's acceptance of the certificate before releasing the certificate for reliance.³⁹ A Subscriber may not be legally bound in relation to a Relying Party if the Subscriber has not accepted the certificate in

³⁷ The concept of "confirming" includes a level of effort reasonable to investigate and ascertain accuracy that is appropriate in light of the uses and reliance foreseeable for the certificate. This relative concept can be further defined in setting a certificate's assurance levels and particularly in specifying a level of certainty. See Illinois Electronic Commerce Security Act , §15-310(2); Utah Code Ann. § 46-3-103(8); ABA Guidelines 1.9 (1995) (defining "confirm" as "to ascertain through appropriate inquiry and investigation").

Confirmation must occur for all information listed in the certificate as confirmed, but it does not follow that confirmation must occur every time a certificate is issued. In a contractually based account system, the Issuer may confirm on a per-account basis. The evidence necessary to confirm the accuracy of information to be listed in a certificate can be gathered and confirmation thus performed as the account is opened, for all certificates to be issued in the account. Further, while the account is open, additional information accumulates about claims filed and other incidents as well as about certificate usage, and that information can be additional source material for confirmation of certificates issued in the account.

³⁸ The obligation of accuracy may be imposed according to varying standards of care. For example, an Issuer could obligate itself to refrain from negligence (*i.e.*, to exercise the degree of care that a reasonable person would exercise in the circumstances), or to be absolutely, unqualifiedly accurate (perhaps up to a specified payout cap).

³⁹ ABA Guidelines 3.10(2).

question, and the Issuer may be in the best position to obtain evidence of acceptance when it occurs.

- **Provide quality operations:** The Issuer uses a “trustworthy system”⁴⁰ to issue and revoke certificates, to publish a certificate or notice of suspension or revocation, and to safeguard its private certification key.⁴¹ If the Issuer creates a private key for the Subscriber, the Issuer must also use a trustworthy system to do so. The Issuer must also employ personnel practices that provide reasonable assurance of trustworthiness.⁴²
- **Give notice of invalidation:** The Issuer gives notice of revocation (and suspension, if supported) using certificate revocation lists or other suitable means, when revocation is required or appropriate.⁴³ Ordinarily, notice of revocation is published into a Repository, from which Relying Parties obtain it as needed. A certificate, Certificate Policy, or other binding document should inform Relying Parties about where to look for notice of invalidation, especially if a project envisions using multiple Repositories within its bounds. Especially when checking for invalidity is automated (as it usually is), the form and manner in which notice is to be given should also be specified.
- **Provide quality customer service:** The Issuer must provide customer service and claims support through several service plan options reflected in Relying Party contracts.

The above list can be extended to include other functions, depending on the needs of a particular project. For example, an Issuer could assist the Subscriber by securely keeping a spare copy of a key used for decryption.

C.2.2.3 Other Issuer-Related Roles

An Issuer’s basic set of obligations can be divided and reallocated by a Certificate Policy or delegated by subcontract in many ways. By definition, an Issuer is a person listed in the certificate in the Issuer field. Besides that basic, defining representation in the certificate, technical standards such as ITU X.509 often assume the Issuer creates and digitally signs the certificate in which its name appears.

In practice, however, the functions associated with the Issuer in the above lists are often performed by other roles, even within a model that basically follows the four-cornered concept. For example, some

⁴⁰ “Trustworthy system” is a relative concept determined according to a reasonableness test. Utah Code Ann. § 46-3-103(37) defines “trustworthy system” as “computer hardware, software, and procedures that: (a) are reasonably secure from intrusion and misuse; (b) provide a reasonable level of availability, reliability, and correct operation; (c) are reasonably suited to performing their intended functions.” The trustworthiness of the system and more details about it can be specified in contracts and their incorporated technical specifications.

⁴¹ See also Illinois Electronic Commerce Security Act § 15-301; Utah Code Ann. § 46-3-301(1) (1996); ABA Guidelines 3.1.

⁴² See also Illinois Electronic Commerce Security Act § 15-301; Utah Code Ann. § 46-3-201(1)(a) and (b) (1996); ABA Guidelines 3.4.

⁴³ See also Illinois Electronic Commerce Security Act § 15-301; Utah Code Ann. § 46-3-306(3) and § 46-3-307(5) (1996); ABA Guidelines 3.12.

functions that the Issuer could and often does perform are assigned instead to the roles of Registrar or Certificate Manufacturer. In many models, a Registrar or Registration Authority performs tasks such as contract formation with Subscribers, confirmation, and other customer service functions with the Subscriber. Alternatively in some models, an Issuer outsources the generation and signing of certificates and notices of revocation and related operational and security obligations to a party in the role of Certificate Manufacturer. The next subsections consider these two examples of roles separated from the overall issuance functions.

C.2.2.3.1 Registrar

A Registrar, as noted, performs a subset of the functions and obligations ascribed to an Issuer. In some situations, using a Registrar local⁴⁴ to the Subscribers rather than having the Issuer develop its own extensive local presence can facilitate good customer service and help assure the quality of information necessary for confirmation. For example, a company obtaining certificates for its employees is usually in a good position to address the certification needs of its employees, the prospective Subscribers, and to provide high-quality information, particularly information about them, for inclusion in certificates. The company, however, may not wish to take on the operational demands and the risk that certificate issuance entails. Thus, while the company would be the original source or gathering point of much of the information in the certificates it needs, it has little interest in generating, digitally signing, or taking responsibility for those certificates. A company in such a situation is a good candidate for the role of Registrar.

Conventionally, the subset of issuance functions and obligations assigned to the Registrar role consists of:

- **Confirmation:** The Registrar gathers evidence necessary to confirm the accuracy of information to be included in the Subscriber's certificate(s). The Registrar may itself be the source of the evidence. Evidence may come from secondary sources (such as driver's licenses, passports, etc.), or from primary sources such as relatives, friends, co-workers, and other sources with direct familiarity with the Subscriber.
- **Intake of revocation requests:** The Registrar may also receive requests from Subscribers for revocation of their outstanding certificates and forward such requests with the Registrar's endorsement to the Issuer (or other person with authority to revoke). In thus initiating a revocation, the Registrar must ordinarily confirm that the person requesting revocation is the Subscriber or one of a class of persons entitled to revoke the certificate.⁴⁵

⁴⁴ The local presence that makes the registrar's role advantageous need not be geographic, although it often is. The principal requirement is that the registrar have access to accurate information about the Subscriber as needed to confirm the content of certificates. The accuracy of that information actually depends on familiarity rather than proximity, although close proximity often coincides with familiarity.

⁴⁵ Both confirmation for issuance and confirmation for revocation may be performed by the registrar, or the revocation process may be delegated to yet another role, often termed a "revocation officer." Revocation may also be handled by a person authorized not only to request revocation but also authorized to sign and give the notice that effects revocation. For example, an Issuer may

The Issuer may also delegate to the Registrar the authority to enter into a contract with the Subscriber on the Issuer's behalf, as well as in the Registrar's own right, to establish the respective obligations of Issuer, Registrar, and Subscriber. A Registrar may also perform various Subscriber-support services, such as help with software use and installation, answering telephone questions about digital signing, and similar help desk tasks.

Involvement of a Registrar having significant obligations related to issuance requires a clear delineation of responsibility between the Registrar and the certificate Issuer; however, it is not always easy for the Issuer to allocate responsibility to a Registrar effectively. A contract, Certificate Policy, or documentary certificate could state that the Issuer is not liable for functions performed by Registrars. From a Relying Party's point of view, however, it may be misleading for the Issuer to be listed as Issuer in the certificate but not be responsible for the accuracy of the certificate. A Relying Party could conclude that responsibility for certificate content is implicit in the role of Issuer, and much of the written work in the field of public key technology would give credence to that conclusion. Avoidance of the responsibility inferred from appearing as the Issuer in the certificate could be egregious if the redirection to the Registrar is not apparent from the certificate (and it almost never is), but rather is buried in a perhaps lengthy external document such as a Certificate Policy. In large-scale projects, many Registrars could be active at any given time, and ascertaining which one is responsible for a given certificate might be difficult. Moreover, if the Issuer received an electronic request from the Registrar, tracing the certificate back to that request, even if it were securely archived and preserved, might also be difficult. From a Relying Party perspective, placing critical responsibility solely on a Registrar who may be difficult to identify is inefficient at best.

Even in the case of a delegation effected by a subcontract requiring a Registrar to perform an obligation otherwise required of the Issuer, the Issuer remains secondarily responsible for the performance of the duties. In such a situation, a Relying Party could recover from either the Registrar or from the delegating Issuer, if the Registrar fails to perform as obligated. For example, suppose that Irving Issuer promises Roger Relying Party to speak the truth in Irving's certificates, and that Reginald Registrar promises Irving to provide true information for Irving to put into certificates. Reginald, however, provides false information to Irving, and Irving puts it into the certificate. Roger relies on it and sues Irving, and Irving sues Reginald. Irving is liable to Roger and Reginald to Irving. Aside from being indirect and inefficient, Irving, in effect, ends up as a sort of surety for Reginald. If Reginald cannot pay Irving, Irving must nevertheless still pay Roger.⁴⁶

If a local person is to be fully responsible for the accuracy of information in the certificate, a good alternative to the Registrar role is to use a Certificate Manufacturer. For example, if a company wishes

empower a person who also serves as a Repository to receive verifiably authenticated requests for revocation from designated persons and then effect the revocation by giving the notice in the Repository. Since both Repository services and revocation services often require every-day, round-the-clock service levels but Issuer services do not, a Repository may be in a position to provide a high level of revocation service more efficiently than the Issuer.

⁴⁶ This chain-reaction liability results from delegating an obligation that one continues to bear. Alternatively, an obligation can simply be allocated to someone else from the start, but if someone not listed as the Issuer in the certificate is obligated to perform issuance-related functions, the confusion and difficulties outlined in the previous paragraph may result.

to equip its employees with certificates, the company can have the Certificate Manufacturer generate and sign certificates in the company's name and at its request. The company would be the "Issuer" of the certificates, although the Certificate Manufacturer is doing the work of generating the certificates and signing the company's name to them. The work done by the company to have such certificates issued is much the same as the work that the company would perform if acting as a Registrar, but it provides a clearer attribution of responsibility to the company in the certificate. Because the Certificate Manufacturer is not the Issuer of the company's certificates, the risk of erroneous information in certificates is not borne jointly but solely by the company. Ultimately, if the company were serving as a Registrar, the risk would rest on the company through indemnification⁴⁷ of the Issuer, but with considerably less efficiency, as the preceding paragraph illustrates. If the company is itself the Issuer, even though it uses a Certificate Manufacturer to do the backroom data-center work, the risk of erroneous information in the certificate is borne directly and simply by the company.

The Issuer can work with Registrars, but the Issuer-Registrar arrangement can sometimes create a complicated and inefficient sharing of the responsibility for accurate certificate content, which is one of the more important aspects of certification. A certificate manufacturing arrangement may be a way of achieving a simpler and more efficient allocation of responsibility between a local, well informed, and risk-capable party and a secure provider of technological services.

C.2.2.3.2 Certificate Manufacturer

A Certificate Manufacturer provides operational services for an Issuer. The exact obligations and functions of a Certificate Manufacturer depend on the contractual arrangements between Issuer and Certificate Manufacturer, but conventionally and generally, an Issuer delegates the following obligations and functions to a Certificate Manufacturer:

- **Generate, sign, and publish certificates on request:** On receipt of a request from the Issuer, the Certificate Manufacturer creates a certificate containing the information supplied in the request. The Certificate Manufacturer then digitally signs the certificate using a private key certified as the Issuer's.⁴⁸ The Certificate Manufacturer uses a trustworthy system in performing these functions.
- **Key generation assistance:** The Certificate Manufacturer often assists the Issuer⁴⁹ in creating the Issuer's key pair that will be used to sign and verify certificates because the Certificate

⁴⁷ An Issuer may well require its registration authorities to indemnify it for providing inaccurate information or failing to perform any other duty for which the Issuer may also be held liable. The Issuer may also inquire into the creditworthiness of prospective registration authorities.

⁴⁸ The certificate manufacturer holds this private key as trustee or custodial agent of the Issuer. A legal instrument must provide for primary or trustor ownership by the Issuer and custodial possession and use, or trusteeship, by the certificate manufacturer.

⁴⁹ An Issuer's key used to sign certificates is particularly important, because uncertainty about the security of that key affects all certificates signed by that key and derivatively, all messages authenticated by reference to those certificates. The need for security in generating an Issuer's private certification key is therefore higher than the need for generating an ordinary Subscriber's private key. Since the certificate manufacturer has a secure facility but the Issuer may not, it is advisable to use the secure facility to generate the Issuer's private key.

Manufacturer has a trustworthy system, which is necessary particularly for generating a certificate-signing key. A certificate Issuer outsourcing its operations may well not have a trustworthy system.

- **Give notice of revocation:** On receipt of a request, the Certificate Manufacturer also creates notice of revocation in a prescribed form, signs the notice using the private key certified as the Issuer's, and publishes the notice into a Repository.

Generally, a Certificate Manufacturer's role in determining certificate content is entirely passive and procedural; the Certificate Manufacturer puts whatever the Issuer instructs it to into the certificates it generates. A Certificate Manufacturer typically has no obligation to anyone to confirm the accuracy of the content of the certificate or to provide customer service or revocation support directly to a Subscriber. A Certificate Manufacturer is also generally not listed anywhere in the certificate, although it could be listed in a Certificate Policy. Subscribers and Relying Parties may not and need not know that a Certificate Manufacturer produced the certificate, and the certificate generally does not indicate as much on its face.

The Issuer is listed as such in the certificates, signs them (by directing the Certificate Manufacturer to perform the signing operation), and is the principal contracting party with Subscribers and Relying Parties. The Issuer's rights and duties to Subscribers and Relying Parties, therefore, are primary and direct. The Issuer has a right of recourse against the Certificate Manufacturer for defects in generation, unauthorized signing, faulty publication, and other shortcomings in the performance of the Certificate Manufacturer's obligations.

C.2.2.3.3 Other Roles Assisting Issuers

Other roles related or complementary to the Issuer include:

- **Approver:** Within the Issuer's organization, this role has the authority to commit the Issuer to certify, revoke, or perform other critical, decisive functions. To improve the organization's control over its commitment process, multiple parties in a defined group can share this role, with a quorum and threshold defined for a commitment to be carried out.⁵⁰
- **Information source:** Large public and private databases such as company and credit reporting agencies, local governments, driver's license and tax authorities, utility companies, and similar resources can provide information about prospective Subscribers, subject to the privacy laws of the local jurisdiction and the provider's own privacy policies. Information sources external to the Issuer can greatly augment the Issuer's own (and any Registrar's) information-gathering capabilities.
- **Auditor:** Auditors, either within or independent of the Issuer, can provide important control and verification of an Issuer's systems and practices.

Other roles can be parsed out of the Issuer's functions listed above or added on alongside the Issuer to augment or reinforce its performance. From a wide-perspective vantage point in the four-cornered

⁵⁰ Certification systems with voting and threshold capabilities are often subject to intellectual property rights.

model, the Issuer role consists of serving the Subscriber by introducing reliable information about the Subscriber into the electronic-commerce information well, and removing it when it is no longer reliable. There are many ways to divide up or augment roles to that same basic end.

C.2.3 Subscriber Functions and Obligations

Subscribers are not simply passive beneficiaries of a public key infrastructure; they have critical functions and obligations. Generally, the Subscriber's obligations remain inchoate, or any harm for breach of them is reversible, until the Subscriber accepts the certificate. Acceptance is ordinarily the legal watershed that places the Subscriber's obligations in full, unconditional effect.⁵¹

The Subscriber owes duties mainly to the Issuer and to Relying Parties. The remainder of this section outlines those duties.

C.2.3.1 Subscriber-Issuer Functions and Obligations

The four-cornered model envisions a Subscriber as obligated to its Issuer to:

- **Cooperate in confirmation:** Before the Issuer can issue certificates for an account, it must have evidence sufficient to confirm the accuracy of the information to be listed in each certificate. The prospective Subscriber is often in the best position to provide much of the needed evidence, such as governmental identification documents (*e.g.* a driver's license or a passport), proof of residence, statements from co-workers, and other identifying evidence and information.
- **Request issuance of a certificate.** The Subscriber ordinarily initiates the issuance process. The Subscriber should not be placed in the position of having to refuse acceptance of a certificate issued without its request or knowledge.⁵²
- **Provide a public key** for inclusion in the certificate. The Issuer may assist the Subscriber in generating the public key, or may perform the entire key generation at the Subscriber's request, if the Issuer can do so securely. The public key must function properly in accordance with the algorithm with which it is to be used.
- **Check over the certificate and accept it,** if the information in it is correct. If the Subscriber refuses to accept a certificate because it is incorrect and it is based on information that the

⁵¹ See ABA Guidelines 1.1; Illinois Electronic Commerce Security Act §20-105; Utah Code Ann. § 46-3-304 (1996).

⁵² The requirement that the Subscriber initiate the issuance process is to preclude officious or over-eager creation and distribution of certificates that could appear effective. The danger is reminiscent of the early days of bank cards, when card Issuers mass-mailed apparently effective cards quite broadly and indiscriminately to potential cardholders. Consumers often ended up bearing the losses due to misuse of such cards, which prompted a statutory and regulatory response that would have been unnecessary, had card Issuers exercised greater self-restraint in their promotional campaigns. The situation for certificates is analogous, because an unrequested issuance and distribution of a certificate can lead to reliance unintended by the Subscriber but nevertheless causing a loss that the Subscriber could be expected to bear.

Subscriber provided, the Issuer will usually expect a reasonable explanation for the inconsistency, or the Issuer may infer a lack of credibility and call the Subscriber's account status into question.

- **Rightfully hold the private key** corresponding to the public key to be listed in the certificate. "Rightfully hold," as defined in the Utah Act,⁵³ has to do with the Subscriber's ownership or legal right to the key to be certified. The private key should not have been stolen or "borrowed" from another Subscriber.⁵⁴ An Issuer can check for rightful holding by determining whether the public key appears in another certificate extant within a defined zone of assurance (such as the content of a specified Repository). Conflicting certification of a key pair already certified to another Subscriber can lead to confusion.
- **Provide for publication, if desired** Certificates issued and accepted by the Subscriber may be published if the contract with the Subscriber so provides.⁵⁵ Publication makes the certificate available to any Relying Party who needs it,⁵⁶ and may include additional, ongoing support for the Subscriber by the Repository.
- **Respect the bounds of the community:** Often, particularly in public key projects common at this writing, certificates are intended for use only within a defined community governed by implementing contracts and a Certificate Policy. Use of certificates outside that community may expose some parties to unanticipated risks. Implementing contracts and certificate policies, therefore, generally require Subscribers to use certificates only within the confines of the community.

The functions and obligations in this brief, partial list interrelate with those of the Issuer listed in above in Section C.2.2.

C.2.3.2 Subscriber-Relying Party Functions and Obligations

A Certificate Policy often envisions Subscribers as having the following functions and obligations in relation to Relying Parties:

- **Use of digital signatures:** Ordinarily, a project's governing documents, such as its Certificate Policy, will require the Subscriber to use a digital signature on certain communications.

⁵³ See Utah Code Ann. § 46-3-103(31) (1996).

⁵⁴ Besides reuse of a key pair, perhaps without understanding the confusion that could result, key duplication could possibly occur through a defect or fluke in key generation. For example, key generation programs may not be sufficiently random in the numbers they use to create key pairs, which will increase the probability of duplicates.

⁵⁵ Some statutory contractual gap-filers (which apply if no overriding contractual provision does) provide for publication as the general rule, subject to preclusion by an express contract to the contrary. See, e.g., Utah Code Ann. § 46-3-302(2) (1996).

⁵⁶ According to common technical protocols, Relying Parties usually receive a copy of the operative certificate with the signed message from the Subscriber. The certificate, however, may become garbled in transmission or reliance on that certificate may be precluded (such as by omission of critical data such as the Subscriber's identification or the public key) in order to prevent reliance outside contractual bounds. An enrolled Relying Party can in any event obtain a complete, proper copy of the certificate from the Repository, if the certificate is published.

- **Private key safekeeping:** The likelihood of forged digital signatures (signatures that falsely appear to be attributable to the Subscriber) is quite negligible if the technology properly implements the underlying cryptography, and if the Subscriber does not lose exclusive control over the private key used to create the digital signatures. Ordinarily, a Certificate Policy or contracts between Subscriber and Relying Party or both will require the Subscriber to keep private keys secure.
- **Initiate certificate invalidation when appropriate:** Often, only the Subscriber can know when an event warrants revocation of a certificate, such as when the Subscriber has lost exclusive control of the private key or when facts stated in the certificate become inaccurate with the passage of time.⁵⁷ The Subscriber is obligated to the Relying Party to have the Issuer invalidate the certificate when the need arises.⁵⁸
- **Certificate quality and suitability:** Certificates are not all the same. Some provide greater assurance than others. A given certificate may not be suitable for a given application. The Issuer of a certificate may be someone whom the Relying Party does not trust. A Certificate Policy or Subscriber-Relying Party agreement may well require the Subscriber to have and use a certificate that reasonably fits the Relying Party's needs.

The Subscriber and Relying Party may agree on other functions and obligations as well.

These functions and obligations are between each Subscriber and Relying Party. PKI Service Providers, such as Issuers and Repositories, ordinarily have no proper role and may be intruding or meddling if they intervene in the Subscriber-Relying Party relationship. Moreover, since the Subscriber and Relying Party decide the terms of their relationship, the Issuer ordinarily does not provide assurance to Relying Parties about whether the Subscriber will use its digital signature capabilities in a manner conducive to sound reliance. For example, the Issuer does not and can not ensure that a Subscriber will adequately safeguard her private key(s). The Issuer could report about the Subscriber's capabilities for private key safekeeping, but it is not in a good position to know whether the Subscriber uses those capabilities properly.⁵⁹

⁵⁷ If inaccuracies crop up in the certificate and could mislead Relying Parties, the Subscriber should correct them. The Issuer should do so as well, but generally has no obligation to monitor the ongoing accuracy of the information in the certificate. The Issuer "speaks" in the certificate on the date when it is issued, and to a great extent, the Subscriber is thereafter in a much better position to know when information becomes inaccurate.

Once signed and issued, the contents of a certificate cannot be altered, even by its Issuer, without the alteration invalidating the digital signature on the certificate. The only way to update a certificate is to revoke it and issue a new one containing the corrected information. The Subscriber should therefore have the inaccurate certificate revoked and request issuance of a new, corrected one.

⁵⁸ The Subscriber owes the duty to request revocation to the Relying Party, but generally not to the Issuer, although the Issuer carries out that request by revoking. In other words, the *function* of revoking is carried out by the Subscriber and Issuer, but the *obligation* to revoke is owed by the Subscriber to the Relying Party (except in any cases where the Issuer should revoke without the Subscriber's consent).

⁵⁹ However, although the Issuer generally does not opine in a certificate about the safety of the Subscriber's private key(s), it may make insurance available to cover errors in private key safekeeping. That insurance may bolster a Relying Party's confidence in

C.2.4 Relying Party Functions and Obligations

Relying Parties have functions and obligations, and, as parties in the Relying Party role are particularly likely to be aggrieved when other roles err, the Relying Party's functions and obligations often work as defenses to, or limits on, the claims that a Relying Party may properly press. This section considers those Relying Party obligations and the scope of the Relying Party's rights, after considering how rules can become applicable to Relying Parties to establish their obligations and rights.

Establishing Relying Party Obligations

According to the assumptions underlying these Guidelines and explained in Section C.1.2.1, an Issuer enters into contracts with the parties relying or expected to rely on certificates from the Issuer. The purpose of those contracts (which incorporate and give legal effect to the Certificate Policy) is to define clearly the rights of Relying Parties in relation to the Issuer. Without a clear definition, those rights are governed by the rather vague and unpredictable rules about negligent misrepresentations or by other common law principles.⁶⁰ That vagueness and unpredictability would cause the Issuer to bear a potentially higher risk, incur a higher cost for risk bearing, and set higher pricing than would be necessary for clearly defined rights.

An Issuer may form implementing contracts with Relying Parties by signing written agreements (with either ink or digital signatures) or by any other means of manifesting assent in a provable manner. Section C.1.2.1.1 describes the legal requirements for contract formation in the Anglo-American tradition, and notes alternatives to paper contracts such as “clickwrap.”

The formation of a contract with a certificate Issuer can be accomplished by the Issuer itself directly, or by another person acting as the Issuer or the agent. In the four-cornered model, the Repository has direct (but perhaps only electronic) contact with Relying Parties, and Relying Parties ordinarily access the Repository, rather than the Issuer (unless the Issuer and Repository roles are performed by the same party), to check the validity of certificates and obtain other certificate support and services. Because the Issuer's contact with Relying Parties is less direct at best, the Repository may act as the Issuer's agent in contracting with Relying Parties, especially if all Relying Parties are not Subscribers and have contact with the Issuer in that role. As an alternative to agency in making the contract, the Repository can contract with Relying Parties in its own right and designate the Issuer an intended third party beneficiary. In the Anglo-American legal tradition, third party beneficiaries can enforce the contract

the safety of the private key, although it is, strictly speaking, not within the scope of the certificate as certificates are generally understood.

⁶⁰ See Froomkin, The Essential Role of Trusted Third Parties in Electronic Commerce, 75 ORE. L. REV. 49, 96-103 (1996).

For the contract to effectively preclude recourse to noncontractual rights of action, the contract must provide that suit for breach of the contract is the Relying Party's exclusive remedy, or a similar provision is necessary. Precluding the Relying Party's recourse to general legal protections may lead to consumer-protection or unconscionability issues, particularly if the contractual remedies are substantively overreaching or one-sided or if the process for making the contract tends to underinform the prospective Relying Party about important terms.

directly against the person obligated to benefit them, but in other legal systems, the contractual rights of third party beneficiaries are generally and traditionally recognized to a lesser extent.

However the Issuer enters into contracts with Relying Parties, the contracts establish the Relying Party's rights in relation to the Issuer. Contracts also establish the relative rights of the Relying Party and Repository. The Repository-Relying Party provisions could appear in the same document as the Issuer-Relying Party provisions, particularly if the Repository is acting as the Issuer's agent. Upon encountering a new Relying Party, the Repository may open an account for the new Relying Party in the Repository in order to provide ongoing, direct service to the Relying Party.

For convenience, a contract with a Relying Party should not be made every time the same Relying Party accesses a Repository but rather only once. Checking for prior contract formation (which is sometimes termed "*enrollment*") when a Relying Party connects with the Repository will make Repository usage more convenient for Relying Parties. To distinguish enrolled, prospective Relying Parties from the unenrolled, the Repository could use a shared secret. The Repository could also issue enrolled Relying Parties a simple certificate for communication with the Repository,⁶¹ unless the Relying Party already has a certificate from an Issuer within the system. The consequence of failing to determine that a Relying Party was previously enrolled is that the possibly vague, uncertain rules applicable in the absence of a contract will apply to the certificate, and that lack of clear rules will make disputes more difficult to resolve and the risks of certification less predictable.

Checking for a contractual relationship with a Relying Party also helps prevent strangers from relying on certificates without being subject to clear rules, such as the intended Certificate Policy. If a significant possibility exists (as it well might) that reliance on certificates could occur outside the contractual bounds of the project, it will be in the interest of the Issuers and other participants in the project to ensure that recipients of digital signatures backed by the system's certificates do not rely on those certificates without a contract in force to govern their relationship. The Certificate Policy and/or Issuer(s) may seek to preclude reliance on the certificates by persons who could receive them without being subject to an implementing contract. Means of precluding reliance by the unenrolled include:⁶²

- **User notice:** The Issuer may include in the certificate a conspicuous, easily-readable notice stating that a recipient of the certificate must enter into an implementing contract before attempting to rely on the certificate or exercise any rights in relation to its Issuer or Subscriber.
- **Documentary certificate:** The Issuer may include in the certificate a conspicuous, easily- readable notice stating that the meaning and significance of the certificate is specified in a documentary version available at a specified URL. The documentary certificate would indicate that the certificate is void and meaningless to persons who have not made a contract to rely on it.

⁶¹ Especially in the case of a contract formed online, this simple, relying-party certificate may well contain no confirmed identification of its Subscriber, the enrolled Relying Party. Usage of such a certificate should therefore ordinarily be confined to the issuing Repository, and its reliance on such a low-grade certificate should be appropriately limited. Relying Parties contracting with the Repository online could be invited to apply for more reliable certificates from a system Issuer.

⁶² This list is drawn from an e-mail by Dwight Arthur to the NACHA CARAT group dated July 21, 1998.

- **Subscriber requirements:** The Certificate Policy or implementing contracts may require Subscribers to refrain from sending certificates to persons outside the boundaries of the contractually-obligated community.
- **Repository checking:** When a prospective Relying Party contacts a participating Repository to ascertain the current validity of the certificate, the Repository can identify the Relying Party by means such as a shared secret and determine whether a prospective Relying Party is enrolled before permitting the prospective Relying Party to proceed.⁶³
- **Encryption in the certificate:** The Issuer may encrypt critical information, such as the Subscriber's public key, in the certificate.⁶⁴
- **Certificate tokens:** The Issuer may omit critical information, such as the Subscriber's public key, in what would otherwise be a certificate, and issue that partial certificate to the Subscriber. A transactional certificate issued in response to the prospective Relying Party's online request could supply the needed information.
- **Pseudonymous certificates:** The Issuer may omit information identifying the Subscriber from the certificate, except for a reference to an identifier that only the Issuer can interpret. The significance of the identifier could be interpreted by the Issuer in response to a request.⁶⁵
- **Incorporation by reference:** The certificate may refer Relying Parties to a Certificate Policy, certification practice statement, or other external document that requires contractual enrollment as a prerequisite to reliance on the certificate.⁶⁶
- **Critical policy field:** The certificate may indicate by a standardized, binary flag that the field referencing the Certificate Policy is "critical," and could thereby perhaps imply that compliance with the policy is mandatory, including its requirement to enter into implementing contracts.⁶⁷

⁶³ This method assumes that a certificate recipient checks the Repository. While checking for revocation is highly advisable, it is far from certain that all Relying Parties will invariably check before relying. However, the system can force a check by omitting critical information, such as the Subscriber's public key, from the certificate. See the certificate token option.

⁶⁴ Encryption within the certificate and algorithms for validation of certificates containing such encryption is the subject of intellectual property claims.

⁶⁵ Once released, the dissemination of the interpretation may prove difficult to control. This method is similar to the omission of critical information and may also be the subject of intellectual property claims.

⁶⁶ Incorporating an external document can fail if the reference is not clear, the authenticity of the referenced document is lacking or uncertain, or if the intent to incorporate (which is distinct from the intent merely to cite) is not clear from the reference. Simply referencing a certificate policy by an object identifier in the certificate may well fall short in both the adequacy of the reference and the expression of an intention to incorporate. An object identifier is nothing more than a unique series of numbers, and its association with a particular document exists apart from those numbers and can be unreliable or obscure. An object identifier is thus not a reference but rather a means of disambiguating references. Moreover, simply listing an object identifier in a field can be interpreted in many ways other than as effecting an incorporation.

⁶⁷ It is by no means certain that recipients of a certificate will infer that the certificate policy is mandatory from the fact that a policy field is marked "critical," and even if such an inference is drawn, binding legal effect requires more than an assertion that a

- **Non-circulation of certificate information:** Particularly where the Relying Party and Subscriber are the same person, system may forego issuing certificates and instead keep the information that a certificate would contain within a secure, limited-access database or directory.

As noted, some of these methods of precluding reliance by unintended Relying Parties are more effective than others. Indeed, some may have so little effect as to be not worth the effort.

C.2.4.2 Relying Party-Issuer Functions and Obligations

As described above in Section C.2.2.2, the Issuer provides certain assurance to Relying Parties in the form of a certificate. The usage of, and reliance on, certificates is limited by obligations required of the Relying Party in an implementing contract, in the Certificate Policy, and perhaps also by general laws governing reliance on certificates, specifically or factual representations, generally.

Pursuant to contracts with the Issuer, Relying Parties promise to:

- **Rely within limits:** Assured reliance on certificates issued by the Issuer is limited by beginning and end dates (`validity:notBefore` and `validity:notAfter`), revocation,⁶⁸ reliance limits⁶⁹ (a monetary amount per transaction or a time period), and other provisions limiting the certificate's assurance level. Validity may also be limited to one specified digital signature (a "transactional certificate"⁷⁰) or in other ways, depending on the Relying Party's needs. In addition, the Relying Party must also take into account notice of other facts or considerations affecting the basis for reliance; in other words, the Relying Party must rely reasonably and justifiably. (All of these limits on reliability are subject to rejection or negotiation. A person is generally not obligated to rely if the limits imposed are unacceptable.⁷¹)
- **Rely on the meaning ascribed to the certificate:** The terse, standardized form prescribed for public key certificates lacks the capability to express clearly and precisely what a certificate means.

counterparty is bound. Furthermore, implications drawn from the critical flag depend on technical parsing and on familiarity with the interpretation specified in the current version of ITU X.509, which may be too abstruse for consumers or non-technologists.

⁶⁸ Since the party would rely at its peril if the certificate is revoked or suspended, the party would need to check the Repository listed in the certificate for notice of revocation. Often, a Relying Party is not under a contractual obligation requiring it to check for revocation, but rather, it relies at its peril in relying on a revoked certificate.

⁶⁹ Utah Code Ann. § 46-3-309(1) (1996) (significance of recommended reliance limit).

⁷⁰ See, e.g., Utah Code Ann. § 46-3-103(36) (1996) ("A transactional certificate means a valid certificate incorporating by reference one or more digital signatures."); § 46-3-103(38) ("...a transactional certificate is a valid certificate only in relation to the digital signature incorporated in it by reference").

⁷¹ Besides referring an unacceptably signed message back to the Subscriber, the Relying Party could inquire through the Repository whether additional assurance or another certificate is available for the Subscriber's account. If the Issuer-Subscriber and Issuer-Repository contracts permit, the Repository can forward to the Relying Party a higher-assurance, already-issued certificate on file in the Repository so that the Relying Party can rely more appropriately on the Subscriber's digital signature. Issuance of a new certificate for this purpose is the subject of intellectual property rights and may accordingly be restricted.

The Issuer can use an online, Web-based process referenced by a URL in a certificate to decode and to interpret the certificate into a pre-defined documentary form. The Relying Party must, therefore, rely only on the meaning given the certificate in its documentary form.

- **Confidentiality and information retention:** The Repository and the Issuer may retain information indicating that the Relying Party has been enrolled and providing some background data about the Relying Party (such as name, billing address, etc.). This information should generally be kept confidential.
- **Claims and dispute resolution:** A Relying Party may agree that all disputes or allegations of loss arising from a certificate must be resolved through a procedure of filing, adjusting, settling, and arbitrating written claims. Further, an implementing contract or Certificate Policy may require that claims be filed before a deadline specified in the certificate (usually a time extending for a specified amount of time after the validity:notAfter date⁷²). The contract or policy could bar a claim (make it thereafter unenforceable) after that deadline.⁷³

A specific implementation may include other functions and obligations as well.

C.2.4.3 Relying Party-Subscriber Functions and Obligations

The Relying Party is ordinarily obligated to the Subscriber to rely on the certificate within its established limits and in accordance with its meaning. Further, the Relying Party has a general duty to rely reasonably and to take into account any material information in addition to the certificate of which the Relying Party has notice. In particular, the Relying Party should be bound by any notice given, including notice by publication in a designated Repository, concerning the validity of the certificate at the time of reliance.

As in the case of Subscriber duties to Relying Parties, the obligations of Relying Parties to Subscribers are not ordinarily within the purview of an Issuer.

C.2.4.4 Relying Party-Repository Functions and Obligations

The Relying Party is a user of both the Repository's online information and the technology for delivering it. The Relying Party, therefore, owes the Repository a duty to observe the Repository's security rules, pay according to a fee schedule, and perform similar obligations of online service users.

⁷² Note that the validity period of the certificate (as specified in the validity field) is the period during which reliance may occur, and that period is not the same as the period during which claims may be filed.

⁷³ For purposes of risk management, the certificate is risk-neutral from the claims bar date on, by analogy to a claims-made insurance policy. *See, e.g.*, National Union Fire Ins. Co. v. Talcott, 931 F.2d 166 (1st Cir. 1991); Brumfield v. Shelton, 831 F. Supp. 562 (E.D. La. 1993); Gilliam v. American Cas. Co., 735 F. Supp. 345 (N.D. Cal. 1990) (applying a payout cap based on the timing of the claim rather than of the loss-causing occurrence).

C.2.5 Repository Functions and Obligations

A Repository is an online source of up-to-date information about certificates, their current reliability, related network infrastructure, legal obligations, and other information helpful for secure electronic commerce. Generally, the value of an information resource like a Repository increases according to the amount of information available in it and the service levels for providing that information. Repositories in a mature public key infrastructure, therefore, may well be large, central, and continually operated stores of online information about certificates and electronic commerce. A defining characteristic of Repositories in the four-cornered model is that they are oriented mainly toward the reliance process; in other words, a Repository's principal customer is the Relying Party.

C.2.5.1 Repository-Relying Party Functions and Obligations

The Relying Party is the focal point of the value to be received through public key certification because Relying Party bears the risk of authentication failures. Legally, a forgery is generally treated as ineffective as the purported signer's signature unless the signer was negligent in enabling the forgery or otherwise at fault. Since a loss due to forgery falls on the Relying Party at first, and perhaps also at last, the assurance of authenticity that public key technology benefits most immediately and greatly the Relying Party. Many public key business models, however, tend to under serve the Relying Party even though the Relying Party has the greatest customer potential because it can realize the greatest benefits from public key technology.

A Repository is obligated to Relying Parties to provide its available information in an accurate and timely manner. A Repository, however, generally does not have a duty to confirm the accuracy of the information it provides. This is particularly true if the information is provided as a certificate, notice of revocation, or other document issued by someone else. In other words, where the Repository acts simply as a conduit for records provided and signed by others, the Repository is not responsible for its accuracy, unless its implementing contracts may provide otherwise.

C.2.5.2 Repository-Subscriber Functions and Obligations

Although the Subscriber is for the most part a customer of the Issuer, a Repository may also have obligations to the Subscriber, obligations that it may provide through the Issuer, who maintains the principal customer relationship with the Subscriber in the four-cornered model. The possibilities for Repository-Subscriber services have not been extensively explored, but two of the more commonly suggested are (1) to protect Subscribers' privacy and (2) to provide account statements to them.

C.2.5.2.1 Privacy and Other Information Rights

Subscribers are the persons about whom information is published in a Repository, which is a generally available, online information resource. The Repository, therefore, may have an obligation to safeguard the Subscriber's rights of privacy, confidentiality, and information accuracy, if implementing contracts, an applicable Certificate Policy, or other laws provide for such rights.

For the most part, statutes in legal systems other than those of the United States require large databases holding information about many members of the public to restrict access to, or the visibility of, information that can be related to a specific individual. To some extent, a Subscriber's rights under such a statute (often termed a "data protection statute") may be the subject of an overriding agreement or a waiver. In some legal systems, however, data protection statutes may impose certain requirements for agreements or waivers, or may otherwise protect the Subscriber's privacy from being given away too lightly.

Aside from legal rules, privacy may simply be a customer need or desire that a Subscriber may be willing to pay for. In banking, for instance, confidentiality and discretion in disclosing customer information are often highly valued and may be prerequisites to doing business.

Where access to, or visibility of, information about the Subscriber is limited, the limitations generally remain subject to law enforcement and administrative searches and seizures, although most legal systems require a process and/or sufficient cause to justify the search and seizure.

C.2.5.2.2 Account Statements

Banks traditionally report account activity to customers to aid in discovering errors or fraud. Account statements to Subscribers can similarly be useful for certification accounts. For example, if the Subscriber's private key has been compromised, the Subscriber may not be aware of the problem—indeed, a smart thief, intent on forging signatures, will endeavor to escape detection. If forged signatures with the stolen key turn up on the Subscriber's account statement, however, the Subscriber can discover the compromise and take corrective action.

Account statements can also help in determining whether the Issuer, Repository, or others are properly carrying out agreed-upon confidentiality and privacy restrictions.

Technology can help greatly in processing account statements and reconciling signatures made with the reliance on them.

C.2.5.3 Repository-Issuer Functions and Obligations

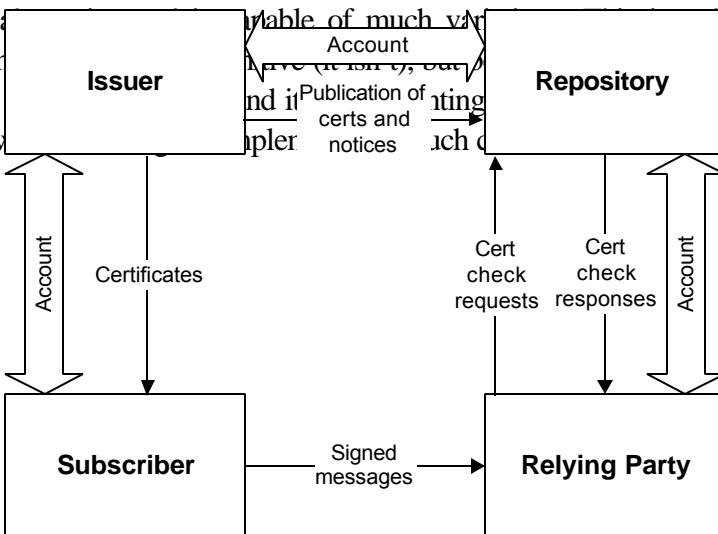
A Repository and an Issuer it serves will generally agree on the terms and conditions governing publication by the Issuer of information (such as certificates and notices of revocation) into the Repository. A Repository is obligated to perform according to that agreement.

The agreement may also provide for other services by the Repository to Issuers besides publication. For example, as noted in Section C.2.4.1 above, a Repository can assist Issuers in making contracts with prospective Relying Parties.

C.2.6 Conclusion on Four-Cornered Model

The four-cornered model, as diagrammed below, basically allocates roles according to customer relationships and interactions.

This model is only one of many possible models for a certificate system. The CARAT Guidelines examines it—rather than the others—in some detail because it is representative of the design work underlying a number of existing systems. The next section considers how this model can be extended to support a wider range of requirements.



PART D. IMPLEMENTING A BUSINESS AND LEGAL MODEL

D.1 Tailoring Certificate Policy to Reflect and Support Underlying Business and Legal Conditions

The first step in writing a Certificate Policy should be assessing the requirements of the underlying business model. The initial allocation of functions to roles, and roles to parties will depend upon an assessment of the business conditions. Such an assessment will define the parties that will be available to accept roles. It is likely that the transactional needs of the system will dictate that a particular party plays a particular role or function. This is especially true for Subscriber and Relying Party roles. In a public sector bidding system, for example, the Subscriber might be a given set of private sector vendors who submit bids, and the Relying Party might be limited to a particular agency of a particular state government.

Similarly, the role of Registrar and even Repository might be naturally allocated to a given party for a given business system. If, for example, it is known that a particular party will have to identify and authenticate a set of people who would fill the role of "Subscriber" in a PKI, then the drafter must consider whether that party would be capable of performing the functions of the Registrar. If this party had some reason why such functions would not be delegated, then unwillingness or inability to act as a Registrar would significantly complicate the drafting of a policy. Conversely, a party may be rendered unfit to perform as a Registrar due to such business or legal conditions as restrictive union contracts, limited technical ability to securely communicate with the Issuer, or unwillingness to use a different Certificate Manufacturer. This last could occur, for example, with a party that has an exclusive arrangement with one or more sub-standard Certificate Manufacturers.

Depending upon the transactions and other factors, however, there may be some latitude available in matching a given role or function to any of several parties. In many cases, it is probable that one or more of the PKI Service Providers roles (Certificate Manufacturer, Registrar, Repository and Issuer) will be "up for grabs" and available for a third party vendor to perform. In such a case, the four-cornered model of PKI relationships can be an efficient way to allocate roles. It is also likely that the underlying business conditions will suggest refinements and modifications of the roles and functions in novel ways. A secure Certificate Manufacturer or Repository may be capable of providing more cost effective service than would be possible by any of the parties to a business system and might, therefore, make a sensible outsourcing partner.

On the other hand, there are any number of underlying business and legal conditions that might suggest maintaining the Repository role "in-house." For example, an organization might be able to avail itself of an existing infrastructure. Any given system may be best served by existing directory servers that are integrated into the applications and existing business practices of some parties who seek to create a PKI and Certificate Policy. This could be the case within a large organization that has implemented an X.500 server that all relevant parties already tie into for E-mail and other network services. There may also be legal or policy reasons, which are not infrastructure-related, that make outsourcing the Repository role undesirable. For example, the information to be placed in the certificates may be

deemed too sensitive to permit a third party Repository to see (for privacy reasons), or a third party Repository might be unwilling to agree not to compile and sell names or other transactional data. Any number of underlying business reasons may cause a decision not to outsource the Repository role. However, as noted in the review of the four-cornered model and elsewhere in these Guidelines, as between two initiating End Entities who intend to be Subscribers and Relying Parties, a review of business conditions for their intended system might indicate that outsourcing of all PKI Service Provider roles and functions is desired.

D.1.1 Parties and Transactions Together Define the Underlying Business Structure

Together, parties and transactions define the underlying business structure enabled by PKI. Examples of underlying business structures might include:

	Party Relationship	Example Transaction Types	
1.	Business to Government	public procurement	regulatory interaction
2.	Business to Business	supply chain	joint projects
3.	Government to Government	sensitive information sharing	reporting requirements
4.	Employees and Contractors to Employer	human resources	payroll management
5.	Prospective and Current Consumers to Business	account creation	account usage
6.	Licensed Professionals and Other Citizens to Government	submittal of filings	requests for information
7.	Students and Faculty to Staff	course registration	grading

Policy Authorities cannot ignore legal and regulatory conditions that apply to parties and transactions in the paper-based world when implementing an electronic business and legal model.,

D.1.1.1 Legal and Regulatory Conditions Related to Certain Parties

In example one (1), above, contracting with a government can raise special issues that bear upon obligations in a PKI environment. In a government environment, parties must be aware of the following:

- **Sovereign immunity** shielding a government from certain sources of liability. Irrespective of the terms of any Certificate Policy, government parties come to the negotiation table with certain liability characteristics that are not typical of private sector parties.
- **Public records laws** that can severely restrict the confidentiality of transactional data. (In some jurisdictions, even the contract to provide PKI services to a government entity must be a public record. Consequently, PKI providers cannot maintain confidential liability terms among government clients.)
- **Limitations on business partners** may restrict or regulate the parties with whom government may transact. Examples include (a) requirements to contract with small, local, or minority owned businesses, and (b) moratoria against contracting with businesses in certain countries.

In addition, any party might prefer to contract only with certain other parties or may have special requirements governing the type and manner of transactions into which it will enter. These preferences and requirements might be based upon external pressures, such compliance with the terms of loans or grants, or upon internal pressures, such as agreements with organized labor or long-standing operational procedures.

D.1.1.2 Legal and Regulatory Conditions Related to Certain Transactions

In example five (5), above, in the securities context or the banking context, certain notice requirements and other regulatory issues may create special circumstances that would affect the latitude available to a Certificate Policy drafter. The obligations of PKI Service Providers or others to disclose materials, to keep records private, or to honor or dishonor a given signature (whether digital or not) may affect the duties of all parties with respect to usage of any particular communications system, including a PKI.

D.2 The Role of the Certificate Policy in the Context of the Business Environment

The Certificate Policy can be used for any number of purposes, as detailed above. Legally, one of the most important and complex uses of a Certificate Policy is as a set of operating rules. To use a Certificate Policy as enforceable operating rules, parties would have to sign "implementing contracts" as discussed elsewhere in this document. Other documents and sources of obligation, such as public law, licenses and conduct that could give rise to common law causes of action in tort, would also bear upon the efficacy of the Certificate Policy. For these reasons, one may not be able to glean all of the relevant rights, obligations and roles of parties merely by reading a Certificate Policy, or any given set of documents.

D.2.1 Sources of Power or Sources of Authority Underlying Certificate Policy Making Process

The range of factors and related documents that are relevant to the relationships detailed in a Certificate Policy will depend in large part upon the source of power or authority by which the Policy Authority

promulgated the policy. As described above, a vital initial issue to be determined prior to the drafting of any particular Certificate Policy is the identity of the parties, especially the stakeholders and in particular, the Policy Authority. This section offers examples of how the identity of the Policy Authority can radically affect the underlying business conditions related to a given PKI. The content and scope of a Certificate Policy will necessarily change, perhaps radically, depending on the status of the Policy Authority. A threshold question is: by what right does the Policy Authority promulgate a Certificate Policy? To indicate that a Certificate Policy may become legally enforceable based upon contract is too facile an answer. The basic question remains: why will parties who would be subject to a Certificate Policy agree to be bound by a contract? As discussed below, a Policy Authority's sources of power and authority will materially shape a Certificate Policy.

D.2.1.1 Power Based on Position in Private Market

An organization with great power in a private market might be capable of becoming a Policy Authority based on its position in the market. This might be the case with a very high-value purchaser who supports a large supply chain, or with a network service provider with a large base of users in an inelastic market.

D.2.1.2 Authority Based on Provisions in Public Law

Other organizations might have great power based on grants in public law. This might be the case in a jurisdiction that has enacted a law empowering a particular governance body to create policy on a certain matter (as with the California Law Enforcement Telecommunications System (CLETS)⁷⁴) or a law entitling a government body to license a PKI Service Provider (as with the Utah Department of Commerce which promulgated detailed regulations governing licensure of Certificate Authorities and Repositories).

D.2.1.3 Agreement Based on Consent of the Parties

Other membership organizations might gain power based on consent and private contract among interested parties. This might be the case among parties who choose to set up or join a representative non-profit council to draft and issue Operating Rules, which the parties would voluntarily agree to follow by contract (as with the Electronic Benefits Council of NACHA). A key element of this source of authority is the 'fact of agreement' as the basis of enforceability. Unlike a system prescribed by public law and implemented through contracts with parties who may have little or no choice but to comply, a truly private system that is based on agreement can be amended or abandoned by the parties. Although power to change the rules could be a source of instability, it is also a significant strength of these

⁷⁴ The CLETS system was created by the California legislature through enactment of a statute. The statute designates a governing body, and that body drafts contracts which bind other parties who seek to gain access to the criminal justice information contained within the CLETS system. For more information (including the governance structure and downloadable copies of the major implementing contracts) see: [<http://caag.state.ca.us/cas/ppp/ppp.htm>].

systems. The ability for parties to adapt to changing business, legal, and other relevant conditions within a responsive and agile governance structure can be critical for the success of a system in the fast-changing electronic commerce markets. On the other hand, Certificate Policies based upon power or authority, absent discussion among the parties can be insulated from the reality of rapid change in the short-term and therefore are vulnerable to becoming obsolete in the long-term.

D.2.2 Order of Precedence of the Certificate Policy vis-à-vis Other Documents

Depending upon the source of authority underlying the process of drafting or otherwise selecting a Certificate Policy and other business and legal conditions, additional documents will either control, or be controlled by, that named policy. Documents that have a higher order of precedence for purposes of interpreting other documents are said to be "controlling." Documents that are governed by other documents are "controlled" or "subordinate" to the higher documents. In some cases, documents seem neither to govern nor to be governed by other documents. Such "peer level" documents are usually not a problem, unless the documents are binding on the same parties and provide inconsistent or conflicting obligations. Structuring the governance model of a PKI will involve a careful investigation of all related documents. When necessary, measures will have to be taken to clarify the order of precedence of each related document.

D.2.2.1 Higher Level "Controlling" Documents

Any of the following documents could exist at a higher level than does the Certificate Policy and could govern the terms of the Certificate Policy:

- **Constitution and Statutes** of the jurisdiction or jurisdictions in which the Certificate Policy will be effective, or may be litigated, or otherwise interpreted
- **Court Orders** that are in effect and that govern the subject matter or parties
- **Public Administrative Regulations** that directly affect the subject matter or parties
- **Charter and Bylaws** of the organization in question
- **Higher Policies** to which the organization has afforded a controlling status
- **Important Contracts** that are difficult or impossible to change materially at the time in question;

D.2.2.2 Lower Level "Subordinate" Documents

Any of the following documents could exist at a lower level than does the Certificate Policy and be governed by the terms of the Certificate Policy:

Lower Policies that the organization has ranked below the Certificate Policy

Implementing Contracts that are created pursuant to the terms of the Certificate Policy

Sub-Contracts that are entered into by any of the parties for the purpose of delegating functions assigned to them under the Certificate Policy

Memoranda of Agreement and Memoranda of Understanding crafted to assist the parties

D.2.2.3 Peer Level Documents

Sometimes the Certificate Policy will compete for precedence with other documents that are neither clearly governing nor governed by the Certificate Policy. Such documents might include any of the following:

- **Other Certificate Policies** that have been agreed upon by a party to the present Certificate Policy
- **Documented Practices** of a party to the Certificate Policy
- **Related Contracts** entered into by a party to the Certificate Policy
- **Existing Employment Agreements** binding upon a party to the Certificate Policy

Similarly, service level guarantees from Internet providers and software licenses with warranties of fitness for a particular purpose may create ambiguous situations, where the expectations of the parties may be different in the event of a dispute involving a Certificate Policy. Often the parties to these types of documents may include both a party that is allocated responsibilities under the Certificate Policy and one or more non-parties to the Certificate Policy that plays a role in the business structure (e.g., Internet service providers, software developers and sellers, or private standards bodies). A Policy Authority has a duty to be diligent in ensuring that the Certificate Policy is realistically scoped. The expectations of the parties would be frustrated by promulgation of a Certificate Policy that purports to govern rights and obligations of parties but that is in fact going to be over-ridden by other documents with different terms and leading to different outcomes. Because the range of issues addressed within the PKIX Framework is so broad, a Policy Authority would be prudent to seek the advice of knowledgeable counsel as part of the policy-setting process.

D.2.3 Analogous Contractually-Based Governance Structures

D.2.3.1 Several Analogous Structures Exist

There are several examples of governance structures that depend upon parties to opt in by contract. These systems usually avail themselves of a single higher level document that is referenced by the contracts signed by each party. For example, the Electronic Benefits Council of the National Automated Clearing House Association uses a higher-level document known as "operating rules" that are referenced by contracts. The fact that a party signs a contract in order to participate in a system does not necessarily mean that the system is governed entirely, or even predominantly, by private law or is subject to changing agreement by the contracting parties. For example, the VISA system (discussed below) requires that each party sign a contract, but critical liability provisions and other terms are directly specified by public law. Similarly, the CLETS example described above is founded upon a

statute enacted by the California legislature, but each party must nonetheless sign a contract to participate in the network. Other systems, such as the program stock trading networks and the multilateral network peering agreements for Internet service providers, provide more variations on the theme. In sum, several examples of governance structures based upon contracts exist in the marketplace today.

D.2.3.2 Mini-Study: The VISA Model

Visa is a membership association of approximately 21,000 financial institutions in 250+ countries and territories worldwide. An International Board of Directors governs the association. Members belong to geographic regions , each with its own Board that reports to the International Board. The payment system supports: 600+ million Visa cards, 14+ million merchant locations, and 400+ thousand ATMs.

Membership categories, rights, and obligations are spelled out in the by-laws. Several categories of membership are available, depending on the type of activity the Member wishes to engage in (issuing cards, acquiring tax from merchants, etc.).

Large Members may sponsor smaller Members, and assume certain responsibilities for the financial performance of their sponsored Members. Members also sponsor (and assume certain liabilities for) processors, third party servicers, or other agents that support their businesses.

Visa owns proprietary payment system brands/marks (Visa, Plus, Interlink, Electron) and runs the Visa payment system (i.e., clears and settles Visa-branded transactions among Members). A key component of the payment system is a comprehensive set of Operating Regulations that define how the brands are to be used and how transactions are to be processed by all parties. Members must agree to abide by Operating Regulations as a condition of their Membership. A formal dispute resolution process is also a part of the Operating Regulations.

Members sign contracts (“agreements”) with consumers and merchants that govern how Visa transactions will be processed among these parties. By extension, these agreements also imply or specify adherence to the processing rules that apply between Visa and its Members. Certain standard contents of these agreements are specified in the Operating Regulations. In addition, Members are free to add more provisions of their own— especially regarding fees, pricing, etc.—as long as those provisions do not conflict with Visa policy or regulations, or with any applicable legislation or regulation from a local governmental agency. This freedom of agreement format is required for the system to work effectively in the 250+ worldwide jurisdictions and thousands of local sub-jurisdictions in which these agreements are concluded.

A key point is that Visa does not have any direct contract or relationship with consumers or merchants. Operating Regulations bind Members and Visa, but not Visa and end users of the payment system. For example, Operating Regulations may allocate liability for fraud losses according to certain rules regarding how the transaction was authorized, whether a signature was obtained, the form of the signature, etc. But this loss allocation is shared between Members; separate rules govern how much loss a cardholder or Merchant will bear in any given situation, and these rules often incorporate various

forms of protective legislation (including, e.g., Reg Z and Reg E) which are required to be incorporated (either explicitly or implicitly) in the Members' agreements with merchants and consumers.

Visa may also establish policies for consumer protection in its own Operating Regulations (e.g., limiting debit cardholder liability to \$0 if a fraud or card loss is reported within two days). These policies are binding on Members, however, and Visa will sanction a Member if the policies are not followed.

Another key part of the Membership arrangement is Visa's role in managing risks of the payment system. Visa constantly evaluates Member soundness and the quality of Member programs. Visa may impose a variety of sanctions, including shutting down a Member's Visa programs or revoking membership, if the offending Member's activity is deemed to be a danger to the overall payment system, the brand, or other Members.

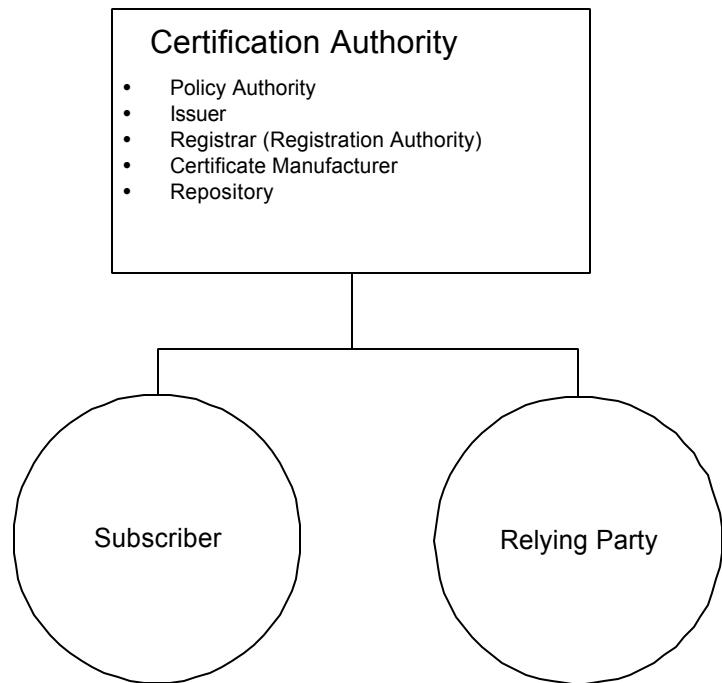
D.2.4 The Relationship of PKI Models to the Certificate Policy Implementation

D.2.4.1 Underlying Business Conditions and Allocation of PKI Functions to Roles

Not all business models mix and match roles in the same way. A number of other possible models exist in addition to the Four-Cornered model detailed in Part C of these Guidelines. It is premature to suggest that any particular model predominates in the market or is generally recommended at this time. This section explores the implementation issues surrounding the drafting of a Certificate Policy using various PKI models. In any model, a Policy Authority, PKI Service Providers and End Entities exist. Depending on business conditions, there is latitude in assigning functions to roles and roles to parties.

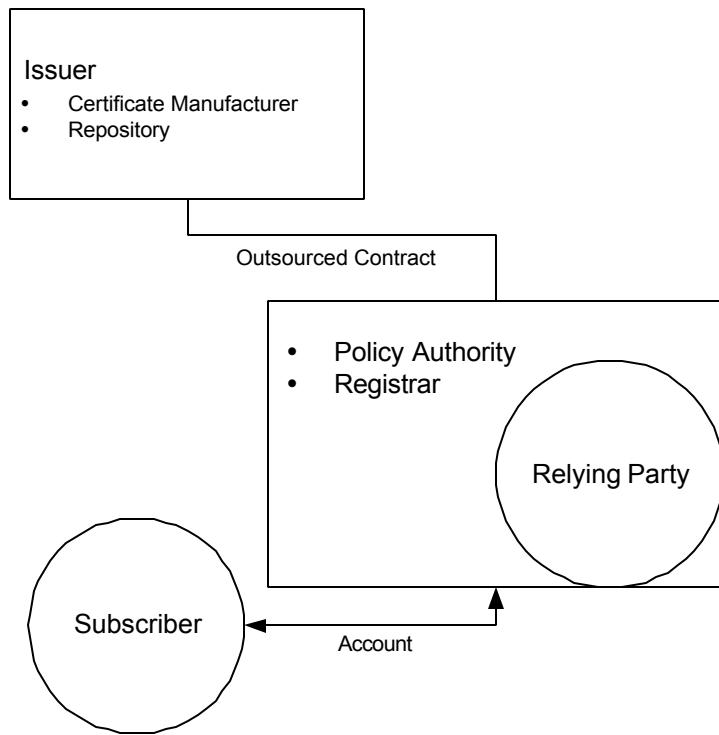
The following diagrams and examples illustrate some of the possible configurations.

Certification Authority Model



The Certification Authority Model is usually associated with “Open PKI.” In Open PKI, it is envisioned that Subscribers will hold one or more certificates of varying classes, and that a Relying Party may accept Subscriber certificates of a suitable class for any transaction. Conceptually, Open PKI has the potential to support an infinite number of transactions with relatively few certificates per Subscriber. At the same time, however, it is difficult to manage or limit the risk of liability in an Open PKI because a certificate could be used for countless types and numbers of transactions. Most PKI Service Providers are not willing to open themselves to unlimited or uncontrollable liability. Furthermore, it may be difficult for a Certificate Policy that generically defines a “class” of certificates to contemplate ancillary business and regulatory considerations that affect the parties and the transactions enabled by PKI.

Relying Party Model



The Relying Party model is a conceptual model based on the Federal Model Certificate Policy Draft (March 25, 1998) and on pilot projects underway at the state government level.⁷⁵

The Federal Model Policy envisions a Certificate Policy as being defined by a Relying Party, an industry association, or a group of entities to specify the level of trust that must be met by certificates used for a *particular transaction*.⁷⁶ The Federal Model Policy envisions a model that more closely resembles a “Closed PKI.” In a Closed PKI, a Subscriber usually possesses one certificate that it uses for one type of transaction with a known Relying Party. Under the Federal Model Policy, the Relying Party plays a central role because it is not only the principal Relying Party, but it also acts as Policy Authority and a Registrar.

In a live PKI pilot project resembling the above diagram, PKI Service Provider roles were allocated to parties in the following manner:

- Private Company A and Bank B are Issuers
- Private Company A created a root key for Bank B in its “hardened facility.”
- Private Company A manufactures certificates on behalf of Bank B using Bank B’s root key. Bank B’s certificates are then issued to Subscribers of Government Agency C.

⁷⁵ At least two live State pilot projects utilize this general model.

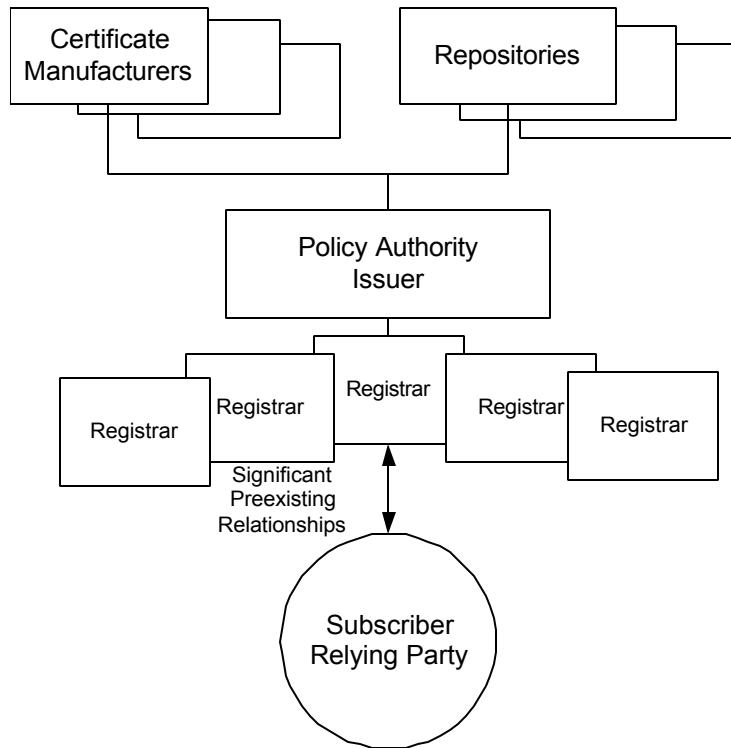
⁷⁶ Federal Model Certificate Policy Discussion Draft (March 25, 1998), page 6.

- It is unclear whether any party performs Repository services.
- Government Agency C, State Administrative Agency D, and State Administrative Agency E (under which the pilot was created) constitute Policy Authority.
- Government Agency C is the Registrar (Registration Authority). Two individuals at Government Agency C perform the Registrar role personally manually using existing Government Agency C's records and callback and fax procedures.
- A Division of Government Agency C is the Relying Party
- The Division of Government Agency C has its own certificate with which it signs receipts. As a result, the Division is also a Subscriber , although this status is not shown in the diagram above.
- Private companies from around the country that do business in-state are Subscribers. Subscribers must file and renew their licenses annually and must pay fees and taxes semi-annually.

Note that in the above diagram, the party performing the role of Issuer, the party that, at the least, places its name in the Issuer field of a certificate, could be performed by Government Agency C.⁷⁷ (For a more detailed discussion of issues to consider in assigning the role of Issuer to a party or Issuer to a government entity, see Part C and Part B, respectively.)

⁷⁷ Another alternative would have been for Private Company A, Bank B, or the Government Agency C to place their names in the Issuer field of the certificate. This co-branding of a certificate may result in additional liability for any one of the parties listed in the certificate but it may also give the certificate more legitimacy or provide marketing benefits. Yet another alternative would be the formation, among the parties, of a joint venture, partnership, or other legal entity that would place its name in the Issuer field of the certificate.

Electronic Court Filing Model



The Electronic Court Filing Model is a hypothetical model that could be applicable in any U.S. State where parties would perform the following roles:

- The Policy Authority and the Issuer would be either a State Bar or a legal entity made up of a members from a State Bar, Court Clerk Associations, State Supreme Court, Federal Courts, and Administrative Office of the Courts (or like entities).
- Certificate Manufacturers and Repositories would be private companies performing Certificate Manufacturer and Repository services. Certificate Manufacturers and Repositories would operate in a particular state if accredited by the Policy Authority or by a means defined in the Certificate Policy. To prevent monopoly and ensure interoperability, the Certificate Policy, or a technical document incorporated by reference in the Certificate Policy, would define a set of technical standards to be followed by Certificate Manufacturers and Repositories to sell PKI services to members of the State Bar or Court Administrators.

- Registrars would be court clerks located anywhere in a state, at State Bar offices or at any other 'bricks and mortar' establishments where attorneys and judges have a significant pre-existing relationship.
- Subscribers and Relying Parties would be lawyers, judges, and court administrators. Subscribers would have one certificate that would be issued by the Policy Authority, but which could be manufactured by any one of several Certificate Manufacturers that operate under a statewide Electronic Court Filing Certificate Policy.

Many other role allocations and business models, besides those listed above, are likely to evolve.

D.3 Determining Whether and How to Draft a Certificate Policy

According to the IETF PKIX Framework (see Part E.), a Certificate Policy may serve the following purposes:

- Provide a human-readable, named policy that may be used by a certificate user to decide whether or not to trust a certificate for a particular purpose;
- Generate a policy that can be recognized by both the user and the Issuer of a certificate Under these Guidelines, the parties would include the Certificate Manufacturer, the Registrar, the Issuer, and the Repository; and users would include the Subscriber and the Relying Party, which would all recognize the policy;
- Simplify comparison between two certificate policies during cross-certification among certificates issued under different policies;
- Create a benchmark for comparison between the policy and the documented practices of a PKI Service Provider to ensure that the provider's practices faithfully implement the policy;
- Constitute a basis for accreditation of a PKI Service Provider by providing a policy against which the provider's practices can be accredited.

A Certificate Policy can assist an organization in the pursuit of the above purposes. In addition, the PKIX Framework provides a valuable and comprehensive check-list for policy makers, managers, attorneys, technologists, and others to use when evaluating an actual or proposed implementation of certificate-based PKI. A review of the issues presented in the PKIX Framework can help an organization determine whether a Certificate Policy is needed or helpful in the context of its current or contemplated usage of certificates. These Guidelines recommends using the PKIX Framework as a starting point for policy development largely because the need for interoperability among users of secure or authenticated electronic records and signatures. Such interoperability is not only needed at the strictly technical level, but also at the policy level.

Indeed, interoperability among policy documents is of vital importance in the fast-paced electronic commerce business environment. Although many parties and transaction types may never overlap, it is anticipated that organizations will be able to realize economic efficiencies or quality enhancements by

easily communicating securely and with authentication among a wide array of new parties. Electronic commerce, as part of the emerging information economy, is pushing organizations to form numerous and quickly shifting alliances with a growing array of other organizations. New markets of customers that have been uneconomical to reach in the past are becoming available because of the Internet.. Existing relationships can be made more effective and less costly through the use of security and authentication over open networks. As e-commerce market forces are brought to bear upon organizations, organization will derive increasing value from the ability to quickly exchange policy documents to evaluate and determine whether it will be possible to send and rely upon important or confidential records over open networks. Policy evaluations will be greatly hampered if policy documents follow non-uniform or conflicting structure and content type.

On the other hand, availability of uniform policy formats can enable rapid scalability by enabling decision makers to evaluate other policies quickly. Uniform formats (and rapid document exchange) will help decision makers to determine whether the desired business transactions can take place under the existing policy, whether the policy and practices need to be amended, or whether no business case exists given the current state of policies and the costs or time entailed to bring them into shape. Similarly, such policies can form an efficient method to effect agreeable operating or system rules among parties with existing business relationships, but that lack a standard method of using PKI. The PKIX Framework, although imperfect, provides organization with a basis for policy interoperability.

D.3.1 Criteria for Making the Determination

Policy Authorities should weigh several factors when determining whether a Certificate Policy is necessary or desirable. Some factors include:

D.3.1.1 Does the use of a PKI involve certificates?

If a PKI does not use or plan on using certificates, then a Certificate Policy may be the wrong form of policy. Using PKI-based digital signatures that are not verifiable with reference to a certificate would not implicate many of the issues addressed in a Certificate Policy. Other forms of policy, such as key usage or binding a party to a key, may be desirable, but a Certificate Policy may be inappropriate.

D.3.1.2 Is this a single party system?

If a single-party system is envisioned, then a formal governance body may not exist and, as a result, a formal policy may not be needed. In large, geographically-dispersed entities such as governments or large corporations, however, internal policy may be an appropriate management tool. Internal policy would be appropriate in cases where sensitive, high-value or mission-critical applications depend upon the proper functioning of certificate-based PKI to operate.

D.3.1.3 Is the underlying transaction of low-value?

If the underlying transaction is of low-value, then it may be inefficient or uneconomical to develop a full Certificate Policy. In this context, the term "value" is broader than a direct cost measure. A cost/benefit and risk analysis, or similar analytical tool, can project whether an application is of high value or not. Even relatively low cost applications may entail high risk in terms of litigation exposure or loss of reputation in the event of system failures. Similarly, a low-cost system may provide high-benefit for an organization, by bringing in a regular revenue stream or by directly facilitating the mission of the entity.

D.3.1.4 Is there already a Certificate Policy in play?

If another Certificate Policy has been promulgated by a party with which the organization must interact, but with which it has little or no bargaining power, the exercise of drafting a policy may, nonetheless, be valuable as a method of testing whether the other organization's Certificate Policy specifies important provisions adequately.

D.3.2 Scope and Detail of the Certificate Policy

A Certificate Policy may have a broad scope of coverage for many different types of underlying transactions but still be relatively general and short. For example, a Certificate Policy may be an amendment to an existing policy document that already handles many of the issues that need to be addressed for a given system, such as financial responsibility, archival, audits, etc. On the other hand, a Certificate Policy could be very detailed, but could have a very narrow scope, such as a single transaction between two parties. Alternately, the Certificate Policy could be short and undetailed as well as narrow in scope (as with an internal application or a relatively informal application between two well-established parties).

D.3.2.1 Public and/or Private Parties in Contract Systems

Because of the difficulty with drafting guidelines in the absence of a particular set of business and legal conditions, these Guidelines were developed with certain *assumptions* about the nature of the parties and transactions. Such assumptions include the assumption that Policy Authorities will seek to draft Certificate Policies to support systems in which each party has signed a contract and entered into a closed or otherwise bounded transactional system. Further, the Guidelines have been written to support both public sector and private sector parties in the drafting of Certificate Policies.

The section of these Guidelines that provides guidance in the form of drafting instructions for a Policy Authority assumes either a fairly significant set of transactions or at least two separate parties. The Task Force expects that the audience for this document seeks to draft a Certificate Policy to facilitate the use of public key certificates for non-trivial business interests that transcend the boundaries of a single party.

D.3.2.1.1 Reference Model: Business to Government Procurement in a Bounded Contract System

Another reason these Guidelines do not contemplate a single, narrowly-defined transaction is because publishing a policy document tailored to the needs of a particular business environment and specified transactions would not be easily ported to another environment with different parties and transactions. These Guidelines are meant to be useful to a range of public and private sector parties who seek assistance drafting policies to support a variety of applications. Unfortunately, it would be nearly impossible to draft a sound policy that is so vague that it could accommodate any number of different transactions. Such a document would not provide sufficient guidance for Policy Authorities to craft a Certificate Policy to meet the needs of their organizations. For these reasons, these Guidelines were drafted with a general business environment in mind as a reference model. The general business environment used as a reference model is as follows:

- Buyers and sellers with a contract in place that governs the terms of the purchase and the business relationship;
- The purchase and sale are conducted via online, web-based catalogues;
- Shopping, enforceable quotes, approved orders, and confirmations are secured and authenticated to some extent based upon the browser certificates of buyers and the server certificates of sellers; and
- The buyer is a public sector party and the seller is a private sector party.

Although the Guidelines make occasional reference to a business to government procurement example, the Task Force has taken care to indicate throughout the document how different business environments might affect the policy drafting process.

D.3.2.1.2 Variations

These Guidelines have been drafted primarily to support closed or bounded communities. In the future, however, it is possible that more open systems will emerge. Some commentators have suggested that standards-based "registries" and reputations-based "clearing houses" will open the way for stranger to stranger, secure and authenticated, global communications based upon certificates.⁷⁸

While accreditation of a PKI Service Provider is beyond the scope of these Guidelines, it is worth noting that such accreditation could become part of the foundation for more open systems that would support secure and authenticated electronic commerce. According to the PKIX Framework, a Certificate Policy can form the requirement set for accreditation of PKI Service Providers. The PKIX Framework states:

⁷⁸ Assuming Certificate Policies continue to proliferate at the current rate, then a widely accessible and organized means for accessing such policies will become increasingly valuable. There is a need to attach meaning to a given Object Identifier and to make the related policy materials available in a manner that is capable of dynamic updating. The need for an online and reliable policy and document registry will become more pronounced over time.

"Certificate policies also constitute a basis for accreditation of CAs. Each CA is accredited against one or more certificate policies which it is recognized as implementing. When one CA issues a CA-certificate for another CA, the issuing CA must assess the set of certificate policies for which it trusts the subject CA (such assessment may be based upon accreditation with respect to the certificate policies involved)."

The states of Utah and Washington have enacted laws that provide for the licensing of Certificate Authorities. These statutes initially caused alarm among some members of Congress and the banking community due to fear of a patchwork of conflicting state laws governing the conduct of interstate commerce facilitated by PKI. These states, however, have worked on cross-border recognition agreements to smooth the treatment of PKI between their jurisdictions. The states of California and Texas both enacted regulations that would allow accredited Certificate Authorities to be qualified for special "approved" status to transact business with the state government or to issue certificates that the state government could rely on. It is hoped that accreditation can provide a means of normalizing the treatment of certificate usage throughout state governments and among public and private sector parties that evaluate PKI Service Providers. Each of the states mentioned in this paragraph participated in the CARAT Task Force as well as in other states and state government professional organizations. The advent of more standardized private law based treatment of PKI could set the stage for interoperability between levels of government and the private sector.

Accreditation of a PKI Service Provider for all purposes is beyond the scope of these Guidelines. These Guidelines have been drafted to support the creation of "affinity" Certificate Policies that govern categories of like parties, similar transactions and non-conflicting business environments. Such a Certificate Policy would not provide useful policy for accreditation of a PKI model as necessarily fit for all possible parties, transactions and environments. Such a policy could be suitable for adoption by multiple organizations for such purposes as:

- Multi-state procurement or joint private sector procurement
- Citizen to government account usage or consumer to private business account usage
- Government to government sensitive information sharing or hospital to hospital sensitive information sharing

For the time being, however, these Guidelines are expected to be used merely to facilitate the drafting of Certificate Policies that govern relatively closed or bounded communities, perhaps around a set of affinity applications. It is interesting to note, however, that the four cornered model, discussed in Part C of this document would be particularly well suited to support scalable and more "open" PKIs.

PART E. DRAFTING A CERTIFICATE POLICY

The following part is a Guideline for drafters of Certificate Policies.

E.1 These Guidelines Follow the IETF PKIX 4 Framework

The IETF PKIX 4 Framework (RFC 2527) is an Internet-Draft. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF) and its working groups. The purpose of the IETF PKIX Framework is to assist writers of certificate policies by providing a comprehensive list of topics that potentially (at the writer's discretion) need to be covered in a Certificate Policy. Although it is a working draft, the IETF PKIX Framework has become a *de facto* standard for organizing both Certificate Policies and Certificate Practice Statements.

In the following sections, the CARAT Task Force provides Certificate Policy writers with drafting instructions for IETF PKIX Framework sections 1, 2, 3, 4, and 8. Sections 5, 6, and 7 were omitted as being too technically detailed to be included as guidelines.

Many commentators agree that the IETF PKIX Framework is not the ideal outline for structuring a Certificate Policy. Nearly all writers will be tempted to change the outline to suit a particular set of logical needs. Nevertheless, the Task Force recommends using the IETF PKIX Framework for the sake of interoperability and efficiency.

E.2 Organization

The Task Force has structured these Guidelines to follow the IETF PKIX Framework. The Task Force has not renumbered or reorganized headings. However, the Task Force has made the following modifications:

- High level numbering and headings have been expanded by the addition of new subheadings to reference new information.
- Headings have not been reorganized or renumbered. However, where additional subject matter is appropriate or the PKIX Framework does not fit an envisioned business mode, headings have been added with highlighting, such as underlining (for paper documents) and bolding them in red (for electronic documents).
- Some low level sub-headings have been collapsed under a higher level heading. (For example, sub-headings 1.3.1, 1.3.2, and 1.3.3 are included under sub-heading 1.3.)
- The words "No Stipulation" are used to designate that no content is included under a given heading.
- Headings are omitted if there is no content for Drafting Instruction, Discussion, or Cross-Reference sections.

To clarify and better organize the Framework sections, the Task Force has added Drafting Instructions, Discussion, and Cross-References to each section.

- *Drafting Instructions*: At the beginning of each section, the Guidelines contain Drafting Instructions to help drafters write certificate policies. Drafting Instructions are written at a high level and are intended to be globally applicable to a variety of business models. Drafters are cautioned to consider differences in individual projects when applying any Drafting Instruction to their specific business model.
- *Discussion*: The second part of each section is a discussion that explains the Drafting Instructions or highlights specific issues that drafters should consider. The Discussion provides background, context, and an educational overview of the issues raised in the corresponding Drafting Instructions.
- *Cross-Reference*: Some sections of the PKIX Framework contain the same or similar subject matter as other sections. Where the subject matter of sections overlap, the Task Force provides cross-references to related sections.

Note: a Certificate Policy will *not* normally follow this three-part format.

INTRODUCTION

1.1 Overview

Drafting Instructions

The Overview of a Certificate Policy is an introduction to the Policy. The Overview states the drafter's methodology in organizing and structuring the Policy. The Overview may also state the type of transactions the Certificate Policy supports, the parties engaged in the transactions, and the broad assumptions necessary to understand and interpret the Certificate Policy.

Discussion

1. A Certificate Policy should contain the "requirements" specified for the utilization of PKI for the particular type(s) of transactions in which End Entities will participate. The Overview should provide a high, summary level statement about the type of transactional relationships that the Certificate Policy supports, as well as the identity of the parties that will participate in the transaction. If expressed at a high level, an overview can help to facilitate the establishment of the contractual arrangements among PKI Service Providers or a Policy Authority and End Entities.
2. The Overview section is a high-level introduction to the Certificate Policy. Drafters are cautioned not to duplicate information contained in Section "1.3 Community and Applicability" unnecessarily
3. Introductions and overviews are usually very similar and are sometimes redundant. Unless there is a clear reason to do otherwise, drafters should include introductions and overviews under the heading, "1.1 Overview" and not under "1. INTRODUCTION."

Cross-Reference

Section 1.3 Community and Applicability.

1.2 Identification

Drafting Instructions

A Certificate Policy may be referenced in this section by an object identifier (OID) assigned to the policy in the United States by the American National Standards Institute (ANSI).

The following format is often used:

This Policy is registered with _____, and has been assigned an object identifier (OID) of _____.

Discussion

1. What is an OID?: An object identifier (OID) is a unique numeric or alphanumeric identifier that unambiguously names an object. An object is anything that can be named, such as a Certificate Policy. It is envisioned that OIDs will be embedded in digital certificates so that PKI Service Providers, End Entities, and others can determine the set of rules under which an Issuer/Certificate Manufacturer has generated a certificate.
2. OIDs should be registered: The International Standards Organization (ISO), internationally, and ANSI, in the United States, facilitate the registration of OIDs for organizations. The purpose of registration is philosophically similar to the registration of legal entity names (corporations, partnerships, etc.) undertaken by the Secretary of State in most U.S. states. The goal of registration is to ensure that all OIDs are unique. If a certificate references a Certificate Policy with an OID, there should never be confusion over which set of rules governs that certificate. Accordingly, if a Certificate Policy drafted under these Guidelines is to be referenced by an OID, the OID should be registered with ANSI or an appropriate international standards body. OIDs should never be contrived.
3. Establishing an OID: The first step in obtaining an OID is to register an organization through an application process established by the American National Standards Institute ("ANSI"). See http://web.ansi.org/public/services/reg_org.html for more information on how to register an organization; see also ISO/IEC 9843-1: 1992, CCITT X.600. Organization Names consist of a unique numeric name and an optional alphanumeric name. After an organization has registered a numeric organization name, it may create object identifiers by appending additional numeric suffixes to the organization name. For instance, if an organization name were {2 16 840 1} then an object identifier for a Certificate Policy written by that organization could be {2 16 840 1 100}.

American National Standards Institute (ANSI) Contact Information:

Address:

American National Standards Institute

11 West 42nd Street

13th floor

New York, N.Y. 10036

Telephone:+ 1 212 642 49 00

Telefax:+ 1 212 398 00 23

E-mail:info@ansi.org

WWW:<http://www.ansi.org/4>. Organization Name Registration Fees: As of August 1998, ANSI's fee schedule for organization name registration is as follows:

Registration fee for both name forms (numeric and alphanumeric)	\$2,500
Registration fee for numeric name	\$1,000
Registration fee for alphanumeric name (numeric name previously assigned)	\$1,500
Challenge Fee	\$2,500
Challenge Loser Fee	To be Determined
Inquiry Fee (per item)	\$100

See <http://web.ansi.org/public/services/org/fee.html>.

5. OID Lookup: Presently, there is no standard means of looking up an OID. As a result, the establishment of an OID at this time may not be helpful in referencing a Certificate Policy. As more OIDs are registered, as demand for standard lookup procedures increases, and as standard rules for the use of OIDs develop, OIDs may prove to be a useful method of referencing a Certificate Policy. Accordingly, it is a business judgment whether or not to obtain an OID for a Certificate Policy.

6. International Name Registration: ANSI provides registration services for organizations within the United States. Organizations operating outside the United States must register with standards bodies in their home countries. See <http://www.iso.ch/>, generally, and <http://www.iso.ch/addresse/membodies.html>, specifically, for more information about standards bodies outside the United States.

7. Trademarking an OID to Deter Use by Issuers/Certificate Manufacturers Not Parties to the Certificate Policy: In a closed system, all certificates should contain the same OID that references the Certificate Policy with which the OID is associated. Likewise, because the system is closed, all Issuers/Certificate Manufacturers who generate certificates using the OID should be contractually bound to abide by the terms of the Certificate Policy with which the OID is associated. Unfortunately there are no means by which a Policy Authority (or anyone else) can prohibit Issuers/Certificate Manufacturers who are not bound by the Certificate Policy from creating certificates with that Policy's OID. As a result, a Relying Party could rely on a certificate from an Issuer/Certificate Manufacturer who is not bound by the Certificate Policy. If reliance results in loss to the Relying Party, the Relying Party may have no recourse against the rogue Issuer/Certificate Manufacture or, at least, the rights and obligations of the Relying Party and the Issuer/Certificate Manufacture may be unclear.

A potential solution to prevent Issuers/Certificate Manufacturers from using an OID improperly or fraudulently might be to trademark it. It is unclear today, however, whether an OID can be trademarked.

8. Whether an OID in a Certificate Incorporates a Certificate Policy by Reference: Incorporating an external document can fail if the reference is not clear, the authenticity of the referenced document is lacking or uncertain, or the intent to incorporate (as distinct from the intent merely to cite) is not clear from the document. Simply referencing a Certificate Policy by an OID in the certificate may well fall short in both the adequacy of the reference and the expression of an intention to incorporate. An object identifier is nothing more than a unique series of numbers, and its association with a particular document exists apart from the numbers, and can be unreliable or obscure. An OID may not be considered a reference at all, and simply listing it in a field can be interpreted in many ways other than as effecting an incorporation.

1.3 Community and Applicability

Drafting Instructions

The Community and Applicability section contains headings under which drafters may state the roles to be played by parties in the system, the legal names of the parties operating under a Certificate Policy (or a means by which legal names can be ascertained), and the specific transactions governed by the Certificate Policy.

Discussion

1. The following issues would be detailed in a Certificate Policy following the PKIX Framework:

- 1.3.1 Certification authorities
- 1.3.2 Registration authorities
- 1.3.3 End entities
- 1.3.4 Applicability

2. Section 1.3 of the PKIX Framework envisions a PKI with only two PKI Service Providers: Certification Authorities and Registration Authorities. The Guidelines, however, have defined additional PKI Service Providers. As a result, this section does not fit well within the assumption contained in these Guidelines. A better outline for these Guidelines would be the following:

1.3.1. PKI Service Providers

1.3.2. End Entities

1.3.3. Applicability

3. Defining the Roles of PKI Service Providers: Under a PKI Service Providers section, drafters would define the roles that parties operating under the Certificate Policy are expected to perform. A role definition might include a summary of the functions assigned to each role. Drafters should note that obligations arise based on functions assigned to a particular role. Thus, if a Party playing Role 1 is

responsible for Functions 1, 2, and 3, then that Party will have obligations associated with Functions 1, 2, and 3. Obligations are stated in Section 2 of the IETF PKIX 4 Framework and should not be duplicated in this section.

4. Stating the Legal Names of PKI Service Providers: This section may state the legal names of PKI Service Providers performing roles or a means by which the legal names of the PKI Service Providers can be ascertained.

Once a Certificate Policy is drafted, it is cumbersome to make changes to the document because change will usually require ratification and republication of the Certificate Policy and may require publication of a notice of change to Subscribers and Relying Parties. While it is useful to be able to add parties to a Certificate Policy, it is not practical to change the Policy every time a new party joins the system. As a result, drafters may choose not to list the legal names of parties in a Certificate Policy.

If it is desirable, nevertheless, to have a means of ascertaining the parties to a Certificate Policy, drafters should consider incorporating party names by reference to an external document. If the Certificate Policy is an electronic record, "incorporation by reference" may be done by including a Uniform Resource Locator ("URL" or web address) in the Policy. The URL points to a document, either a database or a directory, listing all the PKI Service Providers. If the Certificate Policy is a paper document, incorporation by reference may be done by attaching a paper addendum to the Policy. Incorporation by reference is useful because it provides as an easy way to add new parties to the Certificate Policy without redrafting, ratifying, or republishing the Policy.

5. Bricks and Mortar and Online Locations of Registrars: Usually, Registrars take a Subscriber's initial application and verify the Subscriber's identity or credentials. If required to register in person, Subscribers must know the location of Registrar's physical location(s). The Certificate Policy or a document incorporated by reference may provide the location and hours of operation of the Registrar's bricks and mortar establishment. If online identification is required, then Subscribers must know the Uniform Resource Locator ("URL" or web address) of the Registrar's online establishment. The physical and online locations and hours of operation of a Registrar should be listed or incorporated by reference in this section of the Certificate Policy.

6. Online Location of Repositories: If a system uses Repositories with online locations, then such locations should be listed or incorporated by in this section.

7. End Entities: In the End Entities section, drafters may state the types of Subscribers and Relying Parties who are authorized to use the system. It is not necessary and, indeed, it would be cumbersome to list the names of all Subscribers and Relying Parties. It is, however, important to ascertain in a closed system on a per transaction basis whether Subscriber and Relying Parties are contracted into the system. Applicability: The Applicability section should state the transactions governed by the Certificate Policy. The applicability section may also state transactions that are specifically prohibited under the Policy.

1.4 Contact Details

Drafting Instructions

In this section drafters should identify the Policy Authority, its scope of authority, and the contact person for the Policy Authority to whom communications related to the Policy should be referred.

Discussion

1. The following issues would be detailed in a Certificate Policy following the PKIX Framework:

- 1.4.1 Specification administration organization
- 1.4.2 Contact person
- 1.4.3 Person determining CPS suitability for the policy

2. 1.4.1 Specification Administration Organization: This document uses the term Policy Authority rather than Specification Administration Organization. This section contains the legal name of a Policy Authority administering the Certificate Policy. This section may also contain the names and organizations of Policy Authority members.

a. Membership: Unlike most PKI Service Providers, there will be only *one* Policy Authority. A Policy Authority may be a single entity or an association. If a Policy Authority is an association, its membership may be comprised of representatives of PKI Service Providers and End Entities. Policy Authority membership may also include government officials or a government agency.

b. Primary Duties: The primary duties of a Policy Authority are to organize and administer a PKI and to write (or facilitate the writing of) the Certificate Policy that governs the PKI. A Policy Authority may or may not be responsible for organizing and administering the transaction being facilitated by PKI.

3. 1.4.2 Contact Person: Contact details should be supplied for a person at the Policy Authority.

4. 1.4.3 Person Determining CPS Suitability for the Policy: Contact details should be supplied for the person who determines whether a company's documented practices, such as a Certificate Practice Statement, are in compliance with the requirements of the Certificate Policy. Drafters should note clearly if the person determining compliance is not the Policy Authority.

2. GENERAL PROVISIONS

2.1 Obligations

Drafting Instructions

A Certificate Policy should describe the obligations of each PKI Service Provider and End Entity to each of the other parties that are subject to the Certificate Policy.

Cross-Reference

See Part C, above.

2.2 Liability

Drafting Instructions

A Certificate Policy should describe any limits or requirements governing liability of the parties based upon breach of contractual obligations by one or more parties to other parties.

Discussion

1. The following issues would be detailed in a Certificate Policy following the PKIX Framework:

- 2.2.1 CA Liability
- 2.2.2 RA Liability

2. Strictly speaking, in legal language, *liability* is a duty that has been adjudicated as immediately and unconditionally due. Generally, a liability has been reduced to a specified monetary amount or, less frequently, to a specific performance or injunction; and a court will direct law enforcement officials to collect or otherwise enforce the judgment. An *obligation*, on the other hand, is a duty generally based on a promise; and, although its performance is required, it is nevertheless not enforceable without an adjudication that converts it into a liability.⁷⁹

Cross-Reference

See Part C, above.

2.3 Financial responsibility

Drafting Instructions

A Certificate Policy should indicate whether any PKI Service Provider is required to produce evidence of financial responsibility or indications of credit-worthiness that help to assure that a PKI Service Provider is able to satisfy its liabilities.

Discussion

1. The following issues would be detailed in a Certificate Policy following the PKIX Framework:

⁷⁹ This distinction is not always maintained colloquially, although failure to observe it can lead to conceptual confusion.

- 2.3.1 Indemnification by Relying Parties
- 2.3.2 Fiduciary Relationship
- 2.3.3 Administrative Process

2. Evidence of financial responsibility or of creditworthiness might include instruments such as bonds or standby letters of credit. Other evidence of financial responsibility might include insurance policies or balance sheets and asset reports. Where there is a right to collect, a Certificate Policy may also indicate how such rights are to be exercised.

3. Obligations that exist as part of a legally unenforceable ethos are important, but commerce generally insists on legal enforceability. An obligation that cannot be legally enforced may not be trustworthy by commercial standards.

The breach of an obligation can be reduced to a liability through adjudication (or arbitration), but that liability will not mean much if it cannot be collected.

4. In particular, it is to an Issuer's advantage to provide such assurances. Relying Parties are well advised to seek such assurances before trusting a party, especially if the party is an Issuer.

2.4 Interpretation and Enforcement

Drafting Instructions

A Certificate Policy should describe all legal documents contemplated in addition to the Certificate Policy and should indicate the order of precedence of those documents.

2.4.1 Governing law

Drafting Instructions

A Certificate Policy should state the governing law under which the Certificate Policy will be interpreted. A Certificate Policy should also indicate whether implementing contracts and other relevant agreements may state governing law other than that stated for the Certificate Policy itself.

Discussion

1. A Certificate Policy may be governed by the laws of one state or by the laws of several states. In a single-jurisdiction contract system, the law of the jurisdiction should govern a Certificate Policy. It is possible, however, that a larger contract system would permit the same Certificate Policy to be interpreted under the law of more than one state. While inconsistent legal interpretation of a single Certificate Policy among jurisdictions is not an ideal result, such a result may be necessary in order to accommodate important parties to the system who negotiate inclusion of different choice of law

provisions. Indeed, with respect to consumers, it may be impossible to separate a legal dispute from the jurisdiction in which the consumer has its principal contacts.

2. Since the Internet has no international borders, it may be pertinent to include provisions of law for international disputes, and/or disclaimers disavowing any intent to provide services to parties outside the US.

2.4.2 Severability, survival, merger, notice

Drafting Instructions

A Certificate Policy may contain contract provisions such as severability, survival, merger, and notice.

Discussion

1. The legal categories of severability, survival, merger, and notice may require being separated either into individual subheadings under Sub-section 2.4.2 (example: 2.4.2.1, etc.), or into separate headings under Section 2.4. To maintain consistency with the PKIX Framework document and for the purposes of this initial document, they are retained in this section, with distinct numbering..

2. If a Certificate Policy contains contract provisions, it should state the order of precedence of these contract provisions vis-à-vis provisions of any other contracts such as implementing contracts. It may not be possible in all situations to override the provisions of pre-existing contracts with the provisions of the Certificate Policy.

3. Survival: The PKIX Framework includes a reference to a clause related to "survival," but it is unclear which definition of "survival" was intended. There are two clear meanings of "survival." First, "survival" may refer to the continuation of the representations and warranties of the Certificate Policy in the event that clauses are severed, or that the Policy as a whole fails when subjected to legal tests. Second, "survival" may refer to the continuation of rights, duties, and obligations as applied to successors and assigns of the certificate holder. For the purposes of this document, "survival" is assumed to be specific to the successors and assigns of parties associated with the Certificate issued.

4. Notice: Many legal obligations arise or are discharged as a result of notice or lack of notice of an event. A means of giving notification to all parties should be stipulated in a Certificate Policy. The following describes issues to consider regarding notice:

a) *Physical Notice:* Physical notice may include a writing delivered by hand or by certified or registered mail.

b) *Virtual Notice - Insecure:* Insecure electronic methods of delivery such as fax and unsigned e-mail may be appropriate in certain circumstances. Those circumstances, if desired, should be documented in the Certificate Policy to provide notice of appropriate uses of each type of delivery.

c) *Virtual Notice - Secure:* Notice by secure electronic methods, such as digitally signed messages, should be a primary means of providing notification to all parties. A Certificate Policy may

require parties to obtain a Registered E-mail Address which would be considered a secure and reliable place to send and receive notification from all related parties. If Registered E-mail Addresses are used, then a Certificate Policy may deem a message sent to a registered email address as received.

d) *Notice Obligations:* With respect to notice, parties may be responsible for providing notification of (1) changes to the party's registered e-mail and postal address; (2) security compromises on the secrecy of the Subscriber's Private Key. Other types of notice events pertinent to the maintenance of the provisions of this Certificate Policy are covered throughout this document.

e) *Acknowledgement:* In certain cases, notification may be considered ineffectual until the sending party receives a secured electronic acknowledgement.

5. Merger and integration. This section should include requirements that implementing contracts include provisions that incorporate the Certificate Policy and any other relevant documents and that specify the order of precedence of the documents. For example, the Certificate Policy may provide that contracts shall include provisions that require that the contract be governed by the Certificate Policy.

6. Other Contract Provisions: Other contract provisions that may be contained in Certificate Policy are confidentiality, Acts of God, termination, assignment and sub-contracting, waiver, and equal dignities clauses.

7. Acts of God: PKI Service Providers are usually obligated to provide backup procedures that contemplate and eliminate service failures as a result of Acts of God. Drafters should carefully consider whether standard Acts of God provisions should excuse PKI Service Providers in cases of "unforeseen disaster."

8. Examples:

Severability

In the event that one or more of the provisions of this Certificate Policy shall for any reason be held to be invalid, illegal, or unenforceable in the courts of any state or of the United States of America, such unenforceability shall not affect any other provision. This Certificate Policy shall then be construed as if such unenforceable provision or provisions had never been contained herein, and, insofar as possible, construed to maintain the original intent of the parties.

Survival

Each and all of the provisions of the Agreement shall be binding upon and shall inure to the benefit of the parties hereto and their respective successors, executors, heirs, representatives, administrators, and assigns, whether express, implied, or apparent, of the parties. The rights and obligations detailed in this Policy are assignable by the parties, by the operation of law (including as a result of merger or a transfer of a controlling interest in voting securities), or otherwise, provided that such assignment is undertaken consistent with this Policy, and provided further that such assignment does not effect a novation of any other debts or obligations the assigning party owes to other parties at the time of such assignment.

Notice

Whenever any person hereto desires or is required to give any notice, demand, or request with respect to this Certificate Policy, such communication shall be made either by using digitally signed messages consistent with the requirements of this Certificate Policy, or in writing. Electronic communications shall be effective upon the sender receiving a valid, digitally signed acknowledgment of receipt from recipient. Such acknowledgement must be received within five (5) days, or else written notice must then be communicated. Communications in writing must be delivered by a counter service that confirms delivery in writing or via certified or registered mail, postage prepaid, return receipt requested, addressed as follows: <address>. Such communications shall be effective upon receipt.

A Party requiring receipt of notice under this Certificate Policy is required to provide notice of (1) changes in said party's address including postal and e-mail addresses, (2) security compromises on the Subscriber's Private Key, (3) changes in financial or personal information, which would change the basis upon which the Certificate has been granted, and (4) any other notice pertinent to the maintenance of the provisions of this Certificate Policy.

Merger

It is expressly agreed that the provisions set forth herein constitute all understanding and agreements between the parties. Any prior agreements, promises, negotiations, or representations not expressly set forth in this Agreement are of no force and effect. No term or provision of this Certificate Policy directly affecting the respective rights and obligations of any party may be orally amended, waived, supplemented, modified, or terminated, except by an authenticated message or document of such affected party, except to the extent provided otherwise herein.

2.4.3 Dispute resolution procedures

Drafting Instructions

Dispute resolution procedures should be addressed in the Certificate Policy and should include mechanisms for resolving disputes short of litigation.

Discussion

This section may include any requirements relating to dispute resolution for the contracts themselves that may need to exist in implementation contracts. In addition, there should be discussion of resolving disputes prior to going to formal third party alternative dispute resolution. There should be reference to help desk-like functions, and a formal process to communicate a formal request for action/payment (rather than having parties go directly to litigation).

2.5 Fees

Drafting Instructions

This section may state whether PKI Service Providers are authorized to charge fees and to define any limitations or caps on fees.

Discussion

1. The following issues would be detailed in a Certificate Policy following the PKIX Framework:

- 2.5.1 Certificate issuance or renewal fees
- 2.5.2 Certificate access fees
- 2.5.3 Revocation or status information access fees
- 2.5.4 Fees for other services, such as policy information
- 2.5.5 Refund policy

2. The types of fees that PKI Service Providers might charge are access fees on certificates or on certificate status information, or Certificate Revocation Lists ("CRL"s). Usually, a fee should not be charged for reading a Certificate Policy.

2.6 Publication and Repository

Drafting Instructions

A Certificate Policy should state what information PKI Service Providers must publish.

Discussion

1. The following issues would be detailed in a Certificate Policy following the PKIX Framework:

- 2.6.1 Publication of CA information
- 2.6.2 Frequency of publication
- 2.6.3 Access controls
- 2.6.4 Repositories

2. It is presumed that a Policy Authority will make the Certificate Policy available to all parties. A Policy Authority, however, may also require a PKI Service Provider to publish the Certificate Policy to all parties to the Certificate Policy.
3. Other items that PKI Service Providers may be required to publish include: issued certificates that reference the Certificate Policy, a Certificate Revocation List or online certificate status database, and the Issuer's certificate for its signing key.

Cross-Reference

See Section 2.1.1 and 2.1.5.

2.7 Compliance audit

Drafting Instructions

A Certificate Policy should include adequate and enforceable methods to assure compliance by each party.

Discussion

1. The following issues would be detailed in a Certificate Policy following the PKIX Framework:

- 2.7.1 Frequency of entity compliance audit
- 2.7.2 Identity/qualifications of auditor
- 2.7.3 Auditor's relationship to audited party
- 2.7.4 Topics covered by audit
- 2.7.5 Actions taken as a result of deficiency
- 2.7.6 Communication of results

2. A Certificate Policy should establish a reasonable, sound method to assure compliance. Compliance may be accomplished by providing for such measures as (a) contractual warranties of compliance with liquidated damages clauses or agreed upon mechanisms for oversight, (b) self-audit (or self-reporting of audits conducted by independent auditors), (c) for Issuers, proof of licensure by a state (like Utah or Washington) that licenses Issuers (CAs), and (d) if applicable, evidence of acceptance by other states via reciprocity arrangements. If licensure were used as a policy compliance method, then the licensed party would also be expected to provide other evidence of compliance on those topics not addressed by licensure, such as an audit or contractual warranties.

There are different types of audits. There are, for example, financial audits, security audits for technical requirements, and audits that are restricted to assuring compliance with other documented practices. In addition, there are regulatory audits, such as OCC audits of banks and IRS audits of tax paying individuals and entities. Some public agencies may undergo audits by other public entities, such as the GAO or state auditor offices.

3. Depending on the scope of the application and the particular obligations upon parties to the application, any number of methods might be appropriate to assure policy compliance. The compliance method used, audit based or not, should be selected based upon a cost-benefit analysis and risk assessment of the obligations in question. If the pilot is strictly internal, or if there is very little money or liability associated with the pilot, then relatively lax compliance measures may be appropriate. If the

application entails significant risk, then more elaborate and costly compliance measures may be appropriate. The applicable contracts among the parties should fully detail the method chosen and related matters.

2.8 Confidentiality

Drafting Instructions

Generally, a Certificate Policy should provide that information in certificates is not confidential. However, personally identifiable information not in a certificate should be considered confidential, unless there are provisions to the contrary in the Certificate Policy. Notices of any kind, including certificate revocation, should not be considered confidential with respect to parties to whom such notice is due under the Certificate Policy.

Discussion

1. The following issues would be detailed in a Certificate Policy following the PKIX Framework:
 - 2.8.1 Types of information to be kept confidential
 - 2.8.2 Types of information not considered confidential
 - 2.8.3 Disclosure of certificate revocation/suspension information
 - 2.8.4 Release to law enforcement officials
 - 2.8.5 Release as part of civil discovery
 - 2.8.6 Disclosure upon owner's request
 - 2.8.7 Other information release circumstances
2. Data vs. Transactional Privacy: There are two types of privacy that must be considered with respect to electronic transactions: *data privacy* and *transactional privacy*. Data privacy refers to the privacy and accuracy of data that a subject knows is being collected. Transactional privacy refers to the privacy and accuracy of transactional data that a subject may not know is being collected. Transactional information is generated whenever an electronic transaction takes place. Transactional information may or may not be collected as it is generated. When transactional data is collected, even if the subject of the transaction has no knowledge of collection, the subject has the same expectation of privacy as when a data is knowingly given.
3. Means and Methods of Using Data; Expectation of Privacy: There are different means and methods of using data that a subject either gives freely or that is collected without the subject's knowledge.
 - Computer Matching is any computer-supported process in which personal data records relating to many people are compared so that cases of interest can be identified. Data records are usually collected

with the knowledge of the subject, but a subject may not know that information given for a known purpose, such as a certificate application, might also be used to create a saleable customer list using computer matching techniques.

- Dataveillance is the systematic use of personal data systems to investigate or monitor the actions or communications of one or more persons. Personal dataveillance is the investigation or monitoring of an identified person, generally for a specific reason. Mass dataveillance is the investigation or monitoring of groups of people, generally to identify and to categorize individuals by interest groups. Dataveillance is usually done by monitoring transactional data.

Computer matching, dataveillance, and other data management and logging techniques should be employed by PKI Service Providers to increase the security of PKI systems and reduce the risk of fraud. In some situations, the techniques employed to maintain secure systems should not be publicized simply because knowledge of anti-fraud techniques potentially gives rise to new and inventive types of fraud. Nevertheless, all parties, particularly consumer End Entities , have an expectation that any information collected about them, with or without their knowledge, will be remain private.

1. The OECD Guidelines: Policy Authorities are urged to consider the Organisation for Economic Co-operation and Development, Guidelines Governing the Protection of Privacy and Transborder Data Flow of Personal Data state the following Guidelines in developing confidentiality and privacy protections:

- *The collection limitation principle*: data should be obtained lawfully and fairly.
- *The data quality principle*: data should be relevant to their purposes, accurate, complete and up-to-date.
- *The purpose specification principle*: the identification of the purposes for which data will be used and destruction of the data if no longer necessary to serve that purpose.
- *The use limitation principle*: use for purposes other than those specified is authorized only with consent of the data subject or by authority of law.
- *The security safeguard principle*: procedures to guard against loss, corruption, destruction or misuse of data should be established.
- *The openness principle*: it should be possible to acquire information about the collection, storage and use of personal data systems.
- *The individual participation principle*: the data subject normally has a right of access and to challenge data relating to him or her.

- *The accountability principle*: a data controller should be designed and accountable for complying with the measures to give effect to the principles.⁸⁰
1. Anonymous Transactions: One way to inhibit the use of transactional data is to keep transactions anonymous.
 2. Public Relations: A distinction must be made between information that is public and that which is confidential and should not be disclosed. The Policy Authority should ensure, from the outset, that all parties to any pilot are aware of the practices and policies associated with public relations, generally, and with statements to the media, specifically.
 3. Public Records Law: Maintaining confidentiality of data will be an important item for pilot policy and contracts for pilots that involve government entities, which must abide by public records laws
 4. Release to Law Enforcement Officials and Release as Part of Civil Discovery: In some cases, otherwise confidential information may be required by law to be released, either to law enforcement officials or to other authorized parties as part of civil discovery.
 5. Privacy of Information in a Certificate: A certificate is usually publicly available. Accordingly, information in the certificate should not be considered confidential.

Cross-Reference

See Part C.

2.9 Intellectual Property Rights

Drafting Instructions

A Certificate Policy should specify intellectual property requirements as well as limits on the use of intellectual property related to, and materials governed by, the Certificate Policy. The Certificate Policy should limit the assertion of intellectual property rights on information that must be available in accordance with other sections of the Certificate Policy. In addition, any requirements related to intellectual property that must be included in implementing contracts or other agreements may be specified.

Discussion

1. Consider advisability of prohibiting intellectual property rights in certain aspects of system.
2. Trademark of OID may be acceptable.

⁸⁰ Organisation for Economic Co-operation and Development, *Guidelines Governing the Protection of Privacy and Transborder Data Flow of Personal Data*, in 80 OECD Document C 58 (1980), reprinted in 20 I.L.M. 422 (1981).

3. IDENTIFICATION AND AUTHENTICATION

3.1 Initial Registration

Drafting Instructions

A Certificate Policy should require Applicants/Subscribers to sign a Subscriber Agreement during the application process and before a certificate is issued. A Certificate Policy should specify the means by which communications between certificate Applicants/Subscribers and Issuers/Registrars or other PKI Service Providers are conducted.

Discussion

1. Subscriber Agreement: These Guidelines are intended for use with closed PKI systems. Accordingly, participation should be limited to defined Applicants/Subscribers who have signed a Subscriber agreement.
2. Application Process: Depending on the particular business model, an applicant may complete an application and sign a Subscriber agreement before the application is submitted for approval, or an applicant may first complete an application and then, if approved, sign a Subscriber Agreement. Where the Applicant/Subscriber is to be a Relying Party, he or she may sign a Relying Party agreement simultaneously with the Subscriber agreement.
3. Communication: The Certificate Policy should state how a certificate application is to be communicated from the Applicant/Subscriber to the Issuer/Registrar or other PKI Service Provider. Potential options include electronically via e-mail or a web site, (provided that all communication is secure, which can be accomplished by using a suitable cryptographic protocol for electronic communications), by first class U.S. mail, or in person.

The choice of the communication method is dependent upon a number of factors, including whether an in person identity confirmation process is required, (see Section 3.1.9 below) or whether the applicant is already known to the Issuer/Registrar or other PKI Service Provider as would be the case for an employee or an established customer.

3.1.1 Types of names

Drafting Instructions

A Certificate Policy should require that Issuers/Registrars express all names specified in a certificate as X.509 Distinguished Names. Any other information that may be required will be based upon the needs of the particular application.

Discussion

1. X.509 Standard: These Guidelines assume that an X.509 version 3 certificate will be used. The Distinguished Name, therefore, must conform to the X.509 standard.
2. Identifying Information: In determining what other information, if any, may be required, Certificate Policy drafters should consider the applicant's common name, street address, locality name (the name of a city or town), state or province name, and country name. The Distinguished Name may also include an organization name (if the applicant has a significant identifying relationship with a particular organization) and an e-mail address (if the applicant has one and reads mail received at that address).
3. Privacy: In many applications, the information contained in a certificate will not be confidential. Accordingly, Certificate Policy drafters should seriously consider the privacy concerns associated with requiring that personally identifiable data be provided in certificate fields.

3.1.2 Need for names to be meaningful

Drafting Instructions

A Certificate Policy may, but need not, require names to be meaningful.

Discussion

1. Meaningful Names: In the case where it is determined that a Certificate Policy should specify meaningful names, (i.e. where the name itself has meaning) Certificate Policy drafters should consider the following:

Element	Description
Common name	The first name, middle name or middle initial (if the Subscriber has a middle name), and the surname of the Subscriber, in that order, separated by space characters.
Street address	The physical location where the Subscriber resides or conducts business or where the Subscriber can receive paper mail.
Locality name	The city or town where the Subscriber resides or conducts business.
State or province name	The state or province in which the Subscriber resides or conducts business.
Country name	The nation in which the Subscriber resides or conducts business.
Organization name	An organization with which the Subscriber has a significant relationship. The organization name serves only as an additional identifier of the Subscriber and does not imply employment or any authority to act on behalf of the

	organization unless the certificate or its policy specifically provide otherwise.
Electronic mail address	An electronic mail address at which the Subscriber can receive electronic mail via the Internet. (Unless the Certificate Policy provides that the certificate is to be used within another network.)

1. Pseudonymous certificates: As noted in the Discussion section of Guideline 3.1.1, Certificate Policy drafters may seek to protect the privacy of Subscribers by choosing not to include personally identifiable data within a certificate. In this case, the name data in a certificate would still be uniquely associated with the Subscriber, but a Relying Party would link the certificate to the identity of the Subscriber through the use of other external information such as role or authority databases. Such certificates are known as *pseudonymous certificates* because the identity of the Subscriber is dependent upon information not included in the certificate.

3.1.3 Rules for interpreting various name forms

Drafting Instructions

A Certificate Policy may specify whether the presence of Organizational Name is required. If an Organizational Name is required, a Certificate Policy should specify whether it serves only as an additional identifier of the Subscriber, or whether it indicates employment or the authority to act on behalf of the organization.

Discussion

1. Agency law implications: Whether the Organizational Name serves only as an additional identifier of the Subscriber or whether it indicates employment or authority is a significant issue for the Certificate Policy drafter; based upon established agency law, certificates can provide a Subscriber with the authority to speak for an organization and thus incur liability for the organization..

3.1.4 Uniqueness of names

Drafting Instructions

A Certificate Policy should assure that the Distinguished Name listed in a certificate is unambiguous and unique in relation to the person named within a defined naming domain.

Discussion

1. There are important technical and legal implications to this instruction.

Technical Perspective: From a technical perspective, all names listed in a given domain, such as a directory, must be unique. Otherwise, software relying on the uniqueness of names will "break." "Breaking" a directory or other unique domain will usually result in service interruptions.

Legal Perspective: From a legal perspective, even where there is a service interruption resulting from technical problems, legally there may be no actual damages that flow from the service interruption. That is, a directory may break, but if no one is actually damaged, then there are no legal consequences. Thus, while an ambiguous, non-unique name is potentially catastrophic from a technical perspective, the legal consequences of ambiguity may not be.

3.1.7 Method to prove possession of private key

Drafting Instructions

A Certificate Policy should provide that an Issuer/Registrar must confirm that:

- the Applicant/Subscriber is in possession of the private key corresponding to the public key specified in the application
- such private key is capable of creating a digital signature verifiable by the public key and an algorithm listed in the certificate
- the private key has not knowingly been compromised since its creation
- the public key is not shown in another certificate listed within a defined domain;
- there are no reasonable grounds to suspect that the Applicant/Subscriber's private key was obtained through theft, deceit, eavesdropping, or other unlawful means.

Discussion

1. Due diligence: The Issuer/Registrar or other PKI Service Provider must perform basic due diligence during the certificate application approval process.

3.1.8 Authentication of organization identity

Drafting Instructions

These Guidelines are intended for personal identity certificates only.

3.1.9 Authentication of individual identity

Drafting Instructions

A Certificate Policy should specify how the identity and other assertions of an Applicant/Subscriber are to be confirmed, whether in-person or through the use of online techniques.

Discussion

1. Options: Drafters of a Certificate Policy should consider matters such as convenience and cost when determining the method used to confirm the assertions of an applicant. For example, when an applicant is available in the same physical facility as the Issuer/Registrar or other PKI Service Provider, then in-

person identity confirmation may be a convenient and relatively low cost method. It should also be recognized that the use of multiple databases to further confirm the assertions of an applicant could substantially increase the reliability of the confirmation process. In some cases, such as low-value or low-risk transactions, or where the applicant is in a distant location and is already known to the Issuer/Registrar or other PKI Service Provider, online confirmation alone may be more appropriate. In other cases, a combination of in-person and online confirmation may be appropriate.

2. In-person Identity Confirmation: If a Certificate Policy requires personal appearance by the applicant with an Issuer/Registrar or other PKI Service Provider , then a Applicants/Subscribers must appear in person for identity confirmation prior to the issuance of a certificate. Issuers/Registrars or other PKI Service Providers should require the Applicant/Subscriber to submit sufficient evidence of identity when they are confirming the Applicant/Subscriber's assertions. Two pieces of identification, such as a valid government-issued picture ID or other identifying document that appears reasonable to the Issuer/Registrar or other PKI Service Provider, might be sufficient evidence to corroborate the applicant's assertion of identity
3. Online Confirmation: If a Certificate Policy permits online confirmation of identity and other Applicant/Subscriber assertions, Issuers/Registrars or other PKI Service Providers may require that the Applicant/Subscriber submit information that can be verified against independent databases. The information provided by the Applicant/Subscriber should be in substantial agreement with the information in the queried databases and within any tolerance limits specified in the particular Certificate Policy.
4. Additional Information: As described above, identity confirmation is of two fundamentally different kinds. A Certificate Policy should be clear about which of the two is involved. Confirmation procedures of Applicant/Subscriber's assertions should be appropriate for the intended transaction supported by the certificate
5. Standing Behind a Certificate: An Issuer/Registrar may “stand behind” a certificate. “Standing Behind” a certificate means that an Issuer/Registrar guarantees or warrants that the information in a certificate is true. Where an Issuer/Registrar agrees to stand behind a certificate, its confirmation practices are irrelevant, and it may not be necessary to state confirmation procedures in the Certificate Policy. Either the information in the certificate is true or it is not. If information is not true, the Issuer/Registrar will be liable for damages flowing from inaccuracies. An Issuer/Registrar may also state reliance limits on a certificate. Where an Issuer/Registrar stands behind a certificate and states reliance limits, the Issuer/Registrar may disclaim or limit liability to Relying Parties who rely on certificates for amounts beyond the reliance limit. Reliance limits are useful for transactions that can be reduced to monetary terms. Reliance limits are not useful for transactions that cannot be reduced to monetary terms. An example of a transaction that cannot be reduced to monetary terms is a certificate that is used to identify a mother who may authorize her child to be let out of school. If a certificate is issued to an imposter who kidnaps the child, a reliance limit is meaningless.
6. Promise to Perform Confirmation Procedures: An Issuer/Registrar may promise to perform a stated set of confirmation procedures in lieu of standing behind a certificate. Assuming the Issuer/Registrar performs the set of confirmation procedures according to a reasonable standard of care, the

Issuer/Registrar may limit or disclaim all damages flowing from inaccuracies. Where an Issuer/Registrar agrees to perform a set of confirmation procedures, those confirmation procedures should be detailed in the Certificate Policy. Procedures for generating audit trails sufficient to determine whether confirmation procedures were performed, in case of dispute, should also be included in the Certificate Policy.

3.2 Routine Rekey [Renewal]

Drafting Instructions

A Certificate Policy should specify the requirements that a Subscriber must meet in order to obtain renewal of his or her certificate, provided that the original certificate has not been revoked.

Discussion

1. Certificate renewal: Certificate drafters should consider how soon before the expiration of a certificate a renewal request may be made and how such a request may be made. For example, if a renewal request is made electronically, then the Subscriber should submit the renewal request using a digitally signed message generated with the Subscriber's private key that corresponds to the public key contained in the original certificate.

3.3 Rekey After Revocation [Renewal after Revocation]

Drafting Instructions

A Certificate Policy should not permit renewal of a certificate that has been revoked or that has expired.

Discussion

1. Renewal limitations: If a Subscriber does not have a valid certificate which was issued under a Certificate Policy, then a new application and confirmation of identity and other assertions should be required.

3.4 Revocation Request

Drafting Instructions

A Certificate Policy should provide that a revocation request submitted electronically using a digital signature verifiable by a valid certificate will be processed. The Certificate Policy may also allow a revocation request to be submitted in other ways. If so, the certificate should be revoked only after the Issuer/Registrar or other PKI Service Provider is satisfied that the revocation request is authentic and has been submitted by a person authorized by the Subscriber to request revocation.

Discussion

1. Revocation considerations: The method used to confirm a revocation request should be as secure as is appropriate given the underlying business need. An invalid revocation could result in significant liability..

4. OPERATIONAL REQUIREMENTS

4.1 Certificate Application

Drafting Instructions

A Certificate Policy should prescribe the minimum content of a certificate application. The Certificate Policy should also specify that all applications are subject to review, approval, and acceptance by the party specified in the Certificate Policy.

Discussion

1. In this section of a Certificate Policy, the Policy Authority should specify who is eligible to initiate the certificate application process. The Policy Authority must have a clear understanding of how it envisions the application process to function. For example, the Policy Authority may specify that only the individual named as the Subscriber may initiate the certificate application process. The Policy Authority may also require approval by a duly authorized representative of the subscriber. Alternatively, the Policy Authority may require a department head (or other authorized individual) to initiate the process on behalf of specific individuals.
2. If this application process is initiated electronically, it may be in either a secure or insecure environment. How secure the application process needs to be depends on the sensitivity of the intended use of the certificate and other relevant factors, such as the relationship among the parties.
3. The Policy Authority may prescribe what approval process may be used to determine whether or not to issue a given certificate. This approval process includes the method for confirming the identity of the applicant (see Section 3.1.9). The entire application process (in person or online application, initiated by the applicant or by someone on the applicant's behalf, requiring the applicant to be an employee of a specific entity to have the application approved, etc.) should be constructed to address the specific business need for which the Policy Authority is implementing the PKI .. Although this function is typically given to a Registrar, it may be allocated to another role.

Cross-Reference

Section 3.1, Initial Registration, Section 3.1.9, Authentication of Individual Identity

4.2 Certificate Issuance

Drafting Instructions

A Certificate Policy should require the issuance of a requested certificate only after the Subscriber identification and confirmation process is completed. The Certificate Policy should also require that the

Subscriber be notified of the issuance of the certificate and should specify the process by which the certificate is delivered or otherwise made available to the Subscriber.

Discussion

1. When developing a Certificate Policy, the Policy Authority needs to specify who will be notified in the event of a rejected certificate application. In all likelihood, the Registrar will need to be notified; however, there may be situations (depending on the risk of unauthorized applications) when notifying the applicant of the rejection of his or her application is not advisable.
2. When the application is issued, the certificate *should not* be delivered or made available to any party other than the Subscriber (i.e., the certificate should not be delivered to a department head for distribution to personnel).

Cross-Reference

Section 3.1.9, Authentication of Individual Identity

4.3 Certificate Acceptance

Drafting Instructions

A Certificate Policy should require an Issuer to specify how the Subscriber accepts or rejects the certificate. Furthermore, the Certificate Policy should require the Subscriber to acknowledge that by accepting the certificate he or she agrees to the terms and conditions contained in the Certificate Policy in relation to that certificate.

Discussion

1. The policy developed by the Policy Authority should specify what constitutes acceptance of the certificate by the Subscriber. The contract (Subscriber Agreement) between the Subscriber and the party authorized under the Certificate Policy to enter into agreements with Subscribers should address the same issue. Under a particular Certificate Policy, acceptance can be treated in several ways. For instance, a Subscriber may be required to indicate express acceptance of the certificate, or he or she may be deemed to have accepted it upon usage of that certificate. To determine what constitutes 'acceptance' for a given Certificate Policy, a Policy Authority should consider many factors. These include the number of Subscribers, the convenience of requiring express acceptance, and the importance of a Subscriber's reviewing a plain text version of the certificate to insure that the contents are accurate before expressly accepting it.
2. Whatever the method of acceptance prescribed by the Certificate Policy, the Subscriber must understand that acceptance of a certificate includes acceptance of the terms of the Certificate Policy. This provision is generally found in a Subscriber Agreement.

4.4 Certificate Revocation

4.4.1 Circumstances for revocation

Drafting Instructions

A Certificate Policy should specify the circumstances under which a certificate should be revoked. A Certificate Policy should provide for both permissive revocation upon request of the Subscriber and required revocation when it is reasonably determined that a certificate is unreliable.

Discussion

There are two types of revocation: *permissive revocation* and *required revocation*. Permissive revocation occurs when a Subscriber requests revocation. Required revocation occurs when any party reasonably determines that a certificate is unreliable.

1. Permissive Revocation: A Subscriber may request revocation of his or her certificate at any time for any reason.

The Policy Authority should determine whether an authorized representative of the Policy Authority or another member of the community that is subject to the Certificate Policy should be permitted to request the revocation of a certificate issued under the Certificate Policy. In either case, the Policy Authority must decide under what circumstances it will allow such a request. For example, depending on the business model, the Registrar may also be permitted to request the revocation of a certificate.

2. Required Revocation: A certificate should be revoked when:

- any of the information in the certificate is no longer accurate
- the private key associated with the certificate, or the media holding the private key, is or is suspected of having been compromised
- the Subscriber is no longer a member of the community that is subject to the Certificate Policy.
- the Subscriber requests it
- the Issuer determines that the certificate was not properly issued according to the terms of the Certificate Policy or any other applicable practice documents
- the Issuer ceases operations. In such event, all certificates issued by the Issuer shall be revoked prior to the date operations cease.

3. A Certificate Policy should require that a Subscriber promptly notify the Issuer of any facts that could affect the reliability of a certificate. These facts may include compromise of the private key, termination of the Subscriber's relationship with the community subject to the Certificate Policy, or a change in the factual information that appears on the certificate.

- When drafting a Certificate Policy, the Policy Authority needs to consider the circumstances, if any, under which an authorized individual other than the Subscriber may be required to request revocation of a certificate. For instance, if an authorized representative is aware that the Subscriber is using the certificate inappropriately or that the Subscriber's employment is about to be terminated, the Certificate Policy may also permit this individual to request the revocation of a certificate.

Cross-Reference

Section 4.4.2.

4.4.2 Who can request revocation

Drafting Instructions

A Certificate Policy should indicate which parties are permitted to request revocation of a certificate.

Discussion

- As noted in Section 4.4.1 above, the Policy Authority needs to consider the circumstances, if any, under which a certificate revocation request by someone other than the Subscriber must be honored. The Certificate Policy should also address the issue of whether, and under what circumstances, non-Subscribers should be required to request revocation. For instance, if an authorized representative is aware that the Subscriber is using the certificate inappropriately or that the Subscriber's employment is about to be terminated, the Certificate Policy may also permit this individual to request the revocation of a certificate. If the Policy Authority wishes to allow an individual other than the Subscriber to be able to request revocation of a certificate, the Policy Authority will need to add that party to this section.
- A Certificate Policy might only allow the Subscriber and the Issuer to request revocation of a certificate. However, in cases where the Registrar is a separate entity, the policy probably allow the Registrar to request revocation because the Registrar may reasonably be expected to possess information that is relevant to the validity of the certificate. For similar reasons, a Certificate Policy may permit a party such as a Repository to initiate revocation under prescribed circumstances. A Repository, for example, could be in possession of information that reasonably suggests that the Subscriber's private key is compromised. An Issuer should be cautious in responding to requests for revocation that do not originate from the Subscriber. Non-Subscriber requests should be honored only in circumstances where the risks of permitting reliance on a questionable certificate outweigh the inconvenience or potential loss to the Subscriber that could result from revocation.

Cross-Reference

Section 4.4.1.

4.4.3 Procedure for revocation request

Drafting Instructions

A Certificate Policy should specify the revocation request procedures to be followed by authorized parties. The procedures should require a certificate revocation request to be communicated promptly to the Issuer, and in a manner that allows the Issuer to ascertain the identity of the initiating party. A Certificate Policy should require an Issuer to revoke a certificate promptly when it has received a revocation request from a Subscriber or other authorized party, that complies with the procedures specified in the Certificate Policy.

Discussion

1. Depending on the business model being utilized, the revocation request may be submitted either directly to the Issuer or through another party such as the Registrar.
2. Because the various parties involved in a PKI have different rights with respect to certificate revocation, it is important for the Issuer to obtain reliable evidence of the identity of the party initiating the request. A Certificate Policy should require that if a certification request is communicated electronically, it should be digitally signed with the private key of the Subscriber. Alternatively, the Certificate Policy should provide that the Subscriber may request revocation by contacting the Issuer or a Registrar in person if he or she provides adequate proof of identity.
3. If the Policy Authority determines that the Certificate Policy will allow someone other than the Subscriber to request the revocation of a certificate, the Policy Authority should prescribe the procedure to be used by such individual or entity. If the party requesting revocation is not the Subscriber, the Policy Authority should consider whether, and in what manner, the request must be substantiated. In addition, the Certificate Policy should address whether any other due process is to be followed before revocation. For example, a Certificate Policy may address the issue of whether prior notice of revocation should be given to the Subscriber and whether the Subscriber should have an opportunity to object. There may be circumstances when Policy Authority may not wish to grant such due process rights to a Subscriber. A case in point being when a Subscriber's employment is involuntarily terminated by a member of the (Certificate Policy) community who has the right under the Certificate Policy to revoke the Subscriber's certificate.
4. The Policy Authority should realize that there are liability issues associated with the revocation of a certificate and should require a high level of authentication/confirmation of these requests before revoking a certificate.

4.4.4 Revocation request grace period

Drafting Instructions

A Certificate Policy should specify how often requests for revocation must be processed.

Discussion

1. The length of time between the Issuer's receipt of a revocation request and the time the Issuer is required to revoke the certificate should bear a reasonable relationship to the amount of risk the participants are willing to assume that someone may rely on a certificate for which a proper revocation request has been given but has not yet been acted upon.

How quickly revocation requests need to be processed (and CRLs or certificate status databases need to be updated) depends upon the specific application for which the Policy Authority is drafting the Certificate Policy. A Policy Authority should recognize that there may be risk and cost tradeoffs with respect to grace periods for revocation notices. If the Policy Authority determines that its PKI participants are willing to accept a grace period of a few hours in exchange for a lower implementation cost, the Certificate Policy may reflect that decision.

Cross-Reference

Section 4.4.9, CRL Issuance Frequency (If Applicable)

4.4.5 Circumstances for suspension

Drafting Instructions

These Guidelines do not support certificate suspension.

Discussion

1. Suspension is the temporary invalidation of a certificate, but since it wholly invalidates the certificate, albeit only temporarily, it can be seen as an excessively black-or-white tool for dealing with uncertainty. In cases where invalidation is unwarranted but the amounts at stake warrant significant attention, a PKI Service Provider can provide a message to a prospective Relying Party advising the party of a difficulty that has arisen. Such a message can be much more informative than a simple notation of temporary invalidity (suspension) because it can explain the situation and enable the Relying Party to arrive at a more informed decision whether to proceed to rely in a questionable situation or to forbear.

4.4.6 Who can request suspension

No Stipulation.

4.4.7 Procedure for suspension request

No Stipulation.

4.4.8 Limits on suspension period

No Stipulation.

4.4.9 CRL issuance frequency (if applicable)

Drafting Instructions

A Certificate Policy should require the Issuer to provide, promptly following revocation, notice to potential Relying Parties and any other parties specified in the Certificate Policy of the fact of revocation. A Certificate Policy should require prompt updating of the certificate revocation list, if one is used, or of the certificate status database, as applicable, and should require all revocation requests received by the Issuer and the resulting actions taken by the Issuer to be archived. A Certificate Policy should specify the manner and the time period in which the certificate revocation list or certificate status database should be updated following revocation.

Discussion

1. It is critical for a Policy Authority to understand the importance of providing prompt notice of the fact of revocation to all potential Relying Parties, and to reflect such understanding in a Certificate Policy. In current practice, this amounts to updating certificate revocation lists (CRLs) or certificate status databases in a timely manner. Exactly how often these updates need to take place is a function of the particular business of the Policy Authority or the intended use of the certificate. For example, assume that a university is using certificates and is updating the CRL or the certificate status database every 24 hours. The university may not be overly concerned if a student Subscriber with a revoked certificate uses the library database once or twice before the CRL or certificate status database was updated. That same university if using certificates for procurement, however, is likely to be very concerned if a Subscriber with a revoked certificate authorizes a shipment of goods under the same situation.
2. Because the timing of notice to Relying Parties depends on how quickly an Issuer revokes a certificate and then advertises the fact of revocation, a Policy Authority may wish to consider requiring Issuers to perform the update of CRLs or certificate status databases simultaneously with the act of revocation. Whether or not a Policy Authority decides to require this may depend on a number of factors such as the foreseeable adverse consequences of delayed notice and the cost to the participants of simultaneous revocation and notice.
3. It is possible and perhaps likely that other forms of revocation advertisements may become available for use within PKI systems, and Policy Authorities should consider the usefulness of such forms in light of the requirements of their particular systems. As with CRLs and certificate status databases, such forms should be viewed in light of how well they provide effective notice of the fact of certificate revocation to potential Relying Parties, as well as other factors such as the cost to use those forms.

Cross-Reference

Section 2.6, Publication and Validation Services, Section 4.4.4 Revocation Request Grace Period, and Section 4.4.11 Online Revocation/Status Checking Availability

4.4.10 CRL checking requirements

Drafting Instructions

If a certificate revocation list is used, a Certificate Policy should specify when a Relying Party should check a certificate revocation list in order to establish that the Relying Party's reliance upon a certificate was reasonable.

Discussion

A Policy Authority may determine that Relying Parties must check a CRL prior to every instance of reliance on a certificate. A Policy Authority may just as reasonably determine, however, that checking a CRL for each instance of reliance is excessive and unnecessary, depending on the circumstances involved. For example, if a Relying Party engages in frequent transactions involving only one or several Subscribers or involving small-dollar transactions, it may be reasonable to permit not checking a CRL for every use of a certificate. Nevertheless, a Certificate Policy should address the issue of the Relying Party's obligations to check a CRL, because this bears directly on the reasonableness of reliance upon a certificate. In so doing, a Certificate Policy should also address what the appropriate consequences might be in the event that a Relying Party fails to check a CRL as required.

4.4.11 On-line revocation/status checking availability

Drafting Instructions

A Certificate Policy should require the Issuer to provide, promptly following revocation, notice to potential Relying Parties and any other parties specified in the Certificate Policy of the fact of revocation. A Certificate Policy should require prompt updating of the certificate status database, if one is used, and should require all revocation requests received by the Issuer and the resulting actions taken by the Issuer to be archived. A Certificate Policy should specify the manner and the period in which the certificate status database should be updated following revocation.

Discussion

1. This section is closely related to Section 4.4.4 and essentially duplicates Section 4.4.9 above. This section restates the drafting instructions in Section 4.4.9 as they apply to online certificate status databases as opposed to CRLs. A Policy Authority must look at the whole process (how quickly to process revocation requests, how often to update certificate status databases and how often to publish such update to a Repository) in light of the specific application for which the Policy Authority is drafting the Certificate Policy. See Section 4.4.9 for a more complete discussion of the business considerations.

Cross-Reference

Section 4.4.9 CRL Issuance Frequency (If Applicable)

4.4.12 On-line revocation checking requirements

Drafting Instructions

If an online certificate status database is used, a Certificate Policy should specify that the frequency with which a Relying Party must check the database in order to establish that the Relying Party's reliance upon a certificate was reasonable.

Discussion

A Policy Authority may determine that Relying Parties must check an online certificate status database prior to every instance of reliance on a certificate. A Policy Authority, however, may just as reasonably determine that checking an online certificate status database for each instance of reliance is excessive and unnecessary, depending on the circumstances involved. For example, if a Relying Party engages in frequent transactions involving one or a few Subscribers or involving small-dollar transactions, it may be reasonable to permit not checking a CRL for every use of a certificate. Nevertheless, a Certificate Policy should address the issue of the Relying Party's obligations to check the status of a certificate online, since this bears directly on the reasonableness of reliance upon a certificate. In so doing, a Certificate Policy should also address what the appropriate consequences might be in the event that a Relying Party fails to check a certificate status database as required.

Cross-Reference

Section 4.4.9 CRL Issuance Frequency (If Applicable), and Section 4.4.10 CRL Checking requirements.

4.4.13 Other forms of revocation advertisements available

No Stipulation.

4.4.14 Checking requirements for other forms of revocation advertisements

No Stipulation.

4.4.15 Special requirements re key compromise

No Stipulation.

4.5 Security Audit Procedures

Drafting Instructions

A Certificate Policy should ensure that each party that undertakes important obligations also agrees to maintain adequate electronic records that pertain to such obligations. Policies should ensure that sufficient records are kept to allow parties to access relevant and necessary information and to assist in carrying out the dispute resolution policies specified or permitted under the policy and as agreed upon by the parties. Record keeping requirements should be tailored to meet no more than the actual needs for recordation based on the circumstances surrounding the business environment that the policy exists to facilitate.

Discussion

1. The following issues would be detailed in a Certificate Policy following the PKIX Framework:

- 4.5.1 Types of event recorded
- 4.5.2 Frequency of processing log
- 4.5.3 Retention period for audit log
- 4.5.4 Protection of audit log
- 4.5.5 Audit log backup procedures
- 4.5.6 Audit collection system (internal vs. external)
- 4.5.7 Notification to event-causing subject
- 4.5.8 Vulnerability assessments

2. In some cases, a given business system may require such record keeping not only to resolve disputes, but also to detect irregular patterns as they emerge for the purpose of preventing security breaches. The availability of auditable records may also be required under other applicable law, depending on the specific application and the participating parties. The scope, detail, and procedures surrounding record keeping policies should be proportional to the risks and costs in question. For example, an application that is only a relatively small dollar pilot may require only negligible records audit procedures.

Record keeping requirements should be tailored to meet no more than the actual needs for recordation since record keeping can be time-consuming and costly, policies written under these guidelines should not require undue or excessive electronic record keeping.

3. The issue raised in Section 2.7 as to whether to seek quality assurance through pre-audit, government license, contractual warranties or otherwise should not be confused with the word "audit" as it appears in this section. This section refers to the internal record keeping procedures followed by participants that may form the basis of a future audit. The fact that a particular Certificate Policy written in

compliance with these guidelines may include requirements under this section does not necessarily mean that the policy must require a quality assurance audit as a pre-condition to participation by a party. Policies that try to ensure quality assurance through contractual warranties may also specify that a party must be contractually required to keep records that are sufficiently accurate, comprehensive, and secure from tampering for the purpose of assuring compliance with contractually agreed upon processes. The adequacy of credible records to show what actually happened is important in the event of future litigation, which is based in whole, or in part, upon alleged breach of a contractual warranty to use a certificate in a certain way, or to avoid issuing a certificate under certain circumstances. Such records can prevent unnecessary litigation by permitting parties to reconstruct a chain of events, or the records could be critical in determining the outcome of a dispute that does end up in litigation.

4. In circumstances where financial remedies are a sufficient cure for any unfounded reliance on a certificate, then a Certificate Policy may not require specific security procedures to be taken by PKI Service Providers. Specifying security procedures in all circumstances may, in fact, interfere with a PKI Service Provider's business decision as to the most effective security procedures and risk management protocols.

5. Types of event recorded: A Certificate Policy may require that all significant security events on Issuer, Registrar, and Repository systems be automatically recorded to protected, electronically time-stamped audit trail files. Typical events that might be recorded by an Issuer include, but are not limited to, the following examples. (1) certificate issuances, (2) certificate suspensions, (3) certification revocations, (4) changes of Issuer authority or delegations of authority, (5) changes of Issuer employee access rights that affect certificate granting or revocation processes, (6) internal Issuer key pair generation.

6. 4.5.3 Retention period for audit log: A Certificate Policy may state how long temporary audit trail files are required to be maintained onsite so that ad hoc reports and incident investigations can be made immediately, and it may set forth how they are to be securely archived thereafter. (See Section 4.6.) Drafters might require that such files be retained for a period of months or years on-site, and then be securely archived off-site. Long-term (off-site) storage for audit trail records should be accomplished via media storage, for a period of years after the date of the event.

7. 4.5.5 Audit log backup procedures: A Certificate Policy should require backup procedures of audit trail files to allow the same requirements and procedures afforded other critical files within Issuer, Registrar, and Repository automated systems.

8. 4.5.7 Notification to an event-causing subject: A Certificate Policy may state some automated scheme to report critical audited events to an appropriate person or system for immediate response as directed in the security plan.

9. 4.5.8 Vulnerability assessments: A Certificate Policy may require that the Issuer, Registrar, and Repository make vulnerability assessments of all internal processing applications and as needed by external audit functionaries. If required, such reports should be closely controlled and be required to be made available to the Policy Authority or other audit or compliance organizations upon request.

4.6 Records Archival

Drafting Instructions

This section of a Certificate Policy should include any requirements for records archival.

Discussion

1. The following issues would be detailed in a Certificate Policy following the PKIX Framework:

- 4.6.1 Types of event recorded
- 4.6.2 Retention period for archive
- 4.6.3 Protection of archive
- 4.6.4 Archive backup procedures
- 4.6.5 Requirements for time-stamping of records
- 4.6.6 Archive collection system (internal or external)
- 4.6.7 Procedures to obtain and verify archive information

2. A Certificate Policy should address the archival requirements for certain data and files by PKI Service Providers, including how long information is required to be securely maintained and whether or not electronic records are required to be time-stamped. Data and files that a Certificate Policy may require to be archived include computer security audit data, certificate application data, certificates and CRLs generated, key histories, and all correspondence between PKI Service Providers within the system. A Certificate Policy may also require that a complete set of back-up copies be maintained and be readily available within a specified period of time, in the event that the primary archives are lost or destroyed. To prevent the loss or destruction of these archives, the Certificate Policy should also specify how the archived information is to be protected, both physically and cryptographically.

3. 4.6.1 Types of event recorded: A Certificate Policy may require that the following data and files be archived by, or on behalf of, Issuers, Registrars, and Repositories, according to their proper function: (1) computer security audit data, (2) certificate application data, (3) certificates and CRLs generated, (4) key histories, (5) and all correspondence between the parties of the PKI.

4. 4.6.2 Retention period for archive: A Certificate may specify for how long key and certificate information must be securely maintained and for how long audit trail files must be maintained.

5. 4.6.4 Archive backup procedures : Adequate backup procedures should be in place so that in the event of the loss or destruction of the primary archives, a complete set of backup copies can be recovered.

6. 4.6.5 Requirements for time-stamping of records: A Certificate Policy may specify that electronic records must be time-stamped by a trusted third party time keeper.

7. 4.6.7 Procedures to obtain and verify archive information: If a security audit is required by a Certificate Policy, the Policy may require the auditor to verify the integrity of the archives. If the originals or the archives are corrupted or damaged in any material way, the corrupted or damaged copy should be replaced.
8. Drafters should pay attention to public law and internal organizational procedures for additional archive requirements.

4.7 Key changeover

Drafting Instructions

A Certificate Policy should indicate the minimum procedures, including process for secure new key distribution, associated with the change of a key pair used by Issuers to sign certificates.

Discussion

1. Key changeover refers to the change to a new key pair used by the Issuer to sign certificates. Among the issues to be considered are:

- any notice requirements
- assuring reliability of the process for showing how the generations of keys interlock - such as by signing a hash of the new key with the old key.

4.8 Compromise and Disaster Recovery

Drafting Instructions

A Certificate Policy should require that PKI Service Providers to have in place a disaster recovery/business resumption plan in place.

Discussion

1. The following issues would be detailed in a Certificate Policy following the PKIX Framework:

- 4.8.1 Computing resources, software, and/or data are corrupted
- 4.8.2 Entity public key is revoked
- 4.8.3 Entity key is compromised
- 4.8.4 Secure facility after a natural or other type of disaster

2. A disaster recovery plan could include any of the following:

- an operational facility located in a geographically separate area that is capable of providing corresponding services in accordance with the Certificate Policy, in the event of an unanticipated emergency
- provisions for redundancy of critical components, such as servers
- complete and periodic tests of the readiness of the backup facility

For security reasons, this plan should not be made generally available, but it must be made available to the individuals performing a security audit.

3. 4.8.2 Entity public key is revoked: A Certificate Policy may require Issuers to have in place a key compromise plan that addresses the procedures that will be followed if the Issuer's private signing key, the key used to issue certificates or used by a higher level Issuer, is compromised. This plan should include procedures for revoking all affected certificates and promptly notifying all affected parties operating under the Certificate Policy.

4. 4.8.4 Secure facility after a natural or other type of disaster: A Certificate Policy may require all PKI Service Providers to provide secure or backup facilities to prevent loss of service in the event of natural or other types of disasters.

Cross-Reference

Section 2.4.2 (Acts of God).

4.9 CA Termination

Drafting Instructions

If any PKI Service Provider ceases operation, the Provider should promptly notify all parties operating under the Certificate Policy. A Certificate Policy should specify a PKI Service Provider's obligations for cessation of operations. A Certificate Policy should require that all certificates issued by the Issuer that reference the Certificate Policy be revoked no later than the time of the termination.

8. SPECIFICATION ADMINISTRATION

Drafting Instructions

A Certificate Policy should provide for the process by which the policy is promulgated, amended, and terminated. It should also provide for any other relevant functions of the Policy Authority with respect to specification of the Certificate Policy.

Discussion

1. The following issues would be detailed in a Certificate Policy following the PKIX Framework:

- 8.1 Specification change procedures
- 8.2 Publication and notification policies
- 8.3 CPS approval procedures

2. This section should include issues such as:

- policy change procedures
- publication and notice requirements
- document approval process (ex., the documented practices of a party or boilerplate documents of parties)
- substantive or procedural matters relating to the role and functions of the Policy Authority with respect to specification of the Certificate Policy

Cross-Reference

Section 1.4.

Appendix

IETF PKIX Framework

1. INTRODUCTION

1.1 Overview

1.2 Identification

1.3 Community and Applicability

1.3.1 Certification authorities

1.3.2 Registration authorities

1.3.3 End entities

1.3.4 Applicability

1.4 Contact Details

1.4.1 Specification administration organization

1.4.2 Contact person

1.4.3 Person determining CPS suitability for the policy

2. GENERAL PROVISIONS

2.1 Obligations

2.1.1 CA obligations

2.1.2 RA obligations

2.1.3 Subscriber obligations

2.1.4 Relying Party obligations

2.1.5 Repository obligations

2.2 Liability

2.2.1 CA liability

2.2.2 RA liability

2.3 Financial responsibility

2.3.1 Indemnification by Relying Parties

- 2.3.2 Fiduciary relationships
- 2.3.3 Administrative processes
- 2.4 Interpretation and Enforcement
 - 2.4.1 Governing law
 - 2.4.2 Severability, survival, merger, notice
 - 2.4.3 Dispute resolution procedures
- 2.5 Fees
 - 2.5.1 Certificate issuance or renewal fees
 - 2.5.2 Certificate access fees
 - 2.5.3 Revocation or status information access fees
 - 2.5.4 Fees for other services such as policy information
 - 2.5.5 Refund policy
- 2.6 Publication and Repository
 - 2.6.1 Publication of CA information
 - 2.6.2 Frequency of publication
 - 2.6.3 Access controls
 - 2.6.4 Repositories
- 2.7 Compliance audit
 - 2.7.1 Frequency of entity compliance audit
 - 2.7.2 Identity/qualifications of auditor
 - 2.7.3 Auditor's relationship to audited party
 - 2.7.4 Topics covered by audit
 - 2.7.5 Actions taken as a result of deficiency
 - 2.7.6 Communication of results
- 2.8 Confidentiality
 - 2.8.1 Types of information to be kept confidential
 - 2.8.2 Types of information not considered confidential

2.8.3 Disclosure of certificate revocation/suspension information

2.8.4 Release to law enforcement officials

2.8.5 Release as part of civil discovery

2.8.6 Disclosure upon owner's request

2.8.7 Other information release circumstances

2.9 Intellectual Property Rights

3. IDENTIFICATION AND AUTHENTICATION

3.1 Initial Registration

3.1.1 Types of names

3.1.2 Need for names to be meaningful

3.1.3 Rules for interpreting various name forms

3.1.4 Uniqueness of names

3.1.5 Name claim dispute resolution procedure

3.1.6 Recognition, authentication and role of trademarks

3.1.7 Method to prove possession of private key

3.1.8 Authentication of organization identity

3.1.9 Authentication of individual identity

3.2 Routine Rekey

3.3 Rekey after Revocation

3.4 Revocation Request

4. OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.2 Certificate Issuance

4.3 Certificate Acceptance

4.4 Certificate Suspension and Revocation

4.4.1 Circumstances for revocation

4.4.10 CRL checking requirements

- 4.4.11 On-line revocation/status checking availability
- 4.4.12 On-line revocation checking requirements
- 4.4.13 Other forms of revocation advertisements available
- 4.4.14 Checking requirements for other forms of revocation advertisements
- 4.4.15 Special requirements re key compromise
- 4.4.2 Who can request revocation
- 4.4.3 Procedure for revocation request
- 4.4.4 Revocation request grace period
- 4.4.5 Circumstances for suspension
- 4.4.6 Who can request suspension
- 4.4.7 Procedure for suspension request
- 4.4.8 Limits on suspension period
- 4.4.9 CRL issuance frequency (if applicable)
- 4.5 Security Audit Procedures
 - 4.5.1 Types of event recorded
 - 4.5.2 Frequency of processing log
 - 4.5.3 Retention period for audit log
 - 4.5.4 Protection of audit log
 - 4.5.5 Audit log backup procedures
 - 4.5.6 Audit collection system (internal vs external)
 - 4.5.7 Notification to event-causing subject
 - 4.5.8 Vulnerability assessments
- 4.6 Records Archival
 - 4.6.1 Types of event recorded
 - 4.6.2 Retention period for archive
 - 4.6.3 Protection of archive
 - 4.6.4 Archive backup procedures

- 4.6.5 Requirements for time-stamping of records
 - 4.6.6 Archive collection system (internal or external)
 - 4.6.7 Procedures to obtain and verify archive information
 - 4.7 Key changeover
 - 4.8 Compromise and Disaster Recovery
 - 4.8.1 Computing resources, software, and/or data are corrupted
 - 4.8.2 Entity public key is revoked
 - 4.8.3 Entity key is compromised
 - 4.8.4 Secure facility after a natural or other type of disaster
 - 4.9 CA Termination
5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS
- 5.1 Physical Controls
 - 5.1.1 Site location and construction
 - 5.1.2 Physical access
 - 5.1.3 Power and air conditioning
 - 5.1.4 Water exposures
 - 5.1.5 Fire prevention and protection
 - 5.1.6 Media storage
 - 5.1.7 Waste disposal
 - 5.1.8 Off-site backup
 - 5.2 Procedural Controls
 - 5.2.1 Trusted roles
 - 5.2.2 Number of persons required per task
 - 5.2.3 Identification and authentication for each role
 - 5.3 Personnel Controls
 - 5.3.1 Background, qualifications, experience, and clearance requirements
 - 5.3.2 Background check procedures

5.3.3 Training requirements

5.3.4 Retraining frequency and requirements

5.3.5 Job rotation frequency and sequence

5.3.6 Sanctions for unauthorized actions

5.3.7 Contracting personnel requirements

5.3.8 Documentation supplied to personnel

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key pair generation

6.1.2 Private key delivery to entity

6.1.3 Public key delivery to certificate Issuer

6.1.4 CA public key delivery to users

6.1.5 Key sizes

6.1.6 Public key parameters generation

6.1.7 Parameter quality checking

6.1.8 Hardware/software key generation

6.1.9 Key usage purposes (as per X.509 v3 key usage field)

6.2 Private Key Protection

6.2.1 Standards for cryptographic module

6.2.2 Private key (n out of m) multi-person control

6.2.3 Private key escrow

6.2.4 Private key backup

6.2.5 Private key archival

6.2.6 Private key entry into cryptographic module

6.2.7 Method of activating private key

6.2.8 Method of deactivating private key

6.2.9 Method of destroying private key

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archival

6.3.2 Usage periods for the public and private keys

6.4 Activation Data

6.4.1 Activation data generation and installation

6.4.2 Activation data protection

6.4.3 Other aspects of activation data

6.5 Computer Security Controls

6.5.1 Specific computer security technical requirements

6.5.2 Computer security rating

6.6 Life Cycle Technical Controls

6.6.1 System development controls

6.6.2 Security management controls

6.6.3 Life cycle security ratings

6.7 Network Security Controls

6.8 Cryptographic Module Engineering Controls

7. CERTIFICATE AND CRL PROFILES

7.1 Certificate Profile

7.1.1 Version number(s)

7.1.2 Certificate extensions

7.1.3 Algorithm object identifiers

7.1.4 Name forms

7.1.5 Name constraints

7.1.6 Certificate policy Object Identifier

7.1.7 Usage of Policy Constraints extension

7.1.8 Policy qualifiers syntax and semantics

7.1.9 Processing semantics for the critical certificate policy extension

7.2 CRL Profile

7.2.1 Version number(s)

7.2.2 CRL and CRL entry extensions

8. SPECIFICATION ADMINISTRATION

8.1 Specification change procedures

8.2 Publication and notification policies

8.3 CPS approval procedures

**REQUEST FOR PROPOSALS FOR
DEVELOPMENT OF PUBLIC KEY INFRASTRUCTURE STANDARDS**

May 9, 1997

Introduction

The National Association of State Information Resource Executives (NASIRE), the [National Association of State Purchasing Officials \(NASPO\)](#) and the National Association of State Comptrollers (NASC) seek creative proposals from independent organizations to accomplish the objectives listed below by December 31, 1997.

Participating Parties

The following organizations and states (known as "participating parties") are cooperating in connection with this initiative: NASIRE, NASPO, NASC, California, Georgia, Massachusetts, Pennsylvania, Texas, Utah, and Washington.

Background

Digital signatures play a key role in electronic commerce by helping to ensure that electronic documents are accurate and have not been forged. Parties to electronic transactions need a common method of accreditation of certification authorities, the organizations charged with issuing and verifying digital signatures. NASIRE, with support from NASPO and NASC, is taking the lead on this issue to avoid each state developing its own accreditation process, thus slowing down the process for cross certification and accreditation that is necessary for national and international electronic commerce.

Description of Project

The project objectives include:

1. The organization is asked to propose an approach to develop and implement a self supporting (financially sustainable) entity whose function would be to set and maintain operating standards and rules to be used by subscribing members of the entity.

2. The organization shall provide a forum and process for interested government representatives and private sector parties to conduct a joint demonstration project for accreditation of certification authorities. For purposes of this solicitation, a "certification authority" (CA) means an organization that issues a certificate that relates to the validity of an electronic or digital signature.
3. The organization shall survey a representative sample of existing certification authorities to develop a benchmark for assessing technical and legal issues of accreditation.
4. The participating parties shall determine what criteria, including technical, business and legal requirements or standards, shall be applied to certification authorities whose certificates will be accepted by the parties for an online transaction. To the extent practicable, the criteria shall consist of reference to existing sets of standards and other non-proprietary suitable information.
5. Once the criteria is set, the organization shall procure, through an open, fair and competitive process, the services of a neutral party to act as an accreditor. The accreditor shall evaluate more than one CA according to the criteria and shall issue a rating for each CA based on the evaluation.
6. The participating parties shall assess the effectiveness of the rating system by conducting a series of electronic transactions using certificates issued by CAs with various ratings.
7. The organization shall evaluate the process, the criteria, the ratings and the test transactions and write an analysis report which maps a path forward for parties who wish to use CA ratings or accreditation as a basis for relying on certificates in the future. This report shall be submitted to each participating party in the project.
8. All work products, including rating criteria, methodology, and rating scheme, will be in the public domain.
9. Personnel commitments identified shall be considered material to the work to be performed. Staffing must include those individuals as proposed.
10. Interested organizations may not have any interests that would substantially conflict with the requirements of this solicitation or that would impair the organization's independent professional judgment. Specifically, certification authorities and their parent organizations will not be considered.

Requests for Proposals

Proposals shall include:

- a) relevant experience possessed by the organization that shows an ability to organize this type of public/private forum and technical project;

- b) resumes and qualifications of all proposed staff and/or subcontractors, their role(s) in the project and the expected percentage of time they will participate in the project;
- c) indication of how the process would be funded, how much the process would cost, who would pay and how the finances would be accounted for;
- d) definition of the time lines for completion of the project;
- e) description of what additional public and/or private sector parties should be included in the process.

Selection Committee

The Selection Committee will include representatives from NASIRE, NASPO and NASC, as well as other government and private entities who may also join the solicitation process.

Timeframe for Responses

Responses will be accepted until the end of the business day on **Monday, June 9**. The Selection Committee will meet to consider the responses and expect to award the project by the end of June.

If you are interested in responding to this Request for Proposal, please send your response of no more than ten typewritten pages to the attention of Angela Crouch, Program Manager, National Association of State Information Resource Executives, 167 West Main Street, Suite 600, Lexington, KY 40507. You may also fax your response to (606) 231-1928 or e-mail to <acrouch@iglou.com>. If you have questions, please contact Angela Crouch at (606) 231-1925.

[back to the home page](#)

[Comments About This Site?](#)

Copyright 1997, Commonwealth of Massachusetts. All rights reserved.

NEWS FEED@civic.com

At a Glance
Complete List of
May's Stories

Cover Story
Connecticut's
Face-Off

IT Solutions
Fingerprint System
Points Out Welfare
Fraud

IT Solutions,
Part 2
Sniffing Out
Medicaid Fraud
With Neural Nets

civic.com Select
Multimedia
Notebooks

HOME
SUBSCRIBE
CONTACT US

News for the week of May 12, 1997

NASIRE Seeks Proposals for Creation of Digital Signature Standards

Three state information management and finance associations last Friday invited industry proposals to set common standards for accrediting organizations that would certify digital signatures, an important first step in creating a national, and even international, electronic commerce infrastructure.

The National Association of State Information Resource Executives (NASIRE) is spearheading the project, with backing from the National Association of State Purchasing Officials and the National Association of State Comptrollers.

"Industry and government need to agree on a basic set of standards for certification authorities before the potential benefits of electronic commerce can be realized," said Carolyn Purcell, executive director of the Texas Information Resources Department and president of NASIRE, in a statement.

"Today, we require some documents to be notarized, certification authorities serve a role similar to that of a notary for electronic transactions of the future. We must have a common set of standards for rating the trustworthiness of these certification authorities and the electronic verifications they issue. A common set of standards will save resources and promote secure and reliable electronic commerce."

The solicitation came out of a series of meetings among chief information officers from around the country during the past year. "Sometime ago a group of NASIRE members got together as a group of interested parties in San Francisco to explore the states' need for a public-key infrastructure and certification for digital signatures," said Clyde Poole, team manager at the Texas Information Resources Department's oversight and operations division. Poole worked closely with Purcell on the solicitation.

NASIRE involvement is designed to "explore how certification issuing organizations might group together to self-regulate standards for business practices," he added. "That way a state could rely on a certificate without building its own certification process, in which case there could end up being 50 different processes." Those likely to respond to the solicitation are "mostly neutral trade associations" active in the certification authority field, Poole said.

Interested parties will have 30 days to respond. Proposals will be reviewed by a selection committee composed of CIOs from California, Massachusetts, Georgia, Washington, Pennsylvania, Utah and Texas. Also participating in the evaluation will be Jane Smith Patterson, senior adviser to the North Carolina Governor for Science and Technology and chair of the Electronic Commerce Task Force of the U.S. Innovation Partnership.

To become a part of an electronic list on this topic, send an e-mail to majordomo@lists.state.tx.us. In the body of the message, type: subscribe digsig.

-- *Jennifer Jones*

FOR IMMEDIATE RELEASE

May 1, 1997
Contact: Angela Crouch, NASIRE Staff
(606) 231-1925 or acrouch@jdlou.com

NASIRE, NASPO AND NASC SEEK ORGANIZATION TO DEVELOP DIGITAL SIGNATURE STANDARDS

Lexington, Ky.--The National Association of State Information Resource Executives (NASIRE), the [National Association of State Purchasing Officials \(NASPO\)](#) and the National Association of State Comptrollers (NASC) are seeking creative proposals from industry to establish accreditation standards for certification authorities that issue digital signatures. Digital signatures play a key role in electronic commerce by helping to ensure that electronic documents are accurate and have not been forged. Parties to electronic transactions need a common method of accreditation of certification authorities, the organizations charged with issuing and verifying digital signatures. NASIRE is taking the lead on this issue to avoid each state developing its own accreditation process, thus slowing down the process for cross certification and accreditation that is necessary for national and international electronic commerce.

"Industry and government need to agree on a basic set of standards for certification authorities before the potential benefits of electronic commerce can be realized" according to Carolyn Purcell, NASIRE President and Executive Director of the Texas Department of Information Resources. "Today, we require some documents to be notarized, certification authorities serve a role similar to that of a notary for electronic transactions of the future. We must have a common set of standards for rating the trustworthiness of these certification authorities and the electronic verifications they issue. A common set of standards will save resources and promote secure and reliable electronic commerce."

The solicitation will be released to interested parties on May 9. Organizations responding to the solicitation will have 30 days to return a proposal to the NASIRE office. The Selection Committee will include the following state Chief Information Officers: John Thomas Flynn, California; Louis Guiterrez, Massachusetts; Mike Hale, Georgia; Steve Koldeney, Washington; Larry Olson, Pennsylvania; Gordon Peterson, Utah; and Carolyn Purcell, Texas. Jane Smith Patterson, Senior Advisor to the North Carolina Governor for Science and Technology and chair of the Electronic Commerce Task Force of the U.S. Innovation Partnership, will also participate on the Selection Committee. The Committee will be expanded to include representatives from other government and private entities who may also join in the solicitation process.

NASIRE is the leading forum for addressing the opportunities, implications, and challenges of improving the business of government through the application of information technology. NASIRE represents information resource executives and managers from the 50 states, six U. S. territories, and the District of Columbia. Representatives from federal, municipal, and foreign governments also participate in the organization as associate members. Corporations, private universities, and non-profit organizations may participate as corporate members.

NASPO is a non-profit organization through which member purchasing officials provide leadership in professional public purchasing, improve the quality of purchasing and procurement, exchange information, and cooperate to attain greater efficiency, economy and customer satisfaction. The association's office is located in Lexington, Kentucky.

NASC is the professional association of the controllers and chief accounting and financial reporting officials of the 50 states, the District of Columbia and the Commonwealth of Puerto Rico. The association's main office is in Lexington, Kentucky and the Washington, D.C. office is located in the Hall of the States in the nation's capital.

###

Network Working Group
Request for Comments: 3647
Obsoletes: 2527
Category: Informational

S. Chokhani
Orion Security Solutions, Inc.
W. Ford
VeriSign, Inc.

R. Sabet
Cooley Godward LLP
C. Merrill
McCarter & English, LLP
S. Wu
Infoliance, Inc.
November 2003

Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2003). All Rights Reserved.

Abstract

This document presents a framework to assist the writers of certificate policies or certification practice statements for participants within public key infrastructures, such as certification authorities, policy authorities, and communities of interest that wish to rely on certificates. In particular, the framework provides a comprehensive list of topics that potentially (at the writer's discretion) need to be covered in a certificate policy or a certification practice statement. This document supersedes RFC 2527.

Table of Contents

1. Introduction	4
-----------------------	---

1.1. Background	4
1.2. Purpose.....	5
1.3. Scope.....	6
2. Definitions.....	6
3. Concepts	9
3.1. Certificate Policy	9
3.2. Certificate Policy Examples.....	11
3.3. X.509 Certificate Fields	12

Chokhani, et al.

Informational

[Page 1]

3.3.1. Certificate Policies Extension	12
3.3.2. Policy Mappings Extension.....	13
3.3.3. Policy Constraints Extension	13
3.3.4. Policy Qualifiers.....	14
3.4. Certification Practice Statement.....	15
3.5. Relationship Between CP and CPS.....	16
3.6. Relationship Among CPs, CPSs, Agreements, and Other Documents.....	17
3.7. Set of Provisions.....	20
4. Contents of a Set of Provisions.....	21
4.1. Introduction	22
4.1.1. Overview	22
4.1.2. Document Name and Identification	22
4.1.3. PKI Participants	23
4.1.4. Certificate Usage.....	24
4.1.5. Policy Administration.....	24
4.1.6. Definitions and Acronyms	24
4.2. Publication and Repository Responsibilities.....	25
4.3. Identification and Authentication (I&A).....	25
4.3.1. Naming	25
4.3.2. Initial Identity Validation.....	26
4.3.3. I&A for Re-key Requests.....	27
4.3.4. I&A for Revocation Requests.....	27
4.4. Certificate Life-Cycle Operational Requirements....	27
4.4.1. Certificate Application.....	28
4.4.2. Certificate Application Processing	28
4.4.3. Certificate Issuance	28
4.4.4. Certificate Acceptance	29
4.4.5. Key Pair and Certificate Usage	29
4.4.6. Certificate Renewal.....	30
4.4.7. Certificate Re-key	30
4.4.8. Certificate Modification	31
4.4.9. Certificate Revocation and Suspension.....	31
4.4.10. Certificate Status Services.....	33
4.4.11. End of Subscription.....	33
4.4.12. Key Escrow and Recovery.....	33
4.5. Facility, Management, and Operational Controls	33
4.5.1. Physical Security Controls	34
4.5.2. Procedural Controls.....	35
4.5.3. Personnel Controls	35
4.5.4. Audit Logging Procedures	36
4.5.5. Records Archival	37
4.5.6. Key Changeover	38

4.5.7. Compromise and Disaster Recovery	38
4.5.8. CA or RA Termination	38
4.6. Technical Security Controls.....	39
4.6.1. Key Pair Generation and Installation	39
4.6.2. Private Key Protection and Cryptographic	

Module Engineering Controls.....	40
4.6.3. Other Aspects of Key Pair Management.....	42
4.6.4. Activation Data.....	42
4.6.5. Computer Security Controls	42
4.6.6. Life Cycle Security Controls	43
4.6.7. Network Security Controls.....	43
4.6.8. Timestamping	43
4.7. Certificate, CRL, and OCSP Profiles.....	44
4.7.1. Certificate Profile.....	44
4.7.2. CRL Profile.....	44
4.7.3. OCSP Profile	44
4.8. Compliance Audit and Other Assessment.....	45
4.9. Other Business and Legal Matters	45
4.9.1. Fees	46
4.9.2. Financial Responsibility	47
4.9.3. Confidentiality of Business Information.....	47
4.9.4. Privacy of Personal Information.....	48
4.9.5. Intellectual Property Rights	48
4.9.6. Representations and Warranties	48
4.9.7. Disclaimers of Warranties.....	49
4.9.8. Limitations of Liability	49
4.9.9. Indemnities.....	49
4.9.10. Term and Termination	50
4.9.11. Individual notices and communications with participants.....	50
4.9.12. Amendments	50
4.9.13. Dispute Resolution Procedures.....	51
4.9.14. Governing Law.....	51
4.9.15. Compliance with Applicable Law	51
4.9.16. Miscellaneous Provisions	51
4.9.17. Other Provisions	53
5. Security Considerations.....	53
6. Outline of a Set of Provisions	53
7. Comparison to RFC 2527	60
8. Acknowledgements	88
9. References.....	88
10. Notes.....	89
12. List of Acronyms	91
13. Authors' Addresses	92
14. Full Copyright Statement	94

1. Introduction

1.1. Background

In general, a public-key certificate (hereinafter "certificate") binds a public key held by an entity (such as person, organization, account, device, or site) to a set of information that identifies the entity associated with use of the corresponding private key. In most cases involving identity certificates, this entity is known as the "subject" or "subscriber" of the certificate. Two exceptions, however, include devices (in which the subscriber is usually the individual or organization controlling the device) and anonymous certificates (in which the identity of the individual or organization is not available from the certificate itself). Other types of certificates bind public keys to attributes of an entity other than the entity's identity, such as a role, a title, or creditworthiness information.

A certificate is used by a "certificate user" or "relying party" that needs to use, and rely upon the accuracy of, the binding between the subject public key distributed via that certificate and the identity and/or other attributes of the subject contained in that certificate. A relying party is frequently an entity that verifies a digital signature from the certificate's subject where the digital signature is associated with an email, web form, electronic document, or other data. Other examples of relying parties can include a sender of encrypted email to the subscriber, a user of a web browser relying on a server certificate during a secure sockets layer (SSL) session, and an entity operating a server that controls access to online information using client certificates as an access control mechanism. In summary, a relying party is an entity that uses a public key in a certificate (for signature verification and/or encryption). The degree to which a relying party can trust the binding embodied in a certificate depends on several factors. These factors can include the practices followed by the certification authority (CA) in authenticating the subject; the CA's operating policy, procedures, and security controls; the scope of the subscriber's responsibilities (for example, in protecting the private key); and the stated responsibilities and liability terms and conditions of the CA (for example, warranties, disclaimers of warranties, and limitations of liability).

A Version 3 X.509 certificate may contain a field declaring that one

or more specific certificate policies apply to that certificate [ISO1]. According to X.509, a certificate policy (CP) is "a named set of rules that indicates the applicability of a certificate to a particular community and/or class of applications with common security requirements." A CP may be used by a relying party to help

in deciding whether a certificate, and the binding therein, are sufficiently trustworthy and otherwise appropriate for a particular application. The CP concept is an outgrowth of the policy statement concept developed for Internet Privacy Enhanced Mail [PEM1] and expanded upon in [BAU1]. The legal and liability aspects presented in Section 4.9 are outcomes of a collaborative effort between IETF PKIX working group and the American Bar Association (ABA) members who have worked on legal acceptance of digital signature and role of PKI in that acceptance.

A more detailed description of the practices followed by a CA in issuing and otherwise managing certificates may be contained in a certification practice statement (CPS) published by or referenced by the CA. According to the American Bar Association Information Security Committee's Digital Signature Guidelines (hereinafter "DSG")(1) and the Information Security Committee's PKI Assessment Guidelines (hereinafter "PAG")(2), "a CPS is a statement of the practices which a certification authority employs in issuing certificates." [ABA1, ABA2] In general, CPSs also describe practices relating to all certificate lifecycle services (e.g., issuance, management, revocation, and renewal or re-keying), and CPSs provide details concerning other business, legal, and technical matters. The terms contained in a CP or CPS may or may not be binding upon a PKI's participants as a contract. A CP or CPS may itself purport to be a contract. More commonly, however, an agreement may incorporate a CP or CPS by reference and therefore attempt to bind the parties of the agreement to some or all of its terms. For example, some PKIs may utilize a CP or (more commonly) a CPS that is incorporated by reference in the agreement between a subscriber and a CA or RA (called a "subscriber agreement") or the agreement between a relying party and a CA (called a "relying party agreement" or "RPA"). In other cases, however, a CP or CPS has no contractual significance at all. A PKI may intend these CPs and CPSs to be strictly informational or disclosure documents.

1.2. Purpose

The purpose of this document is twofold. First, the document aims to explain the concepts of a CP and a CPS, describe the differences between these two concepts, and describe their relationship to subscriber and relying party agreements. Second, this document aims to present a framework to assist the writers and users of certificate policies or CPSs in drafting and understanding these documents. In

particular, the framework identifies the elements that may need to be considered in formulating a CP or a CPS. The purpose is not to define particular certificate policies or CPSs, *per se*. Moreover, this document does not aim to provide legal advice or recommendations

as to particular requirements or practices that should be contained within CPs or CPSs. (Such recommendations, however, appear in [ABA2].)

1.3. Scope

The scope of this document is limited to discussion of the topics that can be covered in a CP (as defined in X.509) or CPS (as defined in the DSG and PAG). In particular, this document describes the types of information that should be considered for inclusion in a CP or a CPS. While the framework as presented generally assumes use of the X.509 version 3 certificate format for the purpose of providing assurances of identity, it is not intended that the material be restricted to use of that certificate format or identity certificates. Rather, it is intended that this framework be adaptable to other certificate formats and to certificates providing assurances other than identity that may come into use.

The scope does not extend to defining security policies generally (such as organization security policy, system security policy, or data labeling policy). Further, this document does not define a specific CP or CPS. Moreover, in presenting a framework, this document should be viewed and used as a flexible tool presenting topics that should be considered of particular relevance to CPs or CPSs, and not as a rigid formula for producing CPs or CPSs.

This document assumes that the reader is familiar with the general concepts of digital signatures, certificates, and public-key infrastructure (PKI), as used in X.509, the DSG, and the PAG.

2. Definitions

This document makes use of the following defined terms:

Activation data - Data values, other than keys, that are required to operate cryptographic modules and that need to be protected (e.g., a PIN, a passphrase, or a manually-held key share).

Authentication - The process of establishing that individuals, organizations, or things are who or what they claim to be. In the context of a PKI, authentication can be the process of establishing that an individual or organization applying for or seeking access to something under a certain name is, in fact, the proper individual or

organization. This corresponds to the second process involved with identification, as shown in the definition of "identification" below. Authentication can also refer to a security service that provides assurances that individuals, organizations, or things are who or what

they claim to be or that a message or other data originated from a specific individual, organization, or device. Thus, it is said that a digital signature of a message authenticates the message's sender.

CA-certificate - A certificate for one CA's public key issued by another CA.

Certificate policy (CP) - A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular CP might indicate applicability of a type of certificate to the authentication of parties engaging in business-to-business transactions for the trading of goods or services within a given price range.

Certification path - An ordered sequence of certificates that, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.

Certification Practice Statement (CPS) - A statement of the practices that a certification authority employs in issuing, managing, revoking, and renewing or re-keying certificates.

CPS Summary (or CPS Abstract) - A subset of the provisions of a complete CPS that is made public by a CA.

Identification - The process of establishing the identity of an individual or organization, i.e., to show that an individual or organization is a specific individual or organization. In the context of a PKI, identification refers to two processes:

- (1) establishing that a given name of an individual or organization corresponds to a real-world identity of an individual or organization, and
- (2) establishing that an individual or organization applying for or seeking access to something under that name is, in fact, the named individual or organization. A person seeking identification may be a certificate applicant, an applicant for employment in a trusted position within a PKI participant, or a person seeking access to a network or software application, such as a CA administrator seeking access to CA systems.

Issuing certification authority (issuing CA) - In the context of a particular certificate, the issuing CA is the CA that issued the certificate (see also Subject certification authority).

Participant - An individual or organization that plays a role within a given PKI as a subscriber, relying party, CA, RA, certificate manufacturing authority, repository service provider, or similar entity.

PKI Disclosure Statement (PDS) - An instrument that supplements a CP or CPS by disclosing critical information about the policies and practices of a CA/PKI. A PDS is a vehicle for disclosing and emphasizing information normally covered in detail by associated CP and/or CPS documents. Consequently, a PDS is not intended to replace a CP or CPS.

Policy qualifier - Policy-dependent information that may accompany a CP identifier in an X.509 certificate. Such information can include a pointer to the URL of the applicable CPS or relying party agreement. It may also include text (or number causing the appearance of text) that contains terms of the use of the certificate or other legal information.

Registration authority (RA) - An entity that is responsible for one or more of the following functions: the identification and authentication of certificate applicants, the approval or rejection of certificate applications, initiating certificate revocations or suspensions under certain circumstances, processing subscriber requests to revoke or suspend their certificates, and approving or rejecting requests by subscribers to renew or re-key their certificates. RAs, however, do not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA). [Note: The term Local Registration Authority (LRA) is sometimes used in other documents for the same concept.]

Relying party - A recipient of a certificate who acts in reliance on that certificate and/or any digital signatures verified using that certificate. In this document, the terms "certificate user" and "relying party" are used interchangeably.

Relying party agreement (RPA) - An agreement between a certification authority and relying party that typically establishes the rights and responsibilities between those parties regarding the verification of digital signatures or other uses of certificates.

Set of provisions - A collection of practice and/or policy statements, spanning a range of standard topics, for use in

expressing a CP or CPS employing the approach described in this framework.

Subject certification authority (subject CA) - In the context of a particular CA-certificate, the subject CA is the CA whose public key is certified in the certificate (see also Issuing certification authority).

Subscriber - A subject of a certificate who is issued a certificate.

Subscriber Agreement - An agreement between a CA and a subscriber that establishes the right and responsibilities of the parties regarding the issuance and management of certificates.

Validation - The process of identification of certificate applicants. "Validation" is a subset of "identification" and refers to identification in the context of establishing the identity of certificate applicants.

3. Concepts

This section explains the concepts of CP and CPS, and describes their relationship with other PKI documents, such as subscriber agreements and relying party agreements. Other related concepts are also described. Some of the material covered in this section and in some other sections is specific to certificate policies extensions as defined X.509 version 3. Except for those sections, this framework is intended to be adaptable to other certificate formats that may come into use.

3.1. Certificate Policy

When a certification authority issues a certificate, it is providing a statement to a certificate user (i.e., a relying party) that a particular public key is bound to the identity and/or other attributes of a particular entity (the certificate subject, which is usually also the subscriber). The extent to which the relying party should rely on that statement by the CA, however, needs to be assessed by the relying party or entity controlling or coordinating the way relying parties or relying party applications use certificates. Different certificates are issued following different practices and procedures, and may be suitable for different applications and/or purposes.

The X.509 standard defines a CP as "a named set of rules that indicates the applicability of a certificate to a particular

community and/or class of application with common security requirements" [ISO1]. An X.509 Version 3 certificate may identify a specific applicable CP, which may be used by a relying party to

decide whether or not to trust a certificate, associated public key, or any digital signatures verified using the public key for a particular purpose.

CPs typically fall into two major categories. First, some CPs "indicate the applicability of a certificate to a particular community" [ISO1]. These CPs set forth requirements for certificate usage and requirements on members of a community. For instance, a CP may focus on the needs of a geographical community, such as the ETSI policy requirements for CAs issuing qualified certificates [ETS]. Also, a CP of this kind may focus on the needs of a specific vertical-market community, such as financial services [IDT].

The second category of typical CPs "indicate the applicability of a certificate to a . . . class of application with common security requirements." These CPs identify a set of applications or uses for certificates and say that these applications or uses require a certain level of security. They then set forth PKI requirements that are appropriate for these applications or uses. A CP within this category often makes sets requirements appropriate for a certain "level of assurance" provided by certificates, relative to certificates issued pursuant to related CPs. These levels of assurance may correspond to "classes" or "types" of certificates.

For instance, the Government of Canada PKI Policy Management Authority (GOC PMA) has established eight certificate policies in a single document [GOC], four policies for certificates used for digital signatures and four policies for certificates used for confidentiality encryption. For each of these applications, the document establishes four levels of assurances: rudimentary, basic, medium, and high. The GOC PMA described certain types of digital signature and confidentiality uses in the document, each with a certain set of security requirements, and grouped them into eight categories. The GOC PMA then established PKI requirements for each of these categories, thereby creating eight types of certificates, each providing rudimentary, basic, medium, or high levels of assurance. The progression from rudimentary to high levels corresponds to increasing security requirements and corresponding increasing levels of assurance.

A CP is represented in a certificate by a unique number called an "Object Identifier" (OID). That OID, or at least an "arc", can be registered. An "arc" is the beginning of the numerical sequence of

an OID and is assigned to a particular organization. The registration process follows the procedures specified in ISO/IEC and ITU standards. The party that registers the OID or arc also can publish the text of the CP, for examination by relying parties. Any one certificate will typically declare a single CP or, possibly, be

issued consistent with a small number of different policies. Such declaration appears in the Certificate Policies extension of a X.509 Version 3 certificate. When a CA places multiple CPs within a certificate's Certificate Policies extension, the CA is asserting that the certificate is appropriate for use in accordance with any of the listed CPs.

CPs also constitute a basis for an audit, accreditation, or another assessment of a CA. Each CA can be assessed against one or more certificate policies or CPSs that it is recognized as implementing. When one CA issues a CA-certificate for another CA, the issuing CA must assess the set of certificate policies for which it trusts the subject CA (such assessment may be based upon an assessment with respect to the certificate policies involved). The assessed set of certificate policies is then indicated by the issuing CA in the CA-certificate. The X.509 certification path processing logic employs these CP indications in its well-defined trust model.

3.2. Certificate Policy Examples

For example purposes, suppose that the International Air Transport Association (IATA) undertakes to define some certificate policies for use throughout the airline industry, in a PKI operated by IATA in combination with PKIs operated by individual airlines. Two CPs might be defined - the IATA General-Purpose CP, and the IATA Commercial-Grade CP.

The IATA General-Purpose CP could be used by industry personnel for protecting routine information (e.g., casual electronic mail) and for authenticating connections from World Wide Web browsers to servers for general information retrieval purposes. The key pairs may be generated, stored, and managed using low-cost, software-based systems, such as commercial browsers. Under this policy, a certificate may be automatically issued to anybody listed as an employee in the corporate directory of IATA or any member airline who submits a signed certificate request form to a network administrator in his or her organization.

The IATA Commercial-Grade CP could be used to protect financial transactions or binding contractual exchanges between airlines. Under this policy, IATA could require that certified key pairs be generated and stored in approved cryptographic hardware tokens. Certificates and tokens could be provided to airline employees with

disbursement authority. These authorized individuals might then be required to present themselves to the corporate security office, show a valid identification badge, and sign a subscriber agreement requiring them to protect the token and use it only for authorized purposes, as a condition of being issued a token and a certificate.

3.3. X.509 Certificate Fields

The following extension fields in an X.509 certificate are used to support CPs:

- * Certificate Policies extension;
- * Policy Mappings extension; and
- * Policy Constraints extension.

3.3.1. Certificate Policies Extension

A Certificate Policies field lists CPs that the certification authority declares are applicable. Using the example of the IATA General-Purpose and Commercial-Grade policies defined in Section 3.2, the certificates issued to regular airline employees would contain the object identifier for General-Purpose policy. The certificates issued to the employees with disbursement authority would contain the object identifiers for both the General-Purpose policy and the Commercial-Grade policy. The inclusion of both object identifiers in the certificates means that they would be appropriate for either the General-Purpose or Commercial-Grade policies. The Certificate Policies field may also optionally convey qualifier values for each identified policy; the use of qualifiers is discussed in Section 3.4.

When processing a certification path, a CP that is acceptable to the relying party application must be present in every certificate in the path, i.e., in CA-certificates as well as end entity certificates.

If the Certificate Policies field is flagged critical, it serves the same purpose as described above but also has an additional role. Specifically, it indicates that the use of the certificate is restricted to one of the identified policies, i.e., the certification authority is declaring that the certificate must only be used in accordance with the provisions of at least one of the listed CPs. This field is intended to protect the certification authority against claims for damages asserted by a relying party who has used the certificate for an inappropriate purpose or in an inappropriate manner, as stipulated in the applicable CP.

For example, the Internal Revenue Service might issue certificates to taxpayers for the purpose of protecting tax filings. The Internal Revenue Service understands and can accommodate the risks of erroneously issuing a bad certificate, e.g., to an imposter.

Suppose, however, that someone used an Internal Revenue Service tax-filing certificate as the basis for encrypting multi-million-dollar-value proprietary trade secrets, which subsequently fell into the wrong hands because of a cryptanalytic attack by an attacker who is able to decrypt the message. The Internal Revenue Service may want

to defend itself against claims for damages in such circumstances by pointing to the criticality of the Certificate Policies extension to show that the subscriber and relying party misused the certificate. The critical-flagged Certificate Policies extension is intended to mitigate the risk to the CA in such situations.

3.3.2. Policy Mappings Extension

The Policy Mappings extension may only be used in CA-certificates. This field allows a certification authority to indicate that certain policies in its own domain can be considered equivalent to certain other policies in the subject certification authority's domain.

For example, suppose that for purposes of facilitating interoperability, the ACE Corporation establishes an agreement with the ABC Corporation to cross-certify the public keys of each others' certification authorities for the purposes of mutually securing their respective business-to-business exchanges. Further, suppose that both companies have pre-existing financial transaction protection policies called ace-e-commerce and abc-e-commerce, respectively. One can see that simply generating cross-certificates between the two domains will not provide the necessary interoperability, as the two companies' applications are configured with, and employee certificates are populated with, their respective certificate policies. One possible solution is to reconfigure all of the financial applications to require either policy and to reissue all the certificates with both policies appearing in their Certificate Policies extensions. Another solution, which may be easier to administer, uses the Policy Mapping field. If this field is included in a cross-certificate for the ABC Corporation certification authority issued by the ACE Corporation certification authority, it can provide a statement that the ABC's financial transaction protection policy (i.e., abc-e-commerce) can be considered equivalent to that of the ACE Corporation (i.e., ace-e-commerce). With such a statement included in the cross-certificate issued to ABC, relying party applications in the ACE domain requiring the presence of the object identifier for the ace-e-commerce CP can also accept, process, and rely upon certificates issued within the ABC domain containing the object identifier for the abc-e-commerce CP.

3.3.3. Policy Constraints Extension

The Policy Constraints extension supports two optional features. The

first is the ability for a certification authority to require that explicit CP indications be present in all subsequent certificates in a certification path. Certificates at the start of a certification path may be considered by a relying party to be part of a trusted domain, i.e., certification authorities are trusted for all purposes

so no particular CP is needed in the Certificate Policies extension. Such certificates need not contain explicit indications of CP. When a certification authority in the trusted domain, however, certifies outside the domain, it can activate the requirement that a specific CP's object identifier appear in subsequent certificates in the certification path.

The other optional feature in the Policy Constraints field is the ability for a certification authority to disable policy mapping by subsequent certification authorities in a certification path. It may be prudent to disable policy mapping when certifying outside the domain. This can assist in controlling risks due to transitive trust, e.g., a domain A trusts domain B, domain B trusts domain C, but domain A does not want to be forced to trust domain C.

3.3.4. Policy Qualifiers

The Certificate Policies extension field has a provision for conveying, along with each CP identifier, additional policy-dependent information in a qualifier field. The X.509 standard does not mandate the purpose for which this field is to be used, nor does it prescribe the syntax for this field. Policy qualifier types can be registered by any organization.

The following policy qualifier types are defined in PKIX RFC 3280 [PKI1]:

- (a) The CPS Pointer qualifier contains a pointer to a CPS, CPS Summary, RPA, or PDS published by the CA. The pointer is in the form of a uniform resource identifier (URI).
- (b) The User Notice qualifier contains a text string that is to be displayed to subscribers and relying parties prior to the use of the certificate. The text string may be an IA5String or a BMPString - a subset of the ISO 100646-1 multiple octet coded character set. A CA may invoke a procedure that requires that the relying party acknowledge that the applicable terms and conditions have been disclosed and/or accepted.

Policy qualifiers can be used to support the definition of generic, or parameterized, CPs. Provided the base CP so provides, policy qualifier types can be defined to convey, on a per-certificate basis, additional specific policy details that fill in the generic

definition.

3.4. Certification Practice Statement

The term certification practice statement (CPS) is defined by the DSG and PAG as: "A statement of the practices which a certification authority employs in issuing certificates." [ABA1, ABA2] As stated above, a CPS establishes practices concerning lifecycle services in addition to issuance, such as certificate management (including publication and archiving), revocation, and renewal or re-keying. In the DSG, the ABA expands this definition with the following comments:

"A certification practice statement may take the form of a declaration by the certification authority of the details of its trustworthy system and the practices it employs in its operations and in support of issuance of a certificate . . ." This form of CPS is the most common type, and can vary in length and level of detail.

Some PKIs may not have the need to create a thorough and detailed statement of practices. For example, the CA may itself be the relying party and would already be aware of the nature and trustworthiness of its services. In other cases, a PKI may provide certificates providing only a very low level of assurances where the applications being secured may pose only marginal risks if compromised. In these cases, an organization establishing a PKI may only want to write or have CAs use a subscriber agreement, relying party agreement, or agreement combining subscriber and relying party terms, depending on the role of the different PKI participants. In such a PKI, that agreement may serve as the only "statement of practices" used by one or more CAs within that PKI. Consequently, that agreement may also be considered a CPS and can be entitled or subtitled as such.

Likewise, since a detailed CPS may contain sensitive details of its system, a CA may elect not to publish its entire CPS. It may instead opt to publish a CPS Summary (or CPS Abstract). The CPS Summary would contain only those provisions from the CPS that the CA considers to be relevant to the participants in the PKI (such as the responsibilities of the parties or the stages of the certificate lifecycle). A CPS Summary, however, would not contain those sensitive provisions of the full CPS that might provide an attacker with useful information about the CA's operations. Throughout this document, the use of "CPS" includes both a detailed CPS and a CPS Summary (unless otherwise specified).

CPSs do not automatically constitute contracts and do not automatically bind PKI participants as a contract would. Where a document serves the dual purpose of being a subscriber or relying party agreement and CPS, the document is intended to be a contract and constitutes a binding contract to the extent that a subscriber or

relying party agreement would ordinarily be considered as such. Most CPSs, however, do not serve such a dual purpose. Therefore, in most cases, a CPS's terms have a binding effect as contract terms only if a separate document creates a contractual relationship between the parties and that document incorporates part or all of the CPS by reference. Further, if a particular PKI employs a CPS Summary (as opposed to the entire CPS), the CPS Summary could be incorporated into any applicable subscriber or relying party agreement.

In the future, a court or applicable statutory or regulatory law may declare that a certificate itself is a document that is capable of creating a contractual relationship, to the extent its mechanisms designed for incorporation by reference (such as the Certificate Policies extension and its qualifiers) indicate that terms of its use appear in certain documents. In the meantime, however, some subscriber agreements and relying party agreements may incorporate a CPS by reference and therefore make its terms binding on the parties to such agreements.

3.5. Relationship Between Certificate Policy and Certification Practice Statement

The CP and CPS address the same set of topics that are of interest to the relying party in terms of the degree to and purpose for which a public key certificate should be trusted. Their primary difference is in the focus of their provisions. A CP sets forth the requirements and standards imposed by the PKI with respect to the various topics. In other words, the purpose of the CP is to establish what participants must do. A CPS, by contrast, states how a CA and other participants in a given domain implement procedures and controls to meet the requirements stated in the CP. In other words, the purpose of the CPS is to disclose how the participants perform their functions and implement controls.

An additional difference between a CP and CPS relates the scope of coverage of the two kinds of documents. Since a CP is a statement of requirements, it best serves as the vehicle for communicating minimum operating guidelines that must be met by interoperating PKIs. Thus, a CP generally applies to multiple CAs, multiple organizations, or multiple domains. By contrast, a CPS applies only to a single CA or single organization and is not generally a vehicle to facilitate interoperation.

A CA with a single CPS may support multiple CPs (used for different application purposes and/or by different relying party communities). Also, multiple CAs, with non-identical CPSs, may support the same CP.

For example, the Federal Government might define a government-wide CP for handling confidential human resources information. The CP will be a broad statement of the general requirements for participants within the Government's PKI, and an indication of the types of applications for which it is suitable for use. Each department or agency wishing to operate a certification authority in this PKI may be required to write its own certification practice statement to support this CP by explaining how it meets the requirements of the CP. At the same time, a department's or agency's CPS may support other certificate policies.

An additional difference between a CP and CPS concerns the level of detail of the provisions in each. Although the level of detail may vary among CPSs, a CPS will generally be more detailed than a CP. A CPS provides a detailed description of procedures and controls in place to meet the CP requirements, while a CP is more general.

The main differences between CPs and CPSs can therefore be summarized as follows:

- (a) A PKI uses a CP to establish requirements that state what participants within it must do. A single CA or organization can use a CPS to disclose how it meets the requirements of a CP or how it implements its practices and controls.
- (b) A CP facilitates interoperation through cross-certification, unilateral certification, or other means. Therefore, it is intended to cover multiple CAs. By contrast, a CPS is a statement of a single CA or organization. Its purpose is not to facilitate interoperation (since doing so is the function of a CP).
- (c) A CPS is generally more detailed than a CP and specifies how the CA meets the requirements specified in the one or more CPs under which it issues certificates.

In addition to populating the certificate policies extension with the applicable CP object identifier, a certification authority may include, in certificates it issues, a reference to its certification practice statement. A standard way to do this, using a CP qualifier, is described in Section 3.4.

3.6. Relationship Among CPs, CPSs, Agreements, and Other Documents

CPs and CPSs play a central role in documenting the requirements and practices of a PKI. Nonetheless, they are not the only documents relevant to a PKI. For instance, subscriber agreements and relying party agreements play a critical role in allocating responsibilities

to subscribers and relying parties relating to the use of certificates and key pairs. They establish the terms and conditions under which certificates are issued, managed, and used. The term subscriber agreement is defined by the PAG as: "An agreement between a CA and a subscriber that establishes the right and obligations of the parties regarding the issuance and management of certificates." [ABA2] The PAG defines a relying party agreement as: "An agreement between a certification authority and relying party that typically establishes the rights and obligations between those parties regarding the verification of digital signatures or other uses of certificates." [ABA2]

As mentioned in Section 3.5, a subscriber agreement, relying party agreement, or an agreement that combines subscriber and relying party terms may also serve as a CPS. In other PKIs, however, a subscriber or relying party agreement may incorporate some or all of the terms of a CP or CPS by reference. Yet other PKIs may distill from a CP and/or CPS the terms that are applicable to a subscriber and place such terms in a self-contained subscriber agreement, without incorporating a CP or CPS by reference. They may use the same method to distill relying party terms from a CP and/or CPS and place such terms in a self-contained relying party agreement. Creating such self-contained agreements has the advantage of creating documents that are easier for consumers to review. In some cases, subscribers or relying parties may be deemed to be "consumers" under applicable law, who are subject to certain statutory or regulatory protections. Under the legal systems of civil law countries, incorporating a CP or CPS by reference may not be effective to bind consumers to the terms of an incorporated CP or CPS.

CPs and CPSs may be incorporated by reference in other documents, including:

- * Interoperability agreements (including agreements between CAs for cross-certification, unilateral certification, or other forms of interoperation),
- * Vendor agreements (under which a PKI vendor agrees to meet standards set forth in a CP or CPS), or
- * A PDS. See [ABA2]

A PDS serves a similar function to a CPS Summary. It is a relatively

short document containing only a subset of critical details about a PKI or CA. It may differ from a CPS Summary, however, in that its purpose is to act as a summary of information about the overall nature of the PKI, as opposed to simply a condensed form of the CPS.

Moreover, its purpose is to distill information about the PKI, as opposed to protecting security sensitive information contained in an unpublished CPS, although a PDS could also serve that function.

Just as writers may wish to refer to a CP or CPS or incorporate it by reference in an agreement or PDS, a CP or CPS may refer to other documents when establishing requirements or making disclosures. For instance, a CP may set requirements for certificate content by referring to an external document setting forth a standard certificate profile. Referencing external documents permits a CP or CPS to impose detailed requirements or make detailed disclosures without having to reprint lengthy provisions from other documents within the CP or CPS. Moreover, referencing a document in a CP or CPS is another useful way of dividing disclosures between public information and security sensitive confidential information (in addition to or as an alternative to publishing a CPS Summary). For example, a PKI may want to publish a CP or CPS, but maintain site construction parameters for CA high security zones as confidential information. In that case, the CP or CPS could reference an external manual or document containing the detailed site construction parameters.

Documents that a PKI may wish to refer to in a CP or CPS include:

- * A security policy,
- * Training, operational, installation, and user manuals (which may contain operational requirements),
- * Standards documents that apply to particular aspects of the PKI (such as standards specifying the level of protection offered by any hardware tokens used in the PKI or standards applicable to the site construction),
- * Key management plans,
- * Human resource guides and employment manuals (which may describe some aspects of personnel security practices), and
- * E-mail policies (which may discuss subscriber and relying party responsibilities, as well as the implications of key management, if applicable). See [ABA2]

3.7. Set of Provisions

A set of provisions is a collection of practice and/or policy statements, spanning a range of standard topics for use in expressing a CP or CPS employing the approach described in this framework by covering the topic appearing in Section 5 below. They are also described in detail in Section 4 below.

A CP can be expressed as a single set of provisions.

A CPS can be expressed as a single set of provisions with each component addressing the requirements of one or more certificate policies, or, alternatively, as an organized collection of sets of provisions. For example, a CPS could be expressed as a combination of the following:

- (a) a list of certificate policies supported by the CPS;
- (b) for each CP in (a), a set of provisions that contains statements responding to that CP by filling in details not stipulated in that policy or expressly left to the discretion of the CA (in its CPS) ; such statements serve to state how this particular CPS implements the requirements of the particular CP; or
- (c) a set of provisions that contains statements regarding the certification practices on the CA, regardless of CP.

The statements provided in (b) and (c) may augment or refine the stipulations of the applicable CP, but generally must not conflict with any of the stipulations of such CP. In certain cases, however, a policy authority may permit exceptions to the requirements in a CP, because certain compensating controls of the CA are disclosed in its CPS that allow the CA to provide assurances that are equivalent to the assurances provided by CAs that are in full compliance with the CP.

This framework outlines the contents of a set of provisions, in terms of nine primary components, as follows:

1. Introduction
2. Publication and Repository
3. Identification and Authentication
4. Certificate Life-Cycle Operational Requirements

5. Facilities, Management, and Operational Controls
6. Technical Security Controls
7. Certificate, CRL, and OCSP Profile
8. Compliance audit
9. Other Business and Legal Matters

Chokhani, et al.

Informational

[Page 20]

PKIs can use this simple framework of nine primary components to write a simple CP or CPS. Moreover, a CA can use this same framework to write a subscriber agreement, relying party agreement, or agreement containing subscriber and relying party terms. If a CA uses this simple framework to construct an agreement, it can use paragraph 1 as an introduction or recitals, it can set forth the responsibilities of the parties in paragraphs 2-8, and it can use paragraph 9 to cover the business and legal issues described in more detail, using the ordering of Section 4.9 below (such as representations and warranties, disclaimers, and liability limitations). The ordering of topics in this simple framework and the business and legal matters Section 4.9 is the same as (or similar to) the ordering of topics in a typical software or other technology agreement. Therefore, a PKI can establish a set of core documents (with a CP, CPS, subscriber agreement, and relying party agreement) all having the same structure and ordering of topics, thereby facilitating comparisons and mappings among these documents and among the corresponding documents of other PKIs.

This simple framework may also be useful for agreements other than subscriber agreements and relying party agreements. For instance, a CA wishing to outsource certain services to an RA or certificate manufacturing authority (CMA) may find it useful to use this framework as a checklist to write a registration authority agreement or outsourcing agreement. Similarly, two CAs may wish to use this simple framework for the purpose of drafting a cross-certification, unilateral certification, or other interoperability agreement.

In short, the primary components of the simple framework (specified above) may meet the needs of drafters of short CPs, CPSs, subscriber agreements, and relying party agreements. Nonetheless, this framework is extensible, and its coverage of the nine components is flexible enough to meet the needs of drafters of comprehensive CPs and CPSs. Specifically, components appearing above can be further divided into subcomponents, and a subcomponent may comprise multiple elements. Section 4 provides a more detailed description of the contents of the above components, and their subcomponents. Drafters of CPs and CPSs are permitted to add additional levels of subcomponents below the subcomponents described in Section 4 for the purpose of meeting the needs of the drafter's particular PKI.

4. Contents of a Set of Provisions

This section expands upon the contents of the simple framework of provisions, as introduced in Section 3.7. The topics identified in this section are, consequently, candidate topics for inclusion in a detailed CP or CPS.

While many topics are identified, it is not necessary for a CP or a CPS to include a concrete statement for every such topic. Rather, a particular CP or CPS may state "no stipulation" for a component, subcomponent, or element on which the particular CP or CPS imposes no requirements or makes no disclosure. In this sense, the list of topics can be considered a checklist of topics for consideration by the CP or CPS writer.

It is recommended that each and every component and subcomponent be included in a CP or CPS, even if there is "no stipulation"; this will indicate to the reader that a conscious decision was made to include or exclude a provision concerning that topic. This drafting style protects against inadvertent omission of a topic, while facilitating comparison of different certificate policies or CPSs, e.g., when making policy mapping decisions.

In a CP, it is possible to leave certain components, subcomponents, and/or elements unspecified, and to stipulate that the required information will be indicated in a policy qualifier, or the document to which a policy qualifier points. Such CPs can be considered parameterized definitions. The set of provisions should reference or define the required policy qualifier types and should specify any applicable default values.

4.1. Introductions

This component identifies and introduces the set of provisions, and indicates the types of entities and applications for which the document (either the CP or the CPS being written) is targeted.

4.1.1. Overview

This subcomponent provides a general introduction to the document being written. This subcomponent can also be used to provide a synopsis of the PKI to which the CP or CPS applies. For example, it may set out different levels of assurance provided by certificates within the PKI. Depending on the complexity and scope of the particular PKI, a diagrammatic representation of the PKI might be useful here.

4.1.2. Document Name and Identification

This subcomponent provides any applicable names or other identifiers,

including ASN.1 object identifiers, for the document. An example of such a document name would be the US Federal Government Policy for Secure E-mail.

4.1.3. PKI Participants

This subcomponent describes the identity or types of entities that fill the roles of participants within a PKI, namely:

- * Certification authorities, i.e., the entities that issue certificates. A CA is the issuing CA with respect to the certificates it issues and is the subject CA with respect to the CA certificate issued to it. CAs may be organized in a hierarchy in which an organization's CA issues certificates to CAs operated by subordinate organizations, such as a branch, division, or department within a larger organization.
- * Registration authorities, i.e., the entities that establish enrollment procedures for end-user certificate applicants, perform identification and authentication of certificate applicants, initiate or pass along revocation requests for certificates, and approve applications for renewal or re-keying certificates on behalf of a CA. Subordinate organizations within a larger organization can act as RAs for the CA serving the entire organization, but RAs may also be external to the CA.
- * Subscribers. Examples of subscribers who receive certificates from a CA include employees of an organization with its own CA, banking or brokerage customers, organizations hosting e-commerce sites, organizations participating in a business-to-business exchange, and members of the public receiving certificates from a CA issuing certificates to the public at large.
- * Relying parties. Examples of relying parties include employees of an organization having its own CA who receive digitally signed e-mails from other employees, persons buying goods and services from e-commerce sites, organizations participating in a business-to-business exchange who receive bids or orders from other participating organizations, and individuals and organizations doing business with subscribers who have received their certificates from a CA issuing certificates to the public. Relying parties may or may not also be subscribers within a given PKI.
- * Other participants, such as certificate manufacturing authorities, providers of repository services, and other entities providing PKI-related services.

4.1.4. Certificate Usage

This subcomponent contains:

- * A list or the types of applications for which the issued certificates are suitable, such as electronic mail, retail transactions, contracts, and a travel order, and/or
- * A list or the types of applications for which use of the issued certificates is prohibited.

In the case of a CP or CPS describing different levels of assurance, this subcomponent can describe applications or types of applications that are appropriate or inappropriate for the different levels of assurance.

4.1.5. Policy Administration

This subcomponent includes the name and mailing address of the organization that is responsible for the drafting, registering, maintaining, and updating of this CP or CPS. It also includes the name, electronic mail address, telephone number, and fax number of a contact person. As an alternative to naming an actual person, the document may name a title or role, an e-mail alias, and other generalized contact information. In some cases, the organization may state that its contact person, alone or in combination with others, is available to answer questions about the document.

Moreover, when a formal or informal policy authority is responsible for determining whether a CA should be allowed to operate within or interoperate with a PKI, it may wish to approve the CPS of the CA as being suitable for the policy authority's CP. If so, this subcomponent can include the name or title, electronic mail address (or alias), telephone number, fax number, and other generalized information of the entity in charge of making such a determination. Finally, in this case, this subcomponent also includes the procedures by which this determination is made.

4.1.6. Definitions and Acronyms

This subcomponent contains a list of definitions for defined terms used within the document, as well as a list of acronyms in the document and their meanings.

4.2. Publication and Repository Responsibilities

This component contains any applicable provisions regarding:

- * An identification of the entity or entities that operate repositories within the PKI, such as a CA, certificate manufacturing authority, or independent repository service provider;
- * The responsibility of a PKI participant to publish information regarding its practices, certificates, and the current status of such certificates, which may include the responsibilities of making the CP or CPS publicly available using various mechanisms and of identifying components, subcomponents, and elements of such documents that exist but are not made publicly available, for instance, security controls, clearance procedures, or trade secret information due to their sensitivity;
- * When information must be published and the frequency of publication; and
- * Access control on published information objects including CPs, CPS, certificates, certificate status, and CRLs.

4.3. Identification and Authentication

This component describes the procedures used to authenticate the identity and/or other attributes of an end-user certificate applicant to a CA or RA prior to certificate issuance. In addition, the component sets forth the procedures for authenticating the identity and the criteria for accepting applicants of entities seeking to become CAs, RAs, or other entities operating in or interoperating with a PKI. It also describes how parties requesting re-key or revocation are authenticated. This component also addresses naming practices, including the recognition of trademark rights in certain names.

4.3.1. Naming

This subcomponent includes the following elements regarding naming and identification of the subscribers:

- * Types of names assigned to the subject, such as X.500

distinguished names; RFC-822 names; and X.400 names;

* Whether names have to be meaningful or not;(3)

- * Whether or not subscribers can be anonymous or pseudonymous, and if they can, what names are assigned to or can be used by anonymous subscribers;
- * Rules for interpreting various name forms, such as the X.500 standard and RFC-822;
- * Whether names have to be unique; and
- * Recognition, authentication, and the role of trademarks.

4.3.2. Initial Identity Validation

This subcomponent contains the following elements for the identification and authentication procedures for the initial registration for each subject type (CA, RA, subscriber, or other participant):

- * If and how the subject must prove possession of the companion private key for the public key being registered, for example, a digital signature in the certificate request message;(4)
- * Identification and authentication requirements for organizational identity of subscriber or participant (CA; RA; subscriber (in the case of certificates issued to organizations or devices controlled by an organization), or other participant), for example, consulting the database of a service that identifies organizations or inspecting an organization's articles of incorporation;
- * Identification and authentication requirements for an individual subscriber or a person acting on behalf of an organizational subscriber or participant (CA, RA, in the case of certificates issued to organizations or devices controlled by an organization, the subscriber, or other participant),(5) including:
 - * Type of documentation and/or number of identification credentials required;
 - * How a CA or RA authenticates the identity of the organization or individual based on the documentation or credentials provided;
 - * If the individual must personally present to the authenticating

CA or RA;

- * How an individual as an organizational person is authenticated, such as by reference to duly signed authorization documents or a corporate identification badge.

- * List of subscriber information that is not verified (called "non-verified subscriber information") during the initial registration;
- * Validation of authority involves a determination of whether a person has specific rights, entitlements, or permissions, including the permission to act on behalf of an organization to obtain a certificate; and
- * In the case of applications by a CA wishing to operate within, or interoperate with, a PKI, this subcomponent contains the criteria by which a PKI, CA, or policy authority determines whether or not the CA is suitable for such operations or interoperation. Such interoperation may include cross-certification, unilateral certification, or other forms of interoperation.

4.3.3. Identification and Authentication for Re-key Requests

This subcomponent addresses the following elements for the identification and authentication procedures for re-key for each subject type (CA, RA, subscriber, and other participants):

- * Identification and authentication requirements for routine re-key, such as a re-key request that contains the new key and is signed using the current valid key; and
- * Identification and authentication requirements for re-key after certificate revocation. One example is the use of the same process as the initial identity validation.

4.3.4. Identification and Authentication for Revocation Requests

This subcomponent describes the identification and authentication procedures for a revocation request by each subject type (CA, RA, subscriber, and other participant). Examples include a revocation request digitally signed with the private key whose companion public key needs to be revoked, and a digitally signed request by the RA.

4.4. Certificate Life-Cycle Operational Requirements

This component is used to specify requirements imposed upon issuing CA, subject CAs, RAs, subscribers, or other participants with respect to the life-cycle of a certificate.

Within each subcomponent, separate consideration may need to be given to subject CAs, RAs, subscribers, and other participants.

4.4.1. Certificate Application

This subcomponent is used to address the following requirements regarding subject certificate application:

- * Who can submit a certificate application, such as a certificate subject or the RA; and
- * Enrollment process used by subjects to submit certificate applications and responsibilities in connection with this process. An example of this process is where the subject generates the key pair and sends a certificate request to the RA. The RA validates and signs the request and sends it to the CA. A CA or RA may have the responsibility of establishing an enrollment process in order to receive certificate applications. Likewise, certificate applicants may have the responsibility of providing accurate information on their certificate applications.

4.4.2. Certificate Application Processing

This subcomponent is used to describe the procedure for processing certificate applications. For example, the issuing CA and RA may perform identification and authentication procedures to validate the certificate application. Following such steps, the CA or RA will either approve or reject the certificate application, perhaps upon the application of certain criteria. Finally, this subcomponent sets a time limit during which a CA and/or RA must act on and process a certificate application.

4.4.3. Certificate Issuance

This subcomponent is used to describe the following certificate issuance related elements:

- * Actions performed by the CA during the issuance of the certificate, for example a procedure whereby the CA validates the RA signature and RA authority and generates a certificate; and
- * Notification mechanisms, if any, used by the CA to notify the subscriber of the issuance of the certificate; an example is a procedure under which the CA e-mails the certificate to the subscriber or the RA or e-mails information permitting the subscriber to download the certificate from a web site.

4.4.4. Certificate Acceptance

This subcomponent addresses the following:

- * The conduct of an applicant that will be deemed to constitute acceptance of the certificate. Such conduct may include affirmative steps to indicate acceptance, actions implying acceptance, or a failure to object to the certificate or its content. For instance, acceptance may be deemed to occur if the CA does not receive any notice from the subscriber within a certain time period; a subscriber may send a signed message accepting the certificate; or a subscriber may send a signed message rejecting the certificate where the message includes the reason for rejection and identifies the fields in the certificate that are incorrect or incomplete.
- * Publication of the certificate by the CA. For example, the CA may post the certificate to an X.500 or LDAP repository.
- * Notification of certificate issuance by the CA to other entities. As an example, the CA may send the certificate to the RA.

4.4.5. Key Pair and Certificate Usage

This subcomponent is used to describe the responsibilities relating to the use of keys and certificates, including:

- * Subscriber responsibilities relating to use of the subscriber's private key and certificate. For example, the subscriber may be required to use a private key and certificate only for appropriate applications as set forth in the CP and in consistency with applicable certificate content (e.g., key usage field). Use of a private key and certificate are subject to the terms of the subscriber agreement, the use of a private key is permitted only after the subscriber has accepted the corresponding certificate, or the subscriber must discontinue use of the private key following the expiration or revocation of the certificate.
- * Relying party responsibilities relating to the use of a subscriber's public key and certificate. For instance, a relying party may be obligated to rely on certificates only for appropriate applications as set forth in the CP and in consistency with applicable certificate content (e.g., key usage field),

successfully perform public key operations as a condition of relying on a certificate, assume responsibility to check the status of a certificate using one of the required or permitted

mechanisms set forth in the CP/CPS (see Section 4.4.9 below), and assent to the terms of the applicable relying party agreement as a condition of relying on the certificate.

4.4.6. Certificate Renewal

This subcomponent is used to describe the following elements related to certificate renewal. Certificate renewal means the issuance of a new certificate to the subscriber without changing the subscriber or other participant's public key or any other information in the certificate:

- * Circumstances under which certificate renewal takes place, such as where the certificate life has expired, but the policy permits the same key pair to be reused;
- * Who may request certificate renewal, for instance, the subscriber, RA, or the CA may automatically renew an end-user subscriber certificate;
- * A CA or RA's procedures to process renewal requests to issue the new certificate, for example, the use of a token, such as a password, to re-authenticate the subscriber, or procedures that are the same as the initial certificate issuance;
- * Notification of the new certificate to the subscriber;
- * Conduct constituting acceptance of the certificate;
- * Publication of the certificate by the CA; and
- * Notification of certificate issuance by the CA to other entities.

4.4.7. Certificate Re-key

This subcomponent is used to describe the following elements related to a subscriber or other participant generating a new key pair and applying for the issuance of a new certificate that certifies the new public key:

- * Circumstances under which certificate re-key can or must take place, such as after a certificate is revoked for reasons of key compromise or after a certificate has expired and the usage period

of the key pair has also expired;

* Who may request certificate re-key, for example, the subscriber;

- * A CA or RA's procedures to process re-keying requests to issue the new certificate, such as procedures that are the same as the initial certificate issuance;
- * Notification of the new certificate to the subscriber;
- * Conduct constituting acceptance of the certificate;
- * Publication of the certificate by the CA; and
- * Notification of certificate issuance by the CA to other entities.

4.4.8. Certificate Modification

This subcomponent is used to describe the following elements related to the issuance of a new certificate (6) due to changes in the information in the certificate other than the subscriber public key:

- * Circumstances under which certificate modification can take place, such as name change, role change, reorganization resulting in a change in the DN;
- * Who may request certificate modification, for instance, subscribers, human resources personnel, or the RA;
- * A CA or RA's procedures to process modification requests to issue the new certificate, such as procedures that are the same as the initial certificate issuance;
- * Notification of the new certificate to the subscriber;
- * Conduct constituting acceptance of the certificate;
- * Publication of the certificate by the CA; and
- * Notification of certificate issuance by the CA to other entities.

4.4.9. Certificate Revocation and Suspension

This subcomponent addresses the following:

- * Circumstances under which a certificate may be suspended and circumstances under which it must be revoked, for instance, in

cases of subscriber employment termination, loss of cryptographic token, or suspected compromise of the private key;

- * Who can request the revocation of the participant's certificate, for example, the subscriber, RA, or CA in the case of an end-user subscriber certificate.
- * Procedures used for certificate revocation request, such as a digitally signed message from the RA, a digitally signed message from the subscriber, or a phone call from the RA;
- * The grace period available to the subscriber, within which the subscriber must make a revocation request;
- * The time within which CA must process the revocation request;
- * The mechanisms, if any, that a relying party may use or must use in order to check the status of certificates on which they wish to rely;
- * If a CRL mechanism is used, the issuance frequency;
- * If a CRL mechanism is used, maximum latency between the generation of CRLs and posting of the CRLs to the repository (in other words, the maximum amount of processing- and communication-related delays in posting CRLs to the repository after the CRLs are generated);
- * On-line revocation/status checking availability, for instance, OCSP and a web site to which status inquiries can be submitted;
- * Requirements on relying parties to perform on-line revocation/status checks;
- * Other forms of revocation advertisements available;
- * Any variations of the above stipulations for which suspension or revocation is the result of private key compromise (as opposed to other reasons for suspension or revocation).
- * Circumstances under which a certificate may be suspended;
- * Who can request the suspension of a certificate, for example, the subscriber, human resources personnel, a supervisor of the subscriber, or the RA in the case of an end-user subscriber certificate;

- * Procedures to request certificate suspension, such as a digitally signed message from the subscriber or RA, or a phone call from the RA; and
- * How long the suspension may last.

4.4.10. Certificate Status Services

This subcomponent addresses the certificate status checking services available to the relying parties, including:

- * The operational characteristics of certificate status checking services;
- * The availability of such services, and any applicable policies on unavailability; and
- * Any optional features of such services.

4.4.11. End of Subscription

This subcomponent addresses procedures used by the subscriber to end subscription to the CA services, including:

- * The revocation of certificates at the end of subscription (which may differ, depending on whether the end of subscription was due to the expiration of the certificate or termination of the service).

4.4.12. Key Escrow and Recovery

This subcomponent contains the following elements to identify the policies and practices relating to the escrowing, and/or recovery of private keys where private key escrow services are available (through the CA or other trusted third parties):

- * Identification of the document containing private key escrow and recovery policies and practices or a listing of such policies and practices; and
- * Identification of the document containing session key encapsulation and recovery policies and practices or a listing of such policies and practices.

4.5. Management, Operational, and Physical Controls

This component describes non-technical security controls (that is, physical, procedural, and personnel controls) used by the issuing CA to securely perform the functions of key generation, subject

authentication, certificate issuance, certificate revocation, auditing, and archiving.

This component can also be used to define non-technical security controls on repositories, subject CAs, RAs, subscribers, and other participants. The non-technical security controls for the subject CAs, RAs, subscribers, and other participants could be the same, similar, or very different.

These non-technical security controls are critical to trusting the certificates since lack of security may compromise CA operations resulting for example, in the creation of certificates or CRLs with erroneous information or compromising the CA private key.

Within each subcomponent, separate consideration will, in general, need to be given to each entity type, that is, the issuing CA, repository, subject CAs, RAs, subscribers, and other participants.

4.5.1. Physical Security Controls

In this subcomponent, the physical controls on the facility housing the entity systems are described. Topics addressed may include:

- * Site location and construction, such as the construction requirements for high-security zones and the use of locked rooms, cages, safes, and cabinets;
- * Physical access, i.e., mechanisms to control access from one area of the facility to another or access into high-security zones, such as locating CA operations in a secure computer room monitored by guards or security alarms and requiring movement from zone to zone to be accomplished using a token, biometric readers, and/or access control lists;
- * Power and air conditioning;
- * Water exposures;
- * Fire prevention and protection;
- * Media storage, for example, requiring the storage of backup media in a separate location that is physically secure and protected from fire and water damage;
- * Waste disposal; and

* Off-site backup.

Chokhani, et al.

Informational

[Page 34]

4.5.2. Procedural Controls

In this subcomponent, requirements for recognizing trusted roles are described, together with the responsibilities for each role.

Examples of trusted roles include system administrators, security officers, and system auditors.

For each task identified, the number of individuals required to perform the task (n out m rule) should be stated for each role. Identification and authentication requirements for each role may also be defined.

This component also includes the separation of duties in terms of the roles that cannot be performed by the same individuals.

4.5.3. Personnel Security Controls

This subcomponent addresses the following:

- * Qualifications, experience, and clearances that personnel must have as a condition of filling trusted roles or other important roles. Examples include credentials, job experiences, and official government clearances that candidates for these positions must have before being hired;
- * Background checks and clearance procedures that are required in connection with the hiring of personnel filling trusted roles or perhaps other important roles; such roles may require a check of their criminal records, references, and additional clearances that a participant undertakes after a decision has been made to hire a particular person;
- * Training requirements and training procedures for each role following the hiring of personnel;
- * Any retraining period and retraining procedures for each role after completion of initial training;
- * Frequency and sequence for job rotation among various roles;
- * Sanctions against personnel for unauthorized actions, unauthorized use of authority, and unauthorized use of entity systems for the purpose of imposing accountability on a participant's personnel;

* Controls on personnel that are independent contractors rather than employees of the entity; examples include:

- Bonding requirements on contract personnel;

- Contractual requirements including indemnification for damages due to the actions of the contractor personnel;
 - Auditing and monitoring of contractor personnel; and
 - Other controls on contracting personnel.
- * Documentation to be supplied to personnel during initial training, retraining, or otherwise.

4.5.4. Audit Logging Procedures

This subcomponent is used to describe event logging and audit systems, implemented for the purpose of maintaining a secure environment. Elements include the following:

- * Types of events recorded, such as certificate lifecycle operations, attempts to access the system, and requests made to the system;
- * Frequency with which audit logs are processed or archived, for example, weekly, following an alarm or anomalous event, or whenever the audit log is n% full;
- * Period for which audit logs are kept;
- * Protection of audit logs:
 - Who can view audit logs, for example only the audit administrator;
 - Protection against modification of audit logs, for instance a requirement that no one may modify or delete the audit records or that only an audit administrator may delete an audit file as part of rotating the audit file; and
 - Protection against deletion of audit logs.
- * Audit log back up procedures;
- * Whether the audit log accumulation system is internal or external to the entity;

- * Whether the subject who caused an audit event to occur is notified of the audit action; and

- * Vulnerability assessments, for example, where audit data is run through a tool that identifies potential attempts to breach the security of the system.

4.5.5. Records Archival

This subcomponent is used to describe general records archival (or records retention) policies, including the following:

- * Types of records that are archived, for example, all audit data, certificate application information, and documentation supporting certificate applications;
- * Retention period for an archive;
- * Protection of an archive:
 - Who can view the archive, for example, a requirement that only the audit administrator may view the archive;
 - Protection against modification of the archive, such as securely storing the data on a write once medium;
 - Protection against deletion of the archive;
 - Protection against the deterioration of the media on which the archive is stored, such as a requirement for data to be migrated periodically to fresh media; and
 - Protection against obsolescence of hardware, operating systems, and other software, by, for example, retaining as part of the archive the hardware, operating systems, and/or other software in order to permit access to and use of archived records over time.
- * Archive backup procedures;
- * Requirements for time-stamping of records;
- * Whether the archive collection system is internal or external; and
- * Procedures to obtain and verify archive information, such as a requirement that two separate copies of the archive data be kept

under the control of two persons, and that the two copies be compared in order to ensure that the archive information is accurate.

4.5.6. Key Changeover

This subcomponent describes the procedures to provide a new public key to a CA's users following a re-key by the CA. These procedures may be the same as the procedure for providing the current key. Also, the new key may be certified in a certificate signed using the old key.

4.5.7. Compromise and Disaster Recovery

This subcomponent describes requirements relating to notification and recovery procedures in the event of compromise or disaster. Each of the following may need to be addressed separately:

- * Identification or listing of the applicable incident and compromise reporting and handling procedures.
- * The recovery procedures used if computing resources, software, and/or data are corrupted or suspected to be corrupted. These procedures describe how a secure environment is re-established, which certificates are revoked, whether the entity key is revoked, how the new entity public key is provided to the users, and how the subjects are re-certified.
- * The recovery procedures used if the entity key is compromised. These procedures describe how a secure environment is re-established, how the new entity public key is provided to the users, and how the subjects are re-certified.
- * The entity's capabilities to ensure business continuity following a natural or other disaster. Such capabilities may include the availability of a remote hot-site at which operations may be recovered. They may also include procedures for securing its facility during the period of time following a natural or other disaster and before a secure environment is re-established, either at the original site or at a remote site. For example, procedures to protect against theft of sensitive materials from an earthquake-damaged site.

4.5.8. CA or RA Termination

This subcomponent describes requirements relating to procedures for termination and termination notification of a CA or RA, including the

identity of the custodian of CA and RA archival records.

Chokhani, et al.

Informational

[Page 38]

4.6. Technical Security Controls

This component is used to define the security measures taken by the issuing CA to protect its cryptographic keys and activation data (e.g., PINs, passwords, or manually-held key shares). This component may also be used to impose constraints on repositories, subject CAs, subscribers, and other participants to protect their private keys, activation data for their private keys, and critical security parameters. Secure key management is critical to ensure that all secret and private keys and activation data are protected and used only by authorized personnel.

This component also describes other technical security controls used by the issuing CA to perform securely the functions of key generation, user authentication, certificate registration, certificate revocation, auditing, and archiving. Technical controls include life-cycle security controls (including software development environment security, trusted software development methodology) and operational security controls.

This component can also be used to define other technical security controls on repositories, subject CAs, RAs, subscribers, and other participants.

4.6.1. Key Pair Generation and Installation

Key pair generation and installation need to be considered for the issuing CA, repositories, subject CAs, RAs, and subscribers. For each of these types of entities, the following questions potentially need to be answered:

1. Who generates the entity public, private key pair? Possibilities include the subscriber, RA, or CA. Also, how is the key generation performed? Is the key generation performed by hardware or software?
2. How is the private key provided securely to the entity? Possibilities include a situation where the entity has generated it and therefore already has it, handing the entity the private key physically, mailing a token containing the private key securely, or delivering it in an SSL session.
3. How is the entity's public key provided securely to the

certification authority? Some possibilities are in an online SSL session or in a message signed by the RA.

4. In the case of issuing CAs, how is the CA's public key provided securely to potential relying parties? Possibilities include handing the public key to the relying party securely in person, physically mailing a copy securely to the relying party, or delivering it in a SSL session.
5. What are the key sizes? Examples include a 1,024 bit RSA modulus and a 1,024 bit DSA large prime.
6. Who generates the public key parameters, and is the quality of the parameters checked during key generation?
7. For what purposes may the key be used, or for what purposes should usage of the key be restricted? For X.509 certificates, these purposes should map to the key usage flags in X.509 Version 3 certificates.

4.6.2. Private Key Protection and Cryptographic Module Engineering Controls

Requirements for private key protection and cryptographic modules need to be considered for the issuing CA, repositories, subject CAs, RAs, and subscribers. For each of these types of entities, the following questions potentially need to be answered:

1. What standards, if any, are required for the cryptographic module used to generate the keys? A cryptographic module can be composed of hardware, software, firmware, or any combination of them. For example, are the keys certified by the infrastructure required to be generated using modules compliant with the US FIPS 140-1? If so, what is the required FIPS 140-1 level of the module? Are there any other engineering or other controls relating to a cryptographic module, such as the identification of the cryptographic module boundary, input/output, roles and services, finite state machine, physical security, software security, operating system security, algorithm compliance, electromagnetic compatibility, and self tests.
2. Is the private key under n out of m multi-person control?(7) If yes, provide n and m (two person control is a special case of n out of m, where n = m = 2)?
3. Is the private key escrowed?(8) If so, who is the escrow agent,

what form is the key escrowed in (examples include plaintext, encrypted, split key), and what are the security controls on the escrow system?

Chokhani, et al.

Informational

[Page 40]

4. Is the private key backed up? If so, who is the backup agent, what form is the key backed up in (examples include plaintext, encrypted, split key), and what are the security controls on the backup system?
5. Is the private key archived? If so, who is the archival agent, what form is the key archived in (examples include plaintext, encrypted, split key), and what are the security controls on the archival system?
6. Under what circumstances, if any, can a private key be transferred into or from a cryptographic module? Who is permitted to perform such a transfer operation? In what form is the private key during the transfer (i.e., plaintext, encrypted, or split key)?
7. How is the private key stored in the module (i.e., plaintext, encrypted, or split key)?
8. Who can activate (use) the private key? What actions must be performed to activate the private key (e.g., login, power on, supply PIN, insert token/key, automatic, etc.)? Once the key is activated, is the key active for an indefinite period, active for one time, or active for a defined time period?
9. Who can deactivate the private key and how? Examples of methods of deactivating private keys include logging out, turning the power off, removing the token/key, automatic deactivation, and time expiration.
10. Who can destroy the private key and how? Examples of methods of destroying private keys include token surrender, token destruction, and overwriting the key.
11. Provide the capabilities of the cryptographic module in the following areas: identification of the cryptographic module boundary, input/output, roles and services, finite state machine, physical security, software security, operating system security, algorithm compliance, electromagnetic compatibility, and self tests. Capability may be expressed through reference to compliance with a standard such as U.S. FIPS 140-1, associated level, and rating.

4.6.3. Other Aspects of Key Pair Management

Other aspects of key management need to be considered for the issuing CA, repositories, subject CAs, RAs, subscribers, and other participants. For each of these types of entities, the following questions potentially need to be answered:

1. Is the public key archived? If so, who is the archival agent and what are the security controls on the archival system? Also, what software and hardware need to be preserved as part of the archive to permit use of the public key over time? Note: this subcomponent is not limited to requiring or describing the use of digital signatures with archival data, but rather can address integrity controls other than digital signatures when an archive requires tamper protection. Digital signatures do not provide tamper protection or protect the integrity of data; they merely verify data integrity. Moreover, the archival period may be greater than the cryptanalysis period for the public key needed to verify any digital signature applied to archival data.
2. What is the operational period of the certificates issued to the subscriber. What are the usage periods, or active lifetimes, for the subscriber's key pair?

4.6.4. Activation Data

Activation data refers to data values other than whole private keys that are required to operate private keys or cryptographic modules containing private keys, such as a PIN, passphrase, or portions of a private key used in a key-splitting scheme. Protection of activation data prevents unauthorized use of the private key, and potentially needs to be considered for the issuing CA, subject CAs, RAs, and subscribers. Such consideration potentially needs to address the entire life-cycle of the activation data from generation through archival and destruction. For each of the entity types (issuing CA, repository, subject CA, RA, subscriber, and other participants), all of the questions listed in 4.6.1 through 4.6.3 potentially need to be answered with respect to activation data rather than with respect to keys.

4.6.5. Computer Security Controls

This subcomponent is used to describe computer security controls such

as: use of the trusted computing base concept, discretionary access control, labels, mandatory access controls, object re-use, audit, identification and authentication, trusted path, security testing, and penetration testing. Product assurance may also be addressed.

A computer security rating for computer systems may be required. The rating could be based, for example, on the Trusted System Evaluation Criteria (TCSEC), Canadian Trusted Products Evaluation Criteria, European Information Technology Security Evaluation Criteria (ITSEC), or the Common Criteria for Information Technology Security Evaluation, ISO/IEC 15408:1999. This subcomponent can also address requirements for product evaluation analysis, testing, profiling, product certification, and/or product accreditation related activity undertaken.

4.6.6. Life Cycle Security Controls

This subcomponent addresses system development controls and security management controls.

System development controls include development environment security, development personnel security, configuration management security during product maintenance, software engineering practices, software development methodology, modularity, layering, use of failsafe design and implementation techniques (e.g., defensive programming) and development facility security.

Security management controls include execution of tools and procedures to ensure that the operational systems and networks adhere to configured security. These tools and procedures include checking the integrity of the security software, firmware, and hardware to ensure their correct operation.

This subcomponent can also address life-cycle security ratings based, for example, on the Trusted Software Development Methodology (TSDM) level IV and V, independent life-cycle security controls audit, and the Software Engineering Institute's Capability Maturity Model (SEI-CMM).

4.6.7. Network Security Controls

This subcomponent addresses network security related controls, including firewalls.

4.6.8. Time-stamping

This subcomponent addresses requirements or practices relating to the use of timestamps on various data. It may also discuss whether or

not the time-stamping application must use a trusted time source.

4.7. Certificate and CRL Profiles

This component is used to specify the certificate format and, if CRLs and/or OCSP are used, the CRL and/or OCSP format. This includes information on profiles, versions, and extensions used.

4.7.1. Certificate Profile

This subcomponent addresses such topics as the following (potentially by reference to a separate profile definition, such as the one defined in IETF PKIX RFC 3280):

- * Version number(s) supported;
- * Certificate extensions populated and their criticality;
- * Cryptographic algorithm object identifiers;
- * Name forms used for the CA, RA, and subscriber names;
- * Name constraints used and the name forms used in the name constraints;
- * Applicable CP OID(s);
- * Usage of the policy constraints extension;
- * Policy qualifiers syntax and semantics; and
- * Processing semantics for the critical CP extension.

4.7.2. CRL Profile

This subcomponent addresses such topics as the following (potentially by reference to a separate profile definition, such as the one defined in IETF PKIX RFC 3280):

- * Version numbers supported for CRLs; and
- * CRL and CRL entry extensions populated and their criticality.

4.7.3. OCSP Profile

This subcomponent addresses such topics as the following (potentially by reference to a separate profile definition, such as the IETF RFC 2560 profile):

- * Version of OCSP that is being used as the basis for establishing an OCSP system; and
- * OCSP extensions populated and their criticality.

4.8. Compliance Audit and Other Assessment

This component addresses the following:

- * The list of topics covered by the assessment and/or the assessment methodology used to perform the assessment; examples include WebTrust for CAs (9) and SAS 70 (10).
- * Frequency of compliance audit or other assessment for each entity that must be assessed pursuant to a CP or CPS, or the circumstances that will trigger an assessment; possibilities include an annual audit, pre-operational assessment as a condition of allowing an entity to be operational, or investigation following a possible or actual compromise of security.
- * The identity and/or qualifications of the personnel performing the audit or other assessment.
- * The relationship between the assessor and the entity being assessed, including the degree of independence of the assessor.
- * Actions taken as a result of deficiencies found during the assessment; examples include a temporary suspension of operations until deficiencies are corrected, revocation of certificates issued to the assessed entity, changes in personnel, triggering special investigations or more frequent subsequent compliance assessments, and claims for damages against the assessed entity.
- * Who is entitled to see results of an assessment (e.g., assessed entity, other participants, the general public), who provides them (e.g., the assessor or the assessed entity), and how they are communicated.

4.9. Other Business and Legal Matters

This component covers general business and legal matters. Sections 9.1 and 9.2 of the framework discuss the business issues of fees to be charged for various services and the financial responsibility of

participants to maintain resources for ongoing operations and for paying judgments or settlements in response to claims asserted against them. The remaining sections are generally concerned with legal topics.

Chokhani, et al. Informational [Page 45]

Starting with Section 9.3 of the framework, the ordering of topics is the same as or similar to the ordering of topics in a typical software licensing agreement or other technology agreement. Consequently, this framework may not only be used for CPs and CPSs, but also associated PKI-related agreements, especially subscriber agreements, and relying party agreements. This ordering is intended help lawyers review CPs, CPSs, and other documents adhering to this framework.

With respect to many of the legal subcomponents within this component, a CP or CPS drafter may choose to include in the document terms and conditions that apply directly to subscribers or relying parties. For instance, a CP or CPS may set forth limitations of liability that apply to subscribers and relying parties. The inclusion of terms and conditions is likely to be appropriate where the CP or CPS is itself a contract or part of a contract.

In other cases, however, the CP or CPS is not a contract or part of a contract; instead, it is configured so that its terms and conditions are applied to the parties by separate documents, which may include associated agreements, such as subscriber or relying party agreements. In that event, a CP drafter may write a CP so as to require that certain legal terms and conditions appear (or not appear) in such associated agreements. For example, a CP might include a subcomponent stating that a certain limitation of liability term must appear in a CA's subscriber and relying party agreements. Another example is a CP that contains a subcomponent prohibiting the use of a subscriber or relying party agreement containing a limitation upon CA liability inconsistent with the provisions of the CP. A CPS drafter may use legal subcomponents to disclose that certain terms and conditions appear in associated subscriber, relying party, or other agreements in use by the CA. A CPS might explain, for instance, that the CA writing it uses an associated subscriber or relying party agreement that applies a particular provision for limiting liability.

4.9.1. Fees

This subcomponent contains any applicable provisions regarding fees charged by CAs, repositories, or RAs, such as:

- * Certificate issuance or renewal fees;

- * Certificate access fees;
- * Revocation or status information access fees;

Chokhani, et al.

Informational

[Page 46]

- * Fees for other services such as providing access to the relevant CP or CPS; and
- * Refund policy.

4.9.2. Financial Responsibility

This subcomponent contains requirements or disclosures relating to the resources available to CAs, RAs, and other participants providing certification services to support performance of their operational PKI responsibilities, and to remain solvent and pay damages in the event they are liable to pay a judgment or settlement in connection with a claim arising out of such operations. Such provisions include:

- * A statement that the participant maintains a certain amount of insurance coverage for its liabilities to other participants;
- * A statement that a participant has access to other resources to support operations and pay damages for potential liability, which may be couched in terms of a minimum level of assets necessary to operate and cover contingencies that might occur within a PKI, where examples include assets on the balance sheet of an organization, a surety bond, a letter of credit, and a right under an agreement to an indemnity under certain circumstances; and
- * A statement that a participant has a program that offers first-party insurance or warranty protection to other participants in connection with their use of the PKI.

4.9.3. Confidentiality of Business Information

This subcomponent contains provisions relating to the treatment of confidential business information that participants may communicate to each other, such as business plans, sales information, trade secrets, and information received from a third party under a nondisclosure agreement. Specifically, this subcomponent addresses:

- * The scope of what is considered confidential information,
- * The types of information that are considered to be outside the scope of confidential information, and

- * The responsibilities of participants that receive confidential information to secure it from compromise, and refrain from using it or disclosing it to third parties.

4.9.4. Privacy of Personal Information

This subcomponent relates to the protection that participants, particularly CAs, RAs, and repositories, may be required to afford to personally identifiable private information of certificate applicants, subscribers, and other participants. Specifically, this subcomponent addresses the following, to the extent pertinent under applicable law:

- * The designation and disclosure of the applicable privacy plan that applies to a participant's activities, if required by applicable law or policy;
- * Information that is or is not considered private within the PKI;
- * Any responsibility of participants that receive private information to secure it, and refrain from using it and from disclosing it to third parties;
- * Any requirements as to notices to, or consent from individuals regarding use or disclosure of private information; and
- * Any circumstances under which a participant is entitled or required to disclose private information pursuant to judicial, administrative process in a private or governmental proceeding, or in any legal proceeding.

4.9.5. Intellectual Property Rights

This subcomponent addresses the intellectual property rights, such as copyright, patent, trademarks, or trade secrets, that certain participants may have or claim in a CP, CPS, certificates, names, and keys, or are the subject of a license to or from participants.

4.9.6. Representations and Warranties

This subcomponent can include representations and warranties of various entities that are being made pursuant to the CP or CPS. For example, a CPS that serves as a contract might contain a CA's warranty that information contained in the certificate is accurate. Alternatively, a CPS might contain a less extensive warranty to the effect that the information in the certificate is true to the best of the CA's knowledge after performing certain identity authentication

procedures with due diligence. This subcomponent can also include requirements that representations and warranties appear in certain agreements, such as subscriber or relying party agreements. For instance, a CP may contain a requirement that all CAs utilize a subscriber agreement, and that a subscriber agreement must contain a

warranty by the CA that information in the certificate is accurate. Participants that may make representations and warranties include CAs, RAs, subscribers, relying parties, and other participants.

4.9.7. Disclaimers of Warranties

This subcomponent can include disclaimers of express warranties that may otherwise be deemed to exist in an agreement, and disclaimers of implied warranties that may otherwise be imposed by applicable law, such as warranties of merchantability or fitness for a particular purpose. The CP or CPS may directly impose such disclaimers, or the CP or CPS may contain a requirement that disclaimers appear in associated agreements, such as subscriber or relying party agreements.

4.9.8. Limitations of Liability

This subcomponent can include limitations of liability in a CP or CPS or limitations that appear or must appear in an agreement associated with the CP or CPS, such as a subscriber or relying party agreement. These limitations may fall into one of two categories: limitations on the elements of damages recoverable and limitations on the amount of damages recoverable, also known as liability caps. Often, contracts contain clauses preventing the recovery of elements of damages such as incidental and consequential damages, and sometimes punitive damages. Frequently, contracts contain clauses that limit the possible recovery of one party or the other to an amount certain or to an amount corresponding to a benchmark, such as the amount a vendor was paid under the contract.

4.9.9. Indemnities

This subcomponent includes provisions by which one party makes a second party whole for losses or damage incurred by the second party, typically arising out of the first party's conduct. They may appear in a CP, CPS, or agreement. For example, a CP may require that subscriber agreements contain a term under which a subscriber is responsible for indemnifying a CA for losses the CA sustains arising out of a subscriber's fraudulent misrepresentations on the certificate application under which the CA issued the subscriber an inaccurate certificate. Similarly, a CPS may say that a CA uses a relying party agreement, under which relying parties are responsible for indemnifying a CA for losses the CA sustains arising out of use

of a certificate without properly checking revocation information or use of a certificate for purposes beyond what the CA permits.

4.9.10. Term and Termination

This subcomponent can include the time period in which a CP or a CPS remains in force and the circumstances under which the document, portions of the document, or its applicability to a particular participant can be terminated. In addition or alternatively, the CP or CPS may include requirements that certain term and termination clauses appear in agreements, such as subscriber or relying party agreements. In particular, such terms can include:

- * The term of a document or agreement, that is, when the document becomes effective and when it expires if it is not terminated earlier.
- * Termination provisions stating circumstances under which the document, certain portions of it, or its application to a particular participant ceases to remain in effect.
- * Any consequences of termination of the document. For example, certain provisions of an agreement may survive its termination and remain in force. Examples include acknowledgements of intellectual property rights and confidentiality provisions. Also, termination may trigger a responsibility of parties to return confidential information to the party that disclosed it.

4.9.11. Individual notices and communications with participants

This subcomponent discusses the way in which one participant can or must communicate with another participant on a one-to-one basis in order for such communications to be legally effective. For example, an RA may wish to inform the CA that it wishes to terminate its agreement with the CA. This subcomponent is different from publication and repository functions, because unlike individual communications described in this subcomponent, publication and posting to a repository are for the purpose of communicating to a wide audience of recipients, such as all relying parties. This subcomponent may establish mechanisms for communication and indicate the contact information to be used to route such communications, such as digitally signed e-mail notices to a specified address, followed by a signed e-mail acknowledgement of receipt.

4.9.12. Amendments

It will occasionally be necessary to amend a CP or CPS. Some of these changes will not materially reduce the assurance that a CP or its implementation provides, and will be judged by the policy administrator to have an insignificant effect on the acceptability of certificates. Such changes to a CP or CPS need not require a change

in the CP OID or the CPS pointer (URL). On the other hand, some changes to a specification will materially change the acceptability of certificates for specific purposes, and these changes may require corresponding changes to the CP OID or CPS pointer qualifier (URL).

This subcomponent may also contain the following information:

- * The procedures by which the CP or CPS and/or other documents must, may be, or are amended. In the case of CP or CPS amendments, change procedures may include a notification mechanism to provide notice of proposed amendments to affected parties, such as subscribers and relying parties, a comment period, a mechanism by which comments are received, reviewed and incorporated into the document, and a mechanism by which amendments become final and effective.
- * The circumstances under which amendments to the CP or CPS would require a change in CP OID or CPS pointer (URL).

4.9.13. Dispute Resolution Procedures

This subcomponent discusses procedures utilized to resolve disputes arising out of the CP, CPS, and/or agreements. Examples of such procedures include requirements that disputes be resolved in a certain forum or by alternative dispute resolution mechanisms.

4.9.14. Governing Law

This subcomponent sets forth a statement that the law of a certain jurisdiction governs the interpretation and enforcement of the subject CP or CPS or agreements.

4.9.15. Compliance with Applicable Law

This subcomponent relates to stated requirements that participants comply with applicable law, for example, laws relating to cryptographic hardware and software that may be subject to the export control laws of a given jurisdiction. The CP or CPS could purport to impose such requirements or may require that such provisions appear in other agreements.

4.9.16. Miscellaneous Provisions

This subcomponent contains miscellaneous provisions, sometimes called "boilerplate provisions," in contracts. The clauses covered in this subcomponent may appear in a CP, CPS, or agreements and include:

Chokhani, et al.

Informational

[Page 51]

- * An entire agreement clause, which typically identifies the document or documents comprising the entire agreement between the parties and states that such agreements supersede all prior and contemporaneous written or oral understandings relating to the same subject matter;
- * An assignment clause, which may act to limit the ability of a party in an agreement, assigning its rights under the agreement to another party (such as the right to receive a stream of payments in the future) or limiting the ability of a party to delegate its obligations under the agreement;
- * A severability clause, which sets forth the intentions of the parties in the event that a court or other tribunal determines that a clause within an agreement is, for some reason, invalid or unenforceable, and whose purpose is frequently to prevent the unenforceability of one clause from causing the whole agreement to be unenforceable; and
- * An enforcement clause, which may state that a party prevailing in any dispute arising out of an agreement is entitled to attorneys' fees as part of its recovery, or may state that a party's waiver of one breach of contract does not constitute a continuing waiver or a future waiver of other breaches of contract.
- * A force majeure clause, commonly used to excuse the performance of one or more parties to an agreement due to an event outside the reasonable control of the affected party or parties. Typically, the duration of the excused performance is commensurate with the duration of the delay caused by the event. The clause may also provide for the termination of the agreement under specified circumstances and conditions. Events considered to constitute a "force majeure" may include so-called "Acts of God," wars, terrorism, strikes, natural disasters, failures of suppliers or vendors to perform, or failures of the Internet or other infrastructure. Force majeure clauses should be drafted so as to be consistent with other portions of the framework and applicable service level agreements. For instance, responsibilities and capabilities for business continuity and disaster recovery may place some events within the reasonable control of the parties, such as an obligation to maintain backup electrical power in the face of power outages.

4.9.17. Other Provisions

This subcomponent is a "catchall" location where additional responsibilities and terms can be imposed on PKI participants that do not neatly fit within one of the other components or subcomponents of the framework. CP and CPS writers can place any provision within this subcomponent that is not covered by another subcomponent.

5. Security Considerations

According to X.509, a certificate policy (CP) is "a named set of rules that indicates the applicability of a certificate to a particular community and/or class of applications with common security requirements." A CP may be used by a relying party to help in deciding whether a certificate, and the binding therein, are sufficiently trustworthy and otherwise appropriate for a particular application.

The degree to which a relying party can trust the binding embodied in a certificate depends on several factors. These factors can include the practices followed by the certification authority (CA) in authenticating the subject; the CA's operating policy, procedures, and technical security controls, including the scope of the subscriber's responsibilities (for example, in protecting the private key), and the stated responsibilities and liability terms and conditions of the CA (for example, warranties, disclaimers of warranties, and limitations of liability).

This document provides a framework to address technical, procedural, personnel, and physical security aspects of Certification Authorities, Registration Authorities, repositories, subscribers, and relying party cryptographic modules, in order to ensure that the certificate generation, publication, renewal, re-key, usage, and revocation is done in a secure manner. Specifically, Section 4.3 Identification and Authentication (I&A); Section 4.4 Certificate Life-Cycle Operational Requirements; Section 4.5 Facility Management, and Operational Controls; Section 4.6 Technical Security Controls; Section 4.7 Certificate CRL, and OCSP Profiles; and Section 4.8 Compliance Audit and Other Assessment, are oriented towards ensuring secure operation of the PKI entities such as CA, RA, repository, subscriber systems, and relying party systems.

6. Outline of a Set of Provisions

This section contains a recommended outline for a set of provisions, intended to serve as a checklist or (with some further development) a standard template for use by CP or CPS writers. Such a common outline will facilitate:

Chokhani, et al. Informational [Page 53]

- (a) Comparison of two certificate policies during cross-certification or other forms of interoperation (for the purpose of equivalency mapping).
- (b) Comparison of a CPS with a CP to ensure that the CPS faithfully implements the policy.
- (c) Comparison of two CPSs.

In order to comply with the RFC, the drafters of a compliant CP or CPS are strongly advised to adhere to this outline. While use of an alternate outline is discouraged, it may be accepted if a proper justification is provided for the deviation and a mapping table is provided to readily discern where each of the items described in this outline is provided.

1. INTRODUCTION

- 1.1 Overview
- 1.2 Document name and identification
- 1.3 PKI participants
 - 1.3.1 Certification authorities
 - 1.3.2 Registration authorities
 - 1.3.3 Subscribers
 - 1.3.4 Relying parties
 - 1.3.5 Other participants
- 1.4 Certificate usage
 - 1.4.1 Appropriate certificate uses
 - 1.4.2 Prohibited certificate uses
- 1.5 Policy administration
 - 1.5.1 Organization administering the document
 - 1.5.2 Contact person
 - 1.5.3 Person determining CPS suitability for the policy
 - 1.5.4 CPS approval procedures

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

- 2.1 Repositories
- 2.2 Publication of certification information
- 2.3 Time or frequency of publication
- 2.4 Access controls on repositories

3. IDENTIFICATION AND AUTHENTICATION (11)

- 3.1 Naming
 - 3.1.1 Types of names
 - 3.1.2 Need for names to be meaningful

- 3.1.3 Anonymity or pseudonymity of subscribers
- 3.1.4 Rules for interpreting various name forms
- 3.1.5 Uniqueness of names
- 3.1.6 Recognition, authentication, and role of trademarks
- 3.2 Initial identity validation

- 3.2.1 Method to prove possession of private key
- 3.2.2 Authentication of organization identity
- 3.2.3 Authentication of individual identity
- 3.2.4 Non-verified subscriber information
- 3.2.5 Validation of authority
- 3.2.6 Criteria for interoperation
- 3.3 Identification and authentication for re-key requests
 - 3.3.1 Identification and authentication for routine re-key
 - 3.3.2 Identification and authentication for re-key after revocation
- 3.4 Identification and authentication for revocation request
- 4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS (11)
 - 4.1 Certificate Application
 - 4.1.1 Who can submit a certificate application
 - 4.1.2 Enrollment process and responsibilities
 - 4.2 Certificate application processing
 - 4.2.1 Performing identification and authentication functions
 - 4.2.2 Approval or rejection of certificate applications
 - 4.2.3 Time to process certificate applications
 - 4.3 Certificate issuance
 - 4.3.1 CA actions during certificate issuance
 - 4.3.2 Notification to subscriber by the CA of issuance of certificate
 - 4.4 Certificate acceptance
 - 4.4.1 Conduct constituting certificate acceptance
 - 4.4.2 Publication of the certificate by the CA
 - 4.4.3 Notification of certificate issuance by the CA to other entities
 - 4.5 Key pair and certificate usage
 - 4.5.1 Subscriber private key and certificate usage
 - 4.5.2 Relying party public key and certificate usage
 - 4.6 Certificate renewal
 - 4.6.1 Circumstance for certificate renewal
 - 4.6.2 Who may request renewal
 - 4.6.3 Processing certificate renewal requests
 - 4.6.4 Notification of new certificate issuance to subscriber
 - 4.6.5 Conduct constituting acceptance of a renewal certificate
 - 4.6.6 Publication of the renewal certificate by the CA
 - 4.6.7 Notification of certificate issuance by the CA to other entities
 - 4.7 Certificate re-key
 - 4.7.1 Circumstance for certificate re-key
 - 4.7.2 Who may request certification of a new public key
 - 4.7.3 Processing certificate re-keying requests

- 4.7.4 Notification of new certificate issuance to subscriber
- 4.7.5 Conduct constituting acceptance of a re-keyed certificate
- 4.7.6 Publication of the re-keyed certificate by the CA
- 4.7.7 Notification of certificate issuance by the CA to other entities

- 4.8 Certificate modification
 - 4.8.1 Circumstance for certificate modification
 - 4.8.2 Who may request certificate modification
 - 4.8.3 Processing certificate modification requests
 - 4.8.4 Notification of new certificate issuance to subscriber
 - 4.8.5 Conduct constituting acceptance of modified certificate
 - 4.8.6 Publication of the modified certificate by the CA
 - 4.8.7 Notification of certificate issuance by the CA to other entities
- 4.9 Certificate revocation and suspension
 - 4.9.1 Circumstances for revocation
 - 4.9.2 Who can request revocation
 - 4.9.3 Procedure for revocation request
 - 4.9.4 Revocation request grace period
 - 4.9.5 Time within which CA must process the revocation request
 - 4.9.6 Revocation checking requirement for relying parties
 - 4.9.7 CRL issuance frequency (if applicable)
 - 4.9.8 Maximum latency for CRLs (if applicable)
 - 4.9.9 On-line revocation/status checking availability
 - 4.9.10 On-line revocation checking requirements
 - 4.9.11 Other forms of revocation advertisements available
 - 4.9.12 Special requirements re key compromise
 - 4.9.13 Circumstances for suspension
 - 4.9.14 Who can request suspension
 - 4.9.15 Procedure for suspension request
 - 4.9.16 Limits on suspension period
- 4.10 Certificate status services
 - 4.10.1 Operational characteristics
 - 4.10.2 Service availability
 - 4.10.3 Optional features
- 4.11 End of subscription
- 4.12 Key escrow and recovery
 - 4.12.1 Key escrow and recovery policy and practices
 - 4.12.2 Session key encapsulation and recovery policy and practices
- 5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS (11)
 - 5.1 Physical controls
 - 5.1.1 Site location and construction
 - 5.1.2 Physical access
 - 5.1.3 Power and air conditioning
 - 5.1.4 Water exposures
 - 5.1.5 Fire prevention and protection
 - 5.1.6 Media storage
 - 5.1.7 Waste disposal

5.1.8 Off-site backup

5.2 Procedural controls

5.2.1 Trusted roles

5.2.2 Number of persons required per task

5.2.3 Identification and authentication for each role

- 5.2.4 Roles requiring separation of duties
- 5.3 Personnel controls
 - 5.3.1 Qualifications, experience, and clearance requirements
 - 5.3.2 Background check procedures
 - 5.3.3 Training requirements
 - 5.3.4 Retraining frequency and requirements
 - 5.3.5 Job rotation frequency and sequence
 - 5.3.6 Sanctions for unauthorized actions
 - 5.3.7 Independent contractor requirements
 - 5.3.8 Documentation supplied to personnel
- 5.4 Audit logging procedures
 - 5.4.1 Types of events recorded
 - 5.4.2 Frequency of processing log
 - 5.4.3 Retention period for audit log
 - 5.4.4 Protection of audit log
 - 5.4.5 Audit log backup procedures
 - 5.4.6 Audit collection system (internal vs. external)
 - 5.4.7 Notification to event-causing subject
 - 5.4.8 Vulnerability assessments
- 5.5 Records archival
 - 5.5.1 Types of records archived
 - 5.5.2 Retention period for archive
 - 5.5.3 Protection of archive
 - 5.5.4 Archive backup procedures
 - 5.5.5 Requirements for time-stamping of records
 - 5.5.6 Archive collection system (internal or external)
 - 5.5.7 Procedures to obtain and verify archive information
- 5.6 Key changeover
- 5.7 Compromise and disaster recovery
 - 5.7.1 Incident and compromise handling procedures
 - 5.7.2 Computing resources, software, and/or data are corrupted
 - 5.7.3 Entity private key compromise procedures
 - 5.7.4 Business continuity capabilities after a disaster
- 5.8 CA or RA termination
- 6. TECHNICAL SECURITY CONTROLS (11)
 - 6.1 Key pair generation and installation
 - 6.1.1 Key pair generation
 - 6.1.2 Private key delivery to subscriber
 - 6.1.3 Public key delivery to certificate issuer
 - 6.1.4 CA public key delivery to relying parties
 - 6.1.5 Key sizes
 - 6.1.6 Public key parameters generation and quality checking
 - 6.1.7 Key usage purposes (as per X.509 v3 key usage field)

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

6.2.2 Private key (n out of m) multi-person control

6.2.3 Private key escrow

- 6.2.4 Private key backup
 - 6.2.5 Private key archival
 - 6.2.6 Private key transfer into or from a cryptographic module
 - 6.2.7 Private key storage on cryptographic module
 - 6.2.8 Method of activating private key
 - 6.2.9 Method of deactivating private key
 - 6.2.10 Method of destroying private key
 - 6.2.11 Cryptographic Module Rating
 - 6.3 Other aspects of key pair management
 - 6.3.1 Public key archival
 - 6.3.2 Certificate operational periods and key pair usage periods
 - 6.4 Activation data
 - 6.4.1 Activation data generation and installation
 - 6.4.2 Activation data protection
 - 6.4.3 Other aspects of activation data
 - 6.5 Computer security controls
 - 6.5.1 Specific computer security technical requirements
 - 6.5.2 Computer security rating
 - 6.6 Life cycle technical controls
 - 6.6.1 System development controls
 - 6.6.2 Security management controls
 - 6.6.3 Life cycle security controls
 - 6.7 Network security controls
 - 6.8 Time-stamping
7. CERTIFICATE, CRL, AND OCSP PROFILES
- 7.1 Certificate profile
 - 7.1.1 Version number(s)
 - 7.1.2 Certificate extensions
 - 7.1.3 Algorithm object identifiers
 - 7.1.4 Name forms
 - 7.1.5 Name constraints
 - 7.1.6 Certificate policy object identifier
 - 7.1.7 Usage of Policy Constraints extension
 - 7.1.8 Policy qualifiers syntax and semantics
 - 7.1.9 Processing semantics for the critical Certificate Policies extension
 - 7.2 CRL profile
 - 7.2.1 Version number(s)
 - 7.2.2 CRL and CRL entry extensions
 - 7.3 OCSP profile
 - 7.3.1 Version number(s)
 - 7.3.2 OCSP extensions
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

- 8.1 Frequency or circumstances of assessment
- 8.2 Identity/qualifications of assessor
- 8.3 Assessor's relationship to assessed entity
- 8.4 Topics covered by assessment
- 8.5 Actions taken as a result of deficiency

- 8.6 Communication of results
- 9. OTHER BUSINESS AND LEGAL MATTERS
 - 9.1 Fees
 - 9.1.1 Certificate issuance or renewal fees
 - 9.1.2 Certificate access fees
 - 9.1.3 Revocation or status information access fees
 - 9.1.4 Fees for other services
 - 9.1.5 Refund policy
 - 9.2 Financial responsibility
 - 9.2.1 Insurance coverage
 - 9.2.2 Other assets
 - 9.2.3 Insurance or warranty coverage for end-entities
 - 9.3 Confidentiality of business information
 - 9.3.1 Scope of confidential information
 - 9.3.2 Information not within the scope of confidential information
 - 9.3.3 Responsibility to protect confidential information
 - 9.4 Privacy of personal information
 - 9.4.1 Privacy plan
 - 9.4.2 Information treated as private
 - 9.4.3 Information not deemed private
 - 9.4.4 Responsibility to protect private information
 - 9.4.5 Notice and consent to use private information
 - 9.4.6 Disclosure pursuant to judicial or administrative process
 - 9.4.7 Other information disclosure circumstances
 - 9.5 Intellectual property rights
 - 9.6 Representations and warranties
 - 9.6.1 CA representations and warranties
 - 9.6.2 RA representations and warranties
 - 9.6.3 Subscriber representations and warranties
 - 9.6.4 Relying party representations and warranties
 - 9.6.5 Representations and warranties of other participants
 - 9.7 Disclaimers of warranties
 - 9.8 Limitations of liability
 - 9.9 Indemnities
 - 9.10 Term and termination
 - 9.10.1 Term
 - 9.10.2 Termination
 - 9.10.3 Effect of termination and survival
 - 9.11 Individual notices and communications with participants
 - 9.12 Amendments
 - 9.12.1 Procedure for amendment
 - 9.12.2 Notification mechanism and period
 - 9.12.3 Circumstances under which OID must be changed

- 9.13 Dispute resolution provisions
- 9.14 Governing law
- 9.15 Compliance with applicable law
- 9.16 Miscellaneous provisions
- 9.16.1 Entire agreement

- 9.16.2 Assignment
- 9.16.3 Severability
- 9.16.4 Enforcement (attorneys' fees and waiver of rights)
- 9.16.5 Force Majeure
- 9.17 Other provisions

7. Comparison to RFC 2527

This framework represents an incremental improvement over RFC 2527. The new framework benefits from the experience gained in the course of deploying CP and CPS documents under RFC 2527. Further, this new framework is based on coordination with the American Bar Association Information Security Committee within the Section of Science and Technology Law. The ISC wrote the PKI Assessment Guidelines [ABA2], which embodies a great deal of technical, business, and legal experience in PKI operations. In particular, representatives of the ISC made changes to the framework to better suite it to the legal environment and make it more accessible to lawyers.

>From a technical perspective, the changes to the RFC 2527 framework were minimal and incremental, rather than revolutionary. Sections 3-7 have largely been preserved, with modest reorganization and new topics. For example, the new framework includes a revision of Section 4 of the framework to include a full treatment of the certificate life-cycle, the addition of key escrow, key encapsulation, and key recovery policies and practices, and OCSP. Section 2 audit functions now appear alone in Section 8, and Section 2 focuses exclusively on repository functions. The business and legal matters in RFC 2527's Section 2 now appear in a new Section 9.

From a legal perspective, the new Section 9 is useful because it places topics in the framework in an ordering that is similar to software licensing and other technology agreements and thus is familiar to technology lawyers. Moreover, the framework as a whole can double as a framework for a subscriber, relying party, or other PKI-related agreement. The changes are intended to make legal review of, and input into, CP and CPS documents more efficient. Section 9 also adds new legal topics, such as the privacy of personal information, liability terms, and duration of the effectiveness of the document.

Section 1 of the new framework is largely the same as RFC 2527, although it increases coverage of PKI participants by breaking out

subscribers from relying parties and adding a section for other participants. It changes the "applicability" section to one covering appropriate and prohibited uses of certificates. Also, it moves CPS

approval procedures from RFC 2527's Section 8.3 into a collected policy administration section. Finally, Section 1.6 adds a place to list definitions and acronyms.

Section 2 of the new framework is a reorganization of Section 2.6 of the old framework. Section 3 of the new framework is based on a division of the old Section 3.1 into two parts for naming and identification and authentication issues. It adds new issues, such as the permissibility of pseudonyms and anonymity. Old Section 4 topics on audit logging, record archives, key changeover, compromise and disaster recovery, and CA termination have moved to Section 5. The remaining Section 4 topics have been expanded and reorganized to cover a complete certificate lifecycle. New topics include items implicit in the RFC 2527 Section 4, but now explicit, such as certificate application processing, certificate modification, and the end of subscription.

New Sections 5.1 through 5.3 are almost identical to their counterparts in RFC 2527. The remainder of the new Section 5 is the topics moved from RFC 2527's Section 4, in the order that they appeared in Section 4. Section 6 of the new framework is almost the same as the old Section 6, with some exceptions, such as the consolidation of old Section 6.8 (cryptographic module engineering controls) into Section 6.2.1 (now called "cryptographic module standards and controls") and the addition of time-stamping in a new Section 6.8. Section 7 is almost identical to the old Section 7, the major change being the addition of a section covering OCSP profile. Section 8 is almost identical to RFC 2527's Section 2.7.

New Section 9 contains business and legal topics that were covered in RFC 2527's Section 2, including fees, financial responsibility, confidentiality, and intellectual property. It adds a section on the privacy of personal information, which has become a significant policy issue. The "liability" Section 2.2 in RFC 2527 now appears in Sections 9.6 through 9.9, covering representations and warranties, disclaimers, limitations of liability, and indemnities. Section 9.10 adds a section concerning the duration of the effectiveness of documentation. Section 9.12 collects terms concerning the way in which a document (CP, CPS, agreement, or other document) may be amended, formerly appearing in Section 8.1. Section 9 includes "legal boilerplate" topics, some of which were in the old Section 2. Finally, Section 9.17 is a catch-all "other provisions" section where drafters can place information that does not fit well into any other

section of the framework.

The following matrix shows the sections in the old RFC 2527 framework and their successor sections in the new framework.

Chokhani, et al.

Informational

[Page 61]

ORIGINAL RFC 2527 NEW RFC SECTION
SECTION

1. Introduction	1.
1.1 Overview	1.1
1.2 Identification	1.2
1.3 Community and Applicability	1.3
1.3.1 Certification Authorities	1.3.1
1.3.2 Registration Authorities	1.3.2
1.3.3 End entities	1.3.3, 1.3.4
1.3.4 Applicability	1.4, 4.5
1.4 Contact Details	1.5
1.4.1 Specification Administration Organization	1.5.1
1.4.2 Contact Person	1.5.2
1.4.3 Person Determining CPS Suitability for the Policy	1.5.3
2. General Provisions	2, 8, 9
2.1 Obligations	2.6.4
2.1.1 1A Obligations	Integrated throughout portions of the framework that apply to CAs
2.1.2 RA Obligations	Integrated

throughout
portions of the
framework that
apply to RAs

Chokhani, et al.

Informational

[Page 62]

2.1.3 Subscriber Obligations	4.1.2, 4.4, 4.5, 4.5.1, 4.6.5, 4.7.5, 4.8.1, 4.8.5, 4.9.1, 4.9.2, 4.9.13, 4.9.15, 5., 6., 9.6.3, 9.9
2.1.4 Relying Party Obligations	4.5, 4.5.2, 4.9.6, 5., 6., 9.6.4, 9.9
2.1.5 Repository Obligations	2., 4.4.2, 4.4.3, 4.6.6, 4.6.7, 4.7.6, 4.7.7, 4.8.6, 4.8.7
2.2 Liability	9.6, 9.7, 9.8, 9.9
2.2.1 CA Liability	9.6.1, 9.7., 9.8, 9.9
2.2.2 RA Liability	9.6.2, 9.7, 9.8, 9.9
2.3 Financial Responsibility	9.2
2.3.1 Indemnification by Relying Parties	9.9
2.3.2 Fiduciary Relationships	9.7
2.4 Interpretation and Enforcement	9.16
2.4.1 Governing Law	9.14, 9.15
2.4.2 Severability, Survival, Merger, Notice	9.10.3, 9.11, 9.16.1, 9.16.3
2.4.3 Dispute Resolution Procedures	9.13, 9.16.4
2.5 Fees	9.1

2.5.1 Certificate Issuance
or Renewal Fees 9.1.1

2.5.2 Certificate Access Fees 9.1.2

Chokhani, et al. Informational [Page 63]

2.5.3 Revocation or Status Information Access Fees	9.1.3
2.5.4 Fees for Other Services Such as Policy Information	9.1.4
2.5.5 Refund Policy	9.1.5
2.6 Publication and Repository	2.
2.6.1 Publication of CA Information	2.2, 4.4.2, 4.4.3, 4.6.6, 4.6.7, 4.7.6, 4.7.7, 4.8.6, 4.8.7
2.6.2 Frequency of Publication	2.3
2.6.3 Access Controls	2.4
2.6.4 Repositories	2.1
2.7 Compliance Audit	8.
2.7.1 Frequency of Entity Compliance Audit	8.1
2.7.2 Identity/Qualifications of Auditor	8.2
2.7.3 Auditor's Relationship to Audited Party	8.3
2.7.4 Topics Covered by Audit	8.4
2.7.5 Actions Taken as a Result of Deficiency	8.5
2.7.6 Communications of Results	8.6
2.8 Confidentiality	9.3, 9.4

2.8.1 Types of Information to be
Kept Confidential 9.3.1, 9.4.2

Chokhani, et al. Informational [Page 64]

2.8.2 Types of Information Not Considered Confidential	9.3.2, 9.4.3
2.8.3 Disclosure of Certificate Revocation/Suspension Information	9.3.1, 9.3.2, 9.3.3, 9.4.2, 9.4.3, 9.4.4
2.8.4 Release to Law Enforcement Officials	9.3.3, 9.4.6
2.8.5 Release as Part of Civil Discovery	9.3.3, 9.4.6
2.8.6 Disclosure Upon Owner's Request	9.3.3, 9.4.7
2.8.7 Other Information Release Circumstances	9.3.3, 9.4.7
2.9 Intellectual Property Rights	9.5
3. Identification and Authentication	3.
3.1 Initial Registration	3.1, 3.2
3.1.1 Type of Names	3.1.1
3.1.2 Need for Names to be Meaningful	3.1.2, 3.1.3
3.1.3 Rules for Interpreting Various Name Forms	3.1.4
3.1.4 Uniqueness of Names	3.1.5
3.1.5 Name Claim Dispute Resolution Procedure	3.1.6
3.1.6 Recognition, Authentication, and Role of Trademarks	3.1.6

3.1.7 Method to Prove Possession
of Private Key

3.2.1

Chokhani, et al.

Informational

[Page 65]

3.1.8 Authentication of Organization Identity	3.2.2
3.1.9 Authentication of Individual Identity	3.2.3
3.2 Routine Rekey	3.3.1, 4.6, 4.7
3.3 Rekey After Revocation	3.3.2
3.4 Revocation Request	3.4
4. Operational Requirements	4., 5.
4.1 Certificate Application	4.1, 4.2, 4.6, 4.7
4.2 Certificate Issuance	4.2, 4.3, 4.4.3, 4.6, 4.7, 4.8.4, 4.8.6, 4.8.7
4.3 Certificate Acceptance	4.3.2, 4.4, 4.6, 4.7, 4.8.4-4.8.7
4.4 Certificate Suspension and Revocation	4.8, 4.9
4.4.1 Circumstances for Revocation	4.8.1, 4.9.1
4.4.2 Who Can Request Revocation	4.8.2, 4.9.2
4.4.3 Procedure for Revocation Request	4.8.3-4.8.7, 4.9.3
4.4.4 Revocation Request Grace Period	4.9.4
4.4.5 Circumstances for Suspension	4.9.13
4.4.6 Who Can Request Suspension	4.9.14

4.4.7 Procedure for Suspension
Request 4.9.15

4.4.8 Limits on Suspension Period 4.9.16

Chokhani, et al.

Informational

[Page 66]

4.4.9 CRL Issuance Frequency (If Applicable)	4.9.7, 4.9.8, 4.10
4.4.10 CRL Checking Requirements	4.9.6, 4.10
4.4.11 On-Line Revocation/ Status Checking Availability	4.9.9, 4.10
4.4.12 On-Line Revocation Checking Requirements	4.9.6, 4.9.10, 4.10
4.4.13 Other Forms of Revocation Advertisements	4.9.11, 4.10
4.4.14 Checking Requirements for Other Forms of Revocation Advertisements	4.9.6, 4.9.11, 4.10
4.4.15 Special Requirements re Key Compromise	4.9.12
4.5 Security Audit Procedures	5.4
4.5.1 Types of Events Recorded	5.4.1
4.5.2 Frequency of Processing Log	5.4.2
4.5.3 Retention Period for Audit Log	5.4.3
4.5.4 Protection of Audit Log	5.4.4
4.5.5 Audit Log Backup Procedures	5.4.5
4.5.6 Audit Collection System (Internal vs. External)	5.4.6

4.5.7 Notification to Event-Causing
Subject 5.4.7

4.5.8 Vulnerability Assessments 5.4.8

Chokhani, et al. Informational

[Page 67]

4.6 Records Archival	5.5
4.6.1 Types of Records Archived	5.5.1
4.6.2 Retention Period for Archive	5.5.2
4.6.3 Protection of Archive	5.5.3
4.6.4 Archive Backup Procedures	5.5.4
4.6.5 Requirements for Time-Stamping of Records	5.5.5
4.6.6 Archive Collection System (Internal or External)	5.5.6
4.6.6 Procedures to Obtain and Verify Archive Information	5.5.7
4.7 Key Changeover	5.6
4.8 Compromise and Disaster Recovery	5.7, 5.7.1
4.8.1 Computing Resources, Software, and/or Data Are Corrupted	5.7.2
4.8.2 Entity Public Key is Revoked	4.9.7, 4.9.9, 4.9.11
4.8.3 Entity Key is Compromised	5.7.3
4.8.4 Secure Facility After a Natural or Other Type of Disaster	5.7.4
4.9 CA Termination	5.8
5. Physical, Procedural, and Personnel Security Controls	5.
5.1 Physical Controls	5.1

5.1.1 Site Location and Construction 5.1.1

5.1.2 Physical Access 5.1.2

Chokhani, et al. Informational [Page 68]

5.1.3 Power and Air Conditioning	5.1.3
5.1.4 Water Exposures	5.1.4
5.1.5 Fire Prevention and Protection	5.1.5
5.1.6 Media Storage	5.1.6
5.1.7 Waste Disposal	5.1.7
5.1.8 Off-Site Backup	5.1.8
5.2 Procedural Controls	5.2
5.2.1 Trusted Roles	5.2.1, 5.2.4
5.2.2 Number of Persons Required per Task	5.2.2, 5.2.4
5.2.3 Identification and Authentication for Each Role	5.2.3
5.3 Personnel Controls	5.3
5.3.1 Background, Qualifications, Experience, and Clearance Requirements	5.3.1
5.3.2 Background Check Procedures	5.3.2
5.3.3 Training Requirements	5.3.3
5.3.4 Retraining Frequency and Requirements	5.3.4
5.3.5 Job Rotation Frequency and Sequence	5.3.5
5.3.6 Sanctions for Unauthorized Actions	5.3.6

5.3.7 Contracting Personnel
Requirements 5.3.7

5.3.8 Documentation Supplied to
Personnel 5.3.8

Chokhani, et al. Informational [Page 69]

6. Technical Security Controls	6.
6.1 Key Pair Generation and Installation	6.1
6.1.1 Key Pair Generation	6.1.1
6.1.2 Private Key Delivery to Entity	6.1.2
6.1.3 Public Key Delivery to Certificate Issuer	6.1.3
6.1.4 CA Public Key Delivery to Users	6.1.4
6.1.5 Key Sizes	6.1.5
6.1.6 Public Key Parameters Generation	6.1.6
6.1.7 Parameter Quality Checking	6.1.6
6.1.8 Hardware/Software Key Generation	6.1.1
6.1.9 Key Usage Purposes (as per X.509 v3 Key Usage Field)	6.1.9
6.2 Private Key Protection	6.2
6.2.1 Standards for Cryptographic Module	6.2.1
6.2.2 Private Key (n out of m) Multi-Person Control	6.2.2
6.2.3 Private Key Escrow	6.2.3
6.2.4 Private Key Backup	6.2.4
6.2.5 Private Key Archival	6.2.5
6.2.6 Private Key Entry Into Cryptographic Module	6.2.6, 6.2.7

**6.2.7 Method of Activating
Private Key** **6.2.8**

Chokhani, et al. Informational [Page 70]

6.2.8 Method of Deactivating Private Key	6.2.9
6.2.9 Method of Destroying Private Key	6.2.10
6.3 Other Aspects of Key Pair Management	6.3
6.3.1 Public Key Archival	6.3.1
6.3.2 Usage Periods for the Public and Private Keys	6.3.2
6.4 Activation Data	6.4
6.4.1 Activation Data Generation and Installation	6.4.1
6.4.2 Activation Data Protection	6.4.2
6.4.3 Other Aspects of Activation Data	6.4.3
6.5 Computer Security Controls	6.5
6.5.1 Specific Computer Security Technical Requirements	6.5.1
6.5.2 Computer Security Rating	6.5.2
6.6 Life Cycle Technical Controls	6.6
6.6.1 System Development Controls	6.6.1
6.6.2 Security Management Controls	6.6.2
6.6.3 Life Cycle Security Controls	6.6.3
6.7 Network Security Controls	6.7
6.8 Cryptographic Module	

Engineering Controls 6.2.1, 6.2,
 6.2.1, 6.2.11

7.Certificate and CRL Profiles 7.

Chokhani, et al. Informational [Page 71]

7.1 Certificate Profile	7.1
7.1.1 Version Number(s)	7.1.1
7.1.2 Certificate Extensions	7.1.2
7.1.3 Algorithm Object Identifiers	7.1.3
7.1.4 Name Forms	7.1.4
7.1.5 Name Constraints	7.1.5
7.1.6 Certificate Policy Object Identifier	7.1.6
7.1.7 Usage of Policy Constraints Extension	7.1.7
7.1.8 Policy Qualifiers Syntax and Semantics	7.1.8
7.1.9 Processing Semantics for the Critical Certificate Policies Extension	7.1.9
7.2 CRL Profile	7.2
7.2.1 Version Number(s)	7.2.1
7.2.2 CRL and CRL Entry Extensions	7.2.1
8. Specification Administration	N/A
8.1 Specification Change Procedures	9.12
8.2 Publication and Notification Policies	2.2, 2.3
8.3 CPS Approval Procedures	1.5.4

The following matrix shows the sections in the new framework and the sections in RFC 2527 to which the headings in the new framework correspond.

NEW RFC SECTION	ORIGINAL RFC 2527 SECTION
1. Introduction	1.
1.1 Overview	1.1
1.2 Document Name and Identification	1.2
1.3 PKI Participants	1.3
1.3.1 Certification Authorities	1.3.1
1.3.2 Registration Authorities	1.3.2
1.3.3 Subscribers	1.3.3
1.3.4 Relying Parties	1.3.3
1.3.5 Other Participants	N/A
1.4 Certificate Usage	1.3.4
1.4.1 Appropriate Certificate Uses	1.3.4
1.4.2 Prohibited Certificate Uses	1.3.4
1.5 Policy Administration	1.4
1.5.1 Organization Administering the Document	1.4.1
1.5.2 Contact Person	1.4.2
1.5.3 Person Determining CPS Suitability for the Policy	1.4.3
1.5.4 CPS Approval Procedures	8.3

1.6 Definitions and Acronyms N/A

2. Publication and Repository Responsibilities 2.1.5, 2.6

2.1 Repositories	2.6.4
2.2 Publication of Certification Information	2.6.1, 8.2
2.3 Time or Frequency of Publication	2.6.2, 8.2
2.4 Access Controls on Repositories	2.6.3
3. Identification and Authentication	3.
3.1 Naming	3.1
3.1.1 Type of Names	3.1.1
3.1.2 Need for Names to be Meaningful	3.1.2
3.1.3. Anonymity or Pseudonymity of Subscribers	3.1.2
3.1.4 Rules for Interpreting Various Name Forms	3.1.3
3.1.5 Uniqueness of Names	3.1.4
3.1.6 Recognition, Authentication, and Role of Trademarks	3.1.5, 3.1.6
3.2 Initial Identity Validation	3.1
3.2.1 Method to Prove Possession of Private Key	3.1.7
3.2.2 Authentication of Organization Identity	3.1.8
3.2.3 Authentication of Individual Identity	3.1.9
3.2.4 Non-Verified Subscriber Information	N/A

3.2.5 Validation of Authority 3.1.9

Chokhani, et al. Informational [Page 74]

3.2.6 Criteria for Interoperation	4.1
3.3 Identification and Authentication for Re-Key Requests	3.2, 3.3
3.3.1 Identification and Authentication for Routine Re-Key	3.2
3.3.2 Identification and Authentication for Re-Key After Revocation	3.3
3.4 Identification and Authentication for Revocation Request	3.4
4. Certificate Life-Cycle Operational Requirements	4.
4.1 Certificate Application	4.1
4.1.1 Who Can Submit a Certificate Application	4.1
4.1.2 Enrollment Process and Responsibilities	2.1.3, 4.1
4.2 Certificate Application Processing	4.1, 4.2
4.2.1 Performing Identification and Authentication Functions	4.1, 4.2
4.2.2 Approval or Rejection of Certificate Applications	4.1, 4.2
4.2.3 Time to Process Certificate Applications	4.1, 4.2
4.3 Certificate Issuance	4.2
4.3.1 CA Actions During	

Certificate Issuance 4.2

4.3.2 Notifications to Subscriber by
the CA of Issuance of Certificate 4.2, 4.3

Chokhani, et al. Informational [Page 75]

4.4 Certificate Acceptance	2.1.3, 4.3
4.4.1 Conduct Constituting Certificate Acceptance	4.3
4.4.2 Publication of the Certificate by the CA	2.1.5, 2.6.1, 4.3
4.4.3 Notification of Certificate Issuance by the CA to Other Entities	2.1.5, 2.6.1, 4.2, 4.3
4.5 Key Pair and Certificate Usage	1.3.4, 2.1.3, 2.1.4
4.5.1 Subscriber Private Key and Certificate Usage	1.3.4, 2.1.3
4.5.2 Relying Party Public Key and Certificate Usage	1.3.4, 2.1.4
4.6 Certificate Renewal	3.2, 4.1, 4.2, 4.3
4.6.1 Circumstances for Certificate Renewal	3.2, 4.1
4.6.2 Who May Request Renewal	3.2, 4.1
4.6.3 Processing Certificate Renewal Requests	3.2, 4.1, 4.2
4.6.4 Notification of New Certificate Issuance to Subscriber	3.2, 4.2, 4.3
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate	2.1.3, 3.2, 4.3

**4.6.6 Publication of the
Renewal Certificate
by the CA** 2.1.5, 2.6.1,
 3.2, 4.3

Chokhani, et al. Informational [Page 76]

4.6.7 Notification of Certificate Issuance by the CA to Other Entities	2.1.5, 2.6.1, 3.2, 4.2, 4.3
4.7 Certificate Re-Key	3.2, 4.1, 4.2, 4.3
4.7.1 Circumstances for Certificate Re-Key	3.2, 4.1
4.7.2 Who May Request Certification of a New Public Key	3.2, 4.1
4.7.3 Processing Certificate Re-Keying Requests	3.2, 4.1, 4.2
4.7.4 Notification of New Certificate Issuance to Subscriber	3.2, 4.2, 4.3
4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate	2.1.3, 3.2, 4.3
4.7.6 Publication of the Re-Keyed Certificate by the CA	2.1.5, 2.6.1, 3.2, 4.3
4.7.7 Notification of Certificate Issuance by the CA to Other Entities	2.1.5, 2.6.1, 3.2, 4.2, 4.3
4.8 Certificate Modification	4.4
4.8.1 Circumstances for Certificate Modification	2.1.3, 4.4.1
4.8.2 Who May Request Certificate Modification	4.4.2

**4.8.3 Processing Certificate
Modification Requests 4.4.3**

Chokhani, et al. Informational [Page 77]

4.8.4 Notification of New
Certificate Issuance to
Subscriber 4.2, 4.3, 4.4.3

4.8.5 Conduct Constituting
Acceptance of Modified
Certificate 2.1.3, 4.3, 4.4.3

4.8.6 Publication of the Modified
Certificate by
the CA 2.1.5, 2.6.1,
4.2, 4.3, 4.4.3

4.8.7 Notification of
Certificate Issuance by
the CA to Other
Entities 2.1.5, 2.6.1,
4.2, 4.3, 4.4.3

4.9 Certificate Revocation
and Suspension 4.4

4.9.1 Circumstances for Revocation 2.1.3, 4.4.1

4.9.2 Who Can Request Revocation 4.4.2

4.9.3 Procedure for Revocation
Request 2.1.3, 4.4.3

4.9.4 Revocation Request Grace
Period 4.4.4

4.9.5 Time Within Which CA Must
Process the Revocation Request N/A

4.9.6 Revocation Checking
Requirements for Relying
Parties 2.1.4, 4.4.10,
4.4.12, 4.4.14

4.9.7 CRL Issuance Frequency 4.4.9, 4.8.3

4.9.8 Maximum Latency for CRLs 4.4.9

4.9.9 On-Line Revocation/Status
Checking Availability 4.4.11, 4.8.3

Chokhani, et al. Informational [Page 78]

4.9.10 On-Line Revocation Checking Requirements	4.4.12
4.9.11 Other Forms of Revocation Advertisements Available	4.4.13, 4.4.14, 4.8.3
4.9.12 Special Requirements re Key Compromise	4.4.15
4.9.13 Circumstances for Suspension	2.1.3, 4.4.5
4.9.14 Who Can Request Suspension	4.4.6
4.9.15 Procedure for Suspension Request	2.1.3, 4.4.7
4.9.16 Limits on Suspension Period	4.4.8
4.10 Certificate Status Services	4.4.9-4.4.14
4.10.1 Operational Characteristics	4.4.9, 4.4.11, 4.4.13
4.10.2 Service Availability	4.4.9, 4.4.11, 4.4.13
4.10.3 Operational Features	4.4.9, 4.4.11, 4.4.13
4.11 End of Subscription	N/A
4.12 Key Escrow and Recovery	6.2.3
4.12.1 Key Escrow and Recovery Policy and Practices	6.2.3
4.12.2 Session Key Encapsulation and Recovery Policy and Practices	6.2.3

5. Facility, Management, and
Operational Controls 2.1.3, 2.1.4,
 4., 5.

5.1 Physical Controls 5.1

Chokhani, et al. Informational [Page 79]

5.1.1 Site Location and Construction	5.1.1
5.1.2 Physical Access	5.1.2
5.1.3 Power and Air Conditioning	5.1.3
5.1.4 Water Exposures	5.1.4
5.1.5 Fire Prevention and Protection	5.1.5
5.1.6 Media Storage	5.1.6
5.1.7 Waste Disposal	5.1.7
5.1.8 Off-Site Backup	5.1.8
5.2 Procedural Controls	5.2
5.2.1 Trusted Roles	5.2.1
5.2.2 Number of Persons Required per Task	5.2.2
5.2.3 Identification and Authentication for Each Role	5.2.3
5.2.4 Roles Requiring Separation of Duties	5.2.1, 5.2.2
5.3 Personnel Controls	5.3
5.3.1 Qualifications, Experience, and Clearance Requirements	5.3.1
5.3.2 Background Check Procedures	5.3.2
5.3.3 Training Requirements	5.3.3
5.3.4 Retraining Frequency and Requirements	5.3.4
5.3.5 Job Rotation Frequency	

and Sequence 5.3.5

5.3.6 Sanctions for Unauthorized
Actions 5.3.6

Chokhani, et al. Informational [Page 80]

5.3.7 Independent Contractor Requirements	5.3.7
5.3.8 Documentation Supplied to Personnel	5.3.8
5.4 Audit Logging Procedures	4.5
5.4.1 Types of Events Recorded	4.5.1
5.4.2 Frequency of Processing Log	4.5.2
5.4.3 Retention Period for Audit Log	4.5.3
5.4.4 Protection of Audit Log	4.5.4
5.4.5 Audit Log Backup Procedures	4.5.5
5.4.6 Audit Collection System (Internal vs. External)	4.5.6
5.4.7 Notification to Event-Causing Subject	4.5.7
5.4.8 Vulnerability Assessments	4.5.8
5.5 Records Archival	4.6
5.5.1 Types of Records Archived	4.6.1
5.5.2 Retention Period for Archive	4.6.2
5.5.3 Protection of Archive	4.6.3
5.5.4 Archive Backup Procedures	4.6.4
5.5.5 Requirements for Time-Stamping of Records	4.6.5
5.5.6 Archive Collection System (Internal or External)	4.6.6

5.5.7 Procedures to Obtain and
Verify Archive
Information

4.6.7

Chokhani, et al. Informational [Page 81]

5.6 Key Changeover	4.7
5.7 Compromise and Disaster Recovery	4.8
5.7.1 Incident and Compromise Handling Procedures	4.8
5.7.2 Computing Resources, Software, and/or Data Are Corrupted	4.8.1
5.7.3 Entity Private Key Compromise Procedures	4.8.3
5.7.4 Business Continuity Capabilities After a Disaster	4.8.4
5.8 CA or RA Termination	4.9
6. Technical Security Controls	2.1.3, 2.1.4, 6.
6.1 Key Pair Generation and Installation	6.1
6.1.1 Key Pair Generation	6.1.1, 6.1.8
6.1.2 Private Key Delivery to Subscriber	6.1.2
6.1.3 Public Key Delivery to Certificate Issuer	6.1.3
6.1.4 CA Public Key Delivery to Relying Parties	6.1.4
6.1.5 Key Sizes	6.1.5
6.1.6 Public Key Parameters Generation and Quality Checking	6.1.6, 6.1.7
6.1.7 Key Usage Purposes	

(as per X.509 v3
Key Usage Field) 6.1.9

Chokhani, et al. Informational [Page 82]

6.2 Private Key Protection and Cryptographic Module Engineering Controls	6.2, 6.8
6.2.1 Cryptographic Module Standards and Controls	6.2.1, 6.8
6.2.2 Private Key (n out of m) Multi-Person Control	6.2.2
6.2.3 Private Key Escrow	6.2.3
6.2.4 Private Key Backup	6.2.4
6.2.5 Private Key Archival	6.2.5
6.2.6 Private Key Transfer Into or From a Cryptographic Module	6.2.6
6.2.7 Private Key Storage on Cryptographic Module	6.2.6
6.2.8 Method of Activating Private Key	6.2.7
6.2.9 Method of Deactivating Private Key	6.2.8
6.2.10 Method of Destroying Private Key	6.2.9
6.2.11 Cryptographic Module Rating	6.2.1, 6.8
6.3 Other Aspects of Key Pair Management	6.3
6.3.1 Public Key Archival	6.3.1
6.3.2 Certificate Operational Periods and Key Pair Usage Periods	6.3.2

6.4.1 Activation Data Generation and Installation	6.4.1
6.4.2 Activation Data Protection	6.4.2
6.4.3 Other Aspects of Activation Data	6.4.3
6.5 Computer Security Controls	6.5
6.5.1 Specific Computer Security Technical Requirements	6.5.1
6.5.2 Computer Security Rating	6.5.2
6.6 Life Cycle Technical Controls	6.6
6.6.1 System Development Controls	6.6.1
6.6.2 Security Management Controls	6.6.2
6.6.3 Life Cycle Security Controls	6.6.3
6.7 Network Security Controls	6.7
6.8 Time-Stamping	N/A
7. Certificate, CRL, and OCSP Profiles	7.
7.1 Certificate Profile	7.1
7.1.1 Version Number(s)	7.1.1
7.1.2 Certificate Extensions	7.1.2
7.1.3 Algorithm Object Identifiers	7.1.3
7.1.4 Name Forms	7.1.4
7.1.5 Name Constraints	7.1.5

7.1.6 Certificate Policy
Object Identifier 7.1.6

7.1.7 Usage of Policy Constraints
Extension 7.1.7

Chokhani, et al. Informational [Page 84]

7.1.8 Policy Qualifiers Syntax and Semantics	7.1.8
7.1.9 Processing Semantics for the Critical Certificate Policies Extension	7.1.9
7.2 CRL Profile	7.2
7.2.1 Version Number(s)	7.2.1
7.2.2 CRL and CRL Entry Extensions	7.2.1
7.3 OCSP Profile	N/A
7.3.1 Version Number(s)	N/A
7.3.2 OCSP Extensions	N/A
8. Compliance Audit and Other Assessments	2.7
8.1 Frequency and Circumstances of Assessment	2.7.1
8.2 Identity/Qualifications of Assessor	2.7.2
8.3 Assessor's Relationship to Assessed Entity	2.7.3
8.4 Topics Covered by Assessment	2.7.4
8.5 Actions Taken as a Result of Deficiency	2.7.5
8.6 Communications of Results	2.7.6
9. Other Business and Legal Matters	2.

9.1 Fees	2.5

9.1.1 Certificate Issuance or Renewal Fees	2.5.1

Chokhani, et al. Informational [Page 85]

9.1.2 Certificate Access Fees	2.5.2
9.1.3 Revocation or Status Information Access Fees	2.5.3
9.1.4 Fees for Other Services	2.5.4
9.1.5 Refund Policy	2.5.5
9.2 Financial Responsibility	2.3
9.2.1 Insurance Coverage	2.3
9.2.2 Other Assets	2.3
9.2.3 Insurance or Warranty Coverage for End-Entities	2.3
9.3 Confidentiality of Business Information	2.8
9.3.1 Scope of Confidential Information	2.8.1, 2.8.3
9.3.2 Information Not Within the Scope of Confidential Information	2.8.2, 2.8.3
9.3.3 Responsibility to Protect Confidential Information	2.8, 2.8.3-2.8.7
9.4 Privacy of Personal Information	2.8
9.4.1 Privacy Plan	N/A
9.4.2 Information Treated as Private	2.8.1, 2.8.3
9.4.3 Information Not Deemed Private	2.8.2, 2.8.3
9.4.4 Responsibility to Protect	

Private Information 2.8, 2.8.1,
2.8.3

9.4.5 Notice and Consent to Use

Private Information N/A

Chokhani, et al. Informational [Page 86]

9.4.6 Disclosure Pursuant to Judicial or Administrative Process	2.8.4-2.8.5
9.4.7 Other Information Disclosure Circumstances	2.8.6-2.8.7
9.5 Intellectual Property rights	2.9
9.6 Representations and Warranties	2.2
9.6.1 CA Representations and Warranties	2.2.1
9.6.2 RA Representations and Warranties	2.2.2
9.6.3 Subscriber Representations and Warranties	2.1.3
9.6.4 Relying Party Representations and Warranties	2.1.4
9.6.5 Representations and Warranties of Other Participants	N/A
9.7 Disclaimers of Warranties	2.2, 2.3.2
9.8 Limitations of Liability	2.2
9.9 Indemnities	2.1.3, 2.1.4, 2.2, 2.3.1
9.10 Term and Termination	N/A
9.10.1 Term	N/A
9.10.2 Termination	N/A
9.10.3 Effect of Termination and Survival	N/A

9.11 Individual Notices and
Communications with Participants 2.4.2

9.12 Amendments 8.1

Chokhani, et al. Informational [Page 87]

9.12.1 Procedure for Amendment	8.1
9.12.2 Notification Mechanism and Period	8.1
9.12.3 Circumstances Under Which OID Must be Changed	8.1
9.13 Dispute Resolution Provisions	2.4.3
9.14 Governing Law	2.4.1
9.15 Compliance with Applicable Law	2.4.1
9.16 Miscellaneous Provisions	2.4
9.16.1 Entire Agreement	2.4.2
9.16.2 Assignment	N/A
9.16.3 Severability	2.4.2
9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)	2.4.3
9.17 Other Provisions	N/A

8. Acknowledgements

The development of the predecessor document (RFC 2527) was supported by the Government of Canada's Policy Management Authority (PMA) Committee, the National Security Agency, the National Institute of Standards and Technology (NIST), and the American Bar Association Information Security Committee Accreditation Working Group.

This revision effort is largely a result of constant inspiration from Michael Baum. Michael Power, Mike Jenkins, and Alice Sturgeon have also made several contributions.

9. References

[ABA1] American Bar Association, Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce, 1996.

Chokhani, et al. Informational [Page 88]

[ABA2] American Bar Association, PKI Assessment Guidelines, v0.30, Public Draft For Comment, June 2001.

[BAU1] Michael. S. Baum, Federal Certification Authority Liability and Policy, NIST-GCR-94-654, June 1994, available at <http://www.verisign.com/repository/pubs/index.html>.

[ETS] European Telecommunications Standards Institute, "Policy Requirements for Certification Authorities Issuing Qualified Certificates," ETSI TS 101 456, Version 1.1.1, December 2000.

[GOC] Government of Canada PKI Policy Management Authority, "Digital Signature and Confidentiality Certificate Policies for the Government of Canada Public Key Infrastructure," v.3.02, April 1999.

[IDT] Identrus, LLC, "Identrus Identity Certificate Policy" IP-IPC Version 1.7, March 2001.

[ISO1] ISO/IEC 9594-8/ITU-T Recommendation X.509, "Information Technology - Open Systems Interconnection: The Directory: Authentication Framework," 1997 edition. (Pending publication of 2000 edition, use 1997 edition.)

[PEM1] Kent, S., "Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management", RFC 1422, February 1993.

[PKI1] Housley, R., Polk, W. Ford, W. and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.

[CPF] Chokhani, S. and W. Ford, "Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Statement Framework", RFC 2527, March 1999.

10. Notes

1. A paper copy of the ABA Digital Signature Guidelines can be purchased from the ABA. See <http://www.abanet.com> for ordering details. The DSG may also be downloaded without charge from the ABA website at http://www.abanet.org/scitech/ec/isc/digital_signature.html.

2. A draft of the PKI Assessment Guidelines may be downloaded without charge from the ABA website at <http://www.abanet.org/scitech/ec/isc/pag/pag.html>.

3. The term "meaningful" means that the name form has commonly understood semantics to determine the identity of a person and/or organization. Directory names and RFC 822 names may be more or less meaningful.
4. The subject may not need to prove to the CA that the subject has possession of the private key corresponding to the public key being registered if the CA generates the subject's key pair on the subject's behalf.
5. Examples of means to identify and authenticate individuals include biometric means (such as thumb print, ten finger print, and scan of the face, palm, or retina), a driver's license, a credit card, a company badge, and a government badge.
6. Certificate "modification" does not refer to making a change to an existing certificate, since this would prevent the verification of any digital signatures on the certificate and cause the certificate to be invalid. Rather, the concept of "modification" refers to a situation where the information referred to in the certificate has changed or should be changed, and the CA issues a new certificate containing the modified information. One example is a subscriber that changes his or her name, which would necessitate the issuance of a new certificate containing the new name.
7. The n out of m rule allows a private key to be split in m parts. The m parts may be given to m different individuals. Any n parts out of the m parts may be used to fully reconstitute the private key, but having any n-1 parts provides one with no information about the private key.
8. A private key may be escrowed, backed up, or archived. Each of these functions has a different purpose. Thus, a private key may go through any subset of these functions depending on the requirements. The purpose of escrow is to allow a third party (such as an organization or government) to obtain the private key without the cooperation of the subscriber. The purpose of back up is to allow the subscriber to reconstitute the key in case of the destruction or corruption of the key for business continuity purposes. The purpose of archives is to provide for reuse of the private key in the future, e.g., use to decrypt a document.

9. WebTrust refers to the "WebTrust Program for Certification Authorities," from the American Institute of Certified Public Accountants, Inc., and the Canadian Institute of Chartered Accountants.

10. See <<http://www.aicpa.org>>.

11. All or some of the following items may be different for the various types of entities, i.e., CA, RA, and end entities.

11. List of Acronyms

ABA - American Bar Association

CA - Certification Authority

CP - Certificate Policy

CPS - Certification Practice Statement

CRL - Certificate Revocation List

DAM - Draft Amendment

FIPS - Federal Information Processing Standard

I&A - Identification and Authentication

IEC - International Electrotechnical Commission

IETF - Internet Engineering Task Force

IP - Internet Protocol

ISO - International Organization for Standardization

ITU - International Telecommunications Union

NIST - National Institute of Standards and Technology

OID - Object Identifier

PIN - Personal Identification Number

PKI - Public Key Infrastructure

PKIX - Public Key Infrastructure (X.509) (IETF Working Group)

RA - Registration Authority

RFC - Request For Comment

URL - Uniform Resource Locator

US - United States

12. Authors' Addresses

Santosh Chokhani
Orion Security Solutions, Inc.
3410 N. Buchanan Street
Arlington, VA 22207

Phone: (703) 237-4621
Fax: (703) 237-4920
EMail: chokhani@orionsec.com

Warwick Ford
VeriSign, Inc.
6 Ellery Square
Cambridge, MA 02138

Phone: (617) 642-0139
EMail: wford@verisign.com

Randy V. Sabett, J.D., CISSP
Cooley Godward LLP
One Freedom Square, Reston Town Center
11951 Freedom Drive
Reston, VA 20190-5656

Phone: (703) 456-8137
Fax: (703) 456-8100
EMail: rsabett@cooley.com

Charles (Chas) R. Merrill
McCarter & English, LLP
Four Gateway Center
100 Mulberry Street
Newark, New Jersey 07101-0652

Phone: (973) 622-4444
Fax: (973) 624-7070
EMail: cmerrill@mccarter.com

Stephen S. Wu
Infoliance, Inc.
800 West El Camino Real
Suite 180
Mountain View, CA 94040

Phone: (650) 917-8045
Fax: (650) 618-1454
EMail: swu@infoliance.com

13. Full Copyright Statement

Copyright (C) The Internet Society (2003). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assignees.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.

Appendix D: NACHA Electronic Benefits Transfer

Attachment 1: QUEST® Operating Rules

Attachment 2: Amendments & Variances



QUEST® OPERATING RULES

December 2008

Version 2.0

©2008 NACHA – The Electronic Payments Association. All rights reserved.

NACHA – The Electronic Payments Association

13450 Sunrise Valley Drive, Suite 100

Herndon, VA 20171

Phone: 703/561-1100

Web: www.nacha.org and www.electronicpayments.org



TABLE OF CONTENTS

INTRODUCTION.....	3
DEFINITIONS CHAPTER	4
Chapter 1: Issuer Requirements	12
Chapter 2: Card Specifications	18
Chapter 3: Acquirer and Terminal Operator Requirements	21
Chapter 4: Merchant Agreement Requirements	34
Chapter 5: Error Resolution.....	38
Chapter 6: Settlement	55
Chapter 7: Third Party Service Provider Requirements	56
Chapter 8: Arbitration and Grievance Procedures, Assessments	59
Chapter 9: Security	63
Chapter 10: Liabilities and Indemnification	71
Chapter 11: Licensing of the QUEST Mark.....	73
Chapter 12: Miscellaneous.....	76
 APPENDICES	
Appendix II: Form of Issuer Participation Agreement.....	78
Appendix III: EBT Security Compliance Review.....	79
 GUIDELINES	
Guidelines for Including Programs Under the Quest Operating Rules.....	83



INTRODUCTION
(Amended April 14, 1999 and December 16, 2008)

The following Operating Rules set forth the requirements for the distribution of government benefits under the Quest service mark. Government entities may utilize these Rules by incorporating them in their contracts with private sector entities utilized to distribute benefits. There is no fee for use of the QUEST Mark. Of course, government entities may also choose to distribute benefits under other operating rules. The Quest Operating Rules do not address electronic distribution of government benefits under service marks other than the QUEST Mark.

1. NACHA encourages the addition of new benefit programs to the QUEST System.
2. Any unrestricted cash benefits, i.e., benefits that can be fully redeemed for currency without regard to state borders, can be added to the Cash Account without limitation.
3. NACHA will work with interested parties to develop additional standards for programs that have characteristics that distinguish them from Cash and the Supplemental Nutrition Assistance Program but are nonetheless susceptible to universal standards and interoperable distribution without regard to state borders. Such programs would be identified by additional icons, which would be associated with the QUEST Mark at the retail level.
4. Even if benefit programs cannot be made interoperable at this time but still have common elements nationwide, standardization of programs can benefit all participants in EBT. NACHA will work with interested parties to attempt to standardize policies, procedures and standards for such programs nationwide outside of the QUEST System.



As used in these Rules, the capitalized terms below shall have the following meanings:

Account: A Food Stamp Account or a Cash Account.

ACH (Automated Clearing House): A funds transfer system governed by the rules of NACHA which provides for the interbank clearing of electronic entries for participating Depository Institutions.

Acquirer: An ATM Acquirer or POS Acquirer.

Acquirer Agreement: A written agreement between an Acquirer and an Issuer or its Designated Agent pursuant to which the Acquirer confirms its agreement to be bound by and comply with these Rules, as such Rules may be amended from time to time.

Acquirer System: The telecommunications and processing system (including software and hardware) operated by or on behalf of an Acquirer through which Transactions originating at ATMs, POS or POB Terminals of that Acquirer are processed and routed to the Issuer. *(Amended August 28, 2006)*

Affiliated Retailer: Any natural person or organization (including a corporation, partnership, proprietorship, association, or cooperative) which is franchised by, or which is controlled by or under common control with, a Merchant and that has agreed with the Merchant to honor Cards. For purposes of this definition, the terms "controlled by" and "under common control with," as used with respect to any person or organization, shall mean the possession of the power to direct or cause the direction of the management and policies of such person or organization, whether through the ownership of assets or voting securities.

ANSI (American National Standards Institute): The U.S. standards group responsible for issuing U.S. standards and maintaining consistency with similar international standards.

Applicable Law: Any federal, State or local law, regulation, rule or ordinance in effect and applicable to the subject matter referenced.

ATM (Automated Teller Machine): An electronic hardware device designated by an Acquirer to accept Cards that, when activated by a Cardholder through use of a Magnetic Stripe on a Card, are capable of automatically dispensing U.S. currency directly from such device and responding to Balance Inquiries.

ATM Acquirer: A Depository Institution which owns, operates or controls ATMs, or sponsors ATMs owned, operated or controlled by a third party, at which ATMs the QUEST Mark is displayed and Cards are accepted for cash withdrawals from and Balance Inquiries to Cash Accounts. A wholly-owned operating subsidiary of a Depository Institution may act as an ATM Acquirer, provided that such Depository Institution (i) agrees to be responsible and liable for the acts and omissions of such operating subsidiary in connection herewith, and (ii) represents and warrants that it has full right, power and authority to undertake such responsibility and liability. *(Amended March 12, 2003)*

ATM Operator: An Acquirer, or Processor on behalf of an Acquirer, that operates a telecommunications and processing system (including software and hardware) through which Transactions initiated at ATMs are processed and routed, directly or indirectly, to the appropriate Issuer.

ATM Transaction: A Withdrawal from a Cash Account or Balance Inquiry that is initiated with a Card at an ATM pursuant to these Rules.

Authorization (or Authorized): The approval of a request for a Transaction by a CAS or by a third party providing Stand-In Processing for the CAS. A Transaction that is approved in accordance with these Rules is "Authorized." If a Transaction has received "Preauthorization," it is considered Authorized only in the amount of the Preauthorization.

Authorization Code: A code provided by a CAS to a Merchant as part of a Telephone Authorization indicating that a Manual Food Stamp Transaction has been approved.



Available Balance: The amount of funds that may be accessed by a Cardholder for a Transaction from a Cash Account or Food Stamp Account, respectively.

Balance Inquiry: A transaction whereby the Cardholder obtains his or her Available Balance through use of a Card at an ATM, POS or POB Terminal, including a Stand-Alone Balance Inquiry Terminal. *(Amended August 28, 2006)*

Business Day: All weekdays excluding those days on which the Federal Reserve Bank of New York is closed.

Cancellation: The termination of a Transaction prior to Authorization of the Transaction Request from the Terminal Operator to the CAS.

Card: A plastic card, issued in accordance with these Rules, which bears the QUEST Mark and which can be used to effect Transactions.

Cardholder: An individual who has been issued or authorized to use a Card.

CAS (Cardholder Authorization System): The telecommunications and processing system (including software and hardware) operated by or on behalf of an Issuer which authorizes or declines Transaction Requests.

Cash Account: An account or authorization file maintained by an Issuer that represents pre-funded or day-of-draw benefits, or both, administered by one or more Government Entities, and for which the Issuer has agreed to provide access under these Rules. Multiple benefits may be combined in a single Cash Account.

Cash Account Merchant: A person or entity that has agreed to accept Cards for purchases of goods or services from Cash Accounts and not from Food Stamp Accounts.

Cashback Transaction: A Transaction initiated with a Card at a POS Terminal and authorized from a Cash Account, in which the transaction amount debited against the Cardholder's Account is given to the Cardholder by the Merchant in whole or in part in cash.

Cash Only From Cash Account: A Transaction initiated with a Card at a POS or POB Terminal whereby only cash is provided to the Cardholder from a Cash Account. *(Amended August 28, 2006)*

Cash Transaction: A Transaction involving a Cash Account. *(Amended December 1, 2000)*

CAV (Card Authentication Value): A cryptographic value encoded on Track 2 used to validate its contents.

Chained Transactions: Multiple Transactions that occur without the reentry of the Card and/or PIN.

Completion: An electronic message from a POS Terminal to a CAS following the Preauthorization of a Transaction that indicates the actual amount of the Transaction.

Correction Request: A message from an Issuer or Acquirer identifying a System Error or Settlement Error and requesting, or providing notice of, payment of the amount of the error. *(Amended December 1, 2000)*

Correction Response: A message from an Issuer or Acquirer accepting or rejecting a Correction Request. *(Amended December 1, 2000)*

Depository Institution: An insured depository institution, as that term is defined in Section 3 of the Federal Deposit Insurance Act, as amended, or a federally insured credit union pursuant to the Federal Credit Union Act, as amended.

DES (Data Encryption Standard): The cryptographic algorithm adopted by ANSI that utilizes data encryption algorithm (DEA) as specified in ANSI X3.92-1981.



Designated Agent: A Depository Institution, Prime Contractor or Network, or affiliate controlled by or under common control with any of the foregoing, that, pursuant to an agreement with an Issuer, enters into Acquirer Agreements, Processor Agreements or additional Designated Agent Agreements on behalf of such Issuer. *(Amended June 13, 1997)*

Designated Agent Agreement: A written agreement between a Depository Institution, Prime Contractor or Network, or affiliate controlled by or under common control with any of the foregoing, and an Issuer, or a Designated Agent and a Network, pursuant to which the Depository Institution, Prime Contractor or Network, or affiliate thereof agrees to act as a Designated Agent. *(Amended June 13, 1997)*

Dispute Resolution: The process used to (i) respond to Cardholder inquiries, (ii) correct errors and (iii) resolve disagreements between Participants.

EBT or Electronic Benefits Transfer: The electronic transfer of government benefit funds to individuals through the use of card technology and ATMs and POS Terminals.

EBT Program: A program implemented by one or more Government Entities to provide government benefit funds to individuals through the use of card technology and ATMs and POS Terminals.

ESSP (Encryption Support Service Provider): An entity, other than an Acquirer that, on behalf of an Acquirer: (i) loads software into a Terminal that will accept Cards, (ii) loads or injects encryption keys into Terminals or PIN Pads, or (iii) provides Merchant help desk support which includes re-programming of Terminal software, as defined in Chapter 7 of these Rules.

Fair Hearing: An administrative hearing held pursuant to Applicable Law to determine the permissibility a charge to a Cardholder's Account. *(Amended November 15, 2001)*

Fair Hearing Correction Request: A message from an Issuer identifying a correction of a System Error required as the result of a Fair Hearing or as the result of a late request for a Fair Hearing that had been delayed for good cause, as defined by Applicable Law, and requesting, or providing notice of, payment of the amount of the error. A Fair Hearing Correction Request shall be identified as such. *(Amended November 15, 2001)*

FNS: The Food and Nutrition Service of the United States Department of Agriculture. *(Amended December 1, 2000)*

Food Stamp Account: An authorization file maintained by an Issuer that represents benefits administered by a Government Entity under the federal Food Stamp Program.

Food Stamp Authorization Code: A code provided by a CAS indicating the Telephone Authorization of a Manual Food Stamp Transaction by the CAS.

Food Stamp Merchandise Refund: A Transaction initiated with a Card at a POS Terminal to credit a Cardholder's Food Stamp Account for a return of merchandise originally purchased under the Food Stamp Program with the same Card.

Food Stamp Only Merchant: A person or entity that has agreed to accept Cards for purchases of goods or services from Food Stamp Accounts, but not from Cash Accounts, and that has been specifically authorized by FCS to accept Food Stamp Transactions under these Rules, including a Manual Only Merchant. *(Amended January 30, 1997)*

Food Stamp Program: The government benefits program operated under the authority of the Food Stamp Act of 1964, as amended.

Food Stamp Purchase: A transaction initiated with a Card at a POS Terminal located at a Food Stamp Only Merchant or Full Service Merchant that is Authorized from a Food Stamp Account and the entire Transaction amount of which is for the purchase of products or services permitted under the Food Stamp Program.



Food Stamp Transaction: A Food Stamp Purchase, Balance Inquiry to a Food Stamp Account, or Food Stamp Merchandise Refund, including a Manual Food Stamp Transaction or Store and Forward Transaction.

FSMC (Food Stamp Merchant Code): A number assigned by FCS identifying a Merchant that has been authorized by FCS to accept Food Stamps. The FSMC table is a database of all FSMCs and does not distinguish between merchants who are authorized to accept electronic Food Stamp Transactions under these Rules from those authorized to participate solely in existing paper-based systems.

Full Service Merchant: A person or entity that has agreed to accept Cards for purchases of goods or services from Cash Accounts and Food Stamp Accounts and that has been specifically authorized by FCS to accept Food Stamp Transactions under these Rules.

Government Entity: An agency, department or other instrumentality of federal, State or local government that is responsible for the distribution of government benefits pursuant to these Rules.

IIN (Issuer Identification Number): A number assigned by the American Bankers Association that identifies an Issuer for purposes of interchange of Transactions.

including: The word "including" shall have its generally accepted meaning in these Rules and its use shall not be deemed, by implication or otherwise, to exclude any items or matters not specifically referenced.

Independent Sales Organization: An organization or individual, which is not an Acquirer, that engages in Merchant solicitation, sales or service, as defined in Chapter 7, with respect to Transactions.

Initial Issuer Response Cut-Off: The close of the tenth (10th) Business Day following the original Transaction Date or, if the Correction Request is to reverse or adjust a prior Correction Request, close of the tenth (10th) Business Day following the date of such earlier Correction Request. *(Amended November 15, 2001)*

Interchange: The exchange of Authorization requests, Transaction records, funds, or information between an Acquirer and CAS through an intermediate Network or other facility.

Interoperable Transaction: A Transaction initiated with a Card issued by one Issuer at a Terminal of an Acquirer that has an Acquirer Agreement with an Issuer other than that of the Issuer that issued the Card.

ISO: International Organization for Standards.

Issuer: A Government Entity that has agreed to, or an entity that has entered into an agreement with a Government Entity or Prime contractor to, undertake the responsibilities of an Issuer under these Rules. *(Amended November 15, 2001)*

Issuer Agreement: The agreement between an Issuer and a Government Entity or Prime Contractor evidencing the Issuer's agreement to abide by these Rules and setting forth the terms and conditions of the Issuer's services on behalf of the Government Entity or Prime Contractor.

Magnetic Stripe: A stripe of magnetic tape that is affixed on the reverse side of Cards and that meets all applicable standards contained in Chapter 1.

Magnetic Stripe Reader: A device at a Terminal that is capable of reading the entire Track 2 of the Magnetic Stripe on a Card and that meets all applicable standards contained in Chapter 3.

Manual Food Stamp Transaction: An off-line Food Stamp Transaction.

Manual Only Merchant: A Merchant that has been approved specifically authorized by the FCS to accept only Manual Food Stamp Transactions under these Rules.



Merchant: A Full Service Merchant, Cash Account Merchant or Food Stamp Only Merchant, including a Manual Only Merchant. *(Amended January 30, 1997)*

Merchant Agreement: A written agreement between an Acquirer and a Merchant setting forth the respective rights and duties of the parties with respect to Transactions and obligating the Merchant to abide by these Rules, as such may be amended from time to time.

NACHA: The National Automated Clearing House Association.

Network: An organization which: (i) manages and operates a payment system that supports authentication, authorization, clearing and settlement of retail point of sale, ATM and other transactions among Network Participants bound by the Network's Operating Rules; and (ii) has entered into a Processor Agreement with an Issuer or its Designated Agent. Participants in a Network include Financial Institutions, Merchants, and organizations that provide transaction processing services to the Network. Depending on the context, the term Network may be used to apply to the payment system manager/operator, the hardware, software and telecommunication links used to interchange transactions among Network Participants, and/or all Network Participants. *(Amended May 30, 2002)*

Non-Quest Mark: Service marks separate from the QUEST Mark that relate to transactions and agreements not governed by the Rules; a single card may display both the QUEST Mark and Non-Quest marks.

PAN (Primary Account Number): The Account number that identifies the Issuer and the Cardholder and that is fully displayed and encoded on the Card.

Participant: An Issuer, Designated Agent, Acquirer, Processor, Third Party Service Provider, Network or Merchant that has entered into an agreement to participate in the routing and processing of Transactions and servicing of Cardholders or NACHA.

PIN (Personal Identification Number): A four to six character alphanumeric code issued to or selected by a Cardholder, which must be utilized by the Cardholder in conjunction with a Card to initiate a Transaction.

PIN Pad: A device through which a Cardholder may enter his or her PIN at a Terminal.

POB (Point of Banking) Terminal: An electronic hardware device used at a merchant or service provider location and designated by an Acquirer to accept Cards, that, when activated through use of a Magnetic Stripe on the Card, is capable of initiating a request for authorization for a Cash Disbursement or Balance Inquiry from a Cash Account. *(Amended August 28, 2006)*

POB Transaction: A Cash Disbursement or Balance Inquiry transaction authorized from a Cash Account that is initiated with a Card at a POB Terminal pursuant to these Rules. *(Amended August 28, 2006)*

POS (Point of Sale): The location where a Cardholder initiates a Transaction with a Merchant. *(Amended November 16, 2001)*

POS Acquirer: A Depository Institution that enters into Merchant Agreements or owns, operates or controls POS or POB Terminals which accept Cards for purchases and cash disbursements from, and Balance Inquiries to Cash Accounts and which display the QUEST Mark. A wholly-owned operating subsidiary of a Depository Institution may act as a POS Acquirer, provided that such Depository Institution (i) agrees to be responsible and liable for the acts and omissions of such operating subsidiary in connection therewith, and (ii) represents and warrants that it has full right, power and authority to undertake such responsibility and liability. *(Amended March 12, 2003 and August 28, 2006)*

POS Cash Transaction: A Purchase Only from Cash Account, Purchase with Cashback from Cash Account, Cash Only from Cash Account, Preauthorized Transaction or Balance Inquiry to a Cash Account initiated at a POS Terminal.

POS Terminal: An electronic hardware device used at the Point of Sale and designated by an Acquirer to accept Cards, including a Scrip Terminal or Stand-alone Balance Inquiry Terminal, that, when activated by a Cardholder through use



of a Magnetic Stripe on a Card, is capable of initiating a request for Authorization of a purchase from an Account or initiating a Balance Inquiry.

POS Terminal Operator: An Acquirer, or Processor or Merchant on behalf of an Acquirer, that operates a telecommunications and processing system (including software and hardware) through which Transactions initiated at POS and POB Terminals are processed and routed, directly or indirectly, to the appropriate Issuer.

POS Transaction: A Transaction Authorized from either a Cash Account or a Food Stamp Account that is initiated with a Card at a POS Terminal pursuant to these Rules.

Preauthorization: The approval, in advance, of a POS Transaction up to a specified dollar amount by a CAS to guarantee funds for a purchase of goods or services to be completed at a later time within the terms of these Rules.

Preauthorized Transaction: A POS Transaction for which a Preauthorization has been provided by a CAS.

Prime Contractor: The entity with which a Government Entity contracts for the implementation, maintenance and operation of an EBT Program.

Processor: Any company processing Transactions on behalf of an Issuer, Acquirer or Merchant, including any Terminal Operator that is not also an Acquirer or a Network.

Purchase Only from Cash Account: A Transaction initiated with a Card at a POS Terminal whereby only the exact amount of a purchase of goods or services is debited from a Cash Account.

Purchase with Cashback from Cash Account: A Transaction initiated with a Card at a POS Terminal whereby the total amount debited from a Cash Account includes the amount of a purchase of goods or services plus an amount designated by the Cardholder to be received in cash.

Quest Graphic Standards Manual: A document, as amended from time to time that contains the graphic standards for use of the QUEST Mark.

QUEST Mark: The Quest design mark and such other service marks as may be adopted from time to time in accordance with these Rules.

Registered State Representative: A representative of a Government Entity for a State who registers on behalf of such State pursuant to procedures promulgated by NACHA. (*Amended December 16, 2008*)

Resubmission: The submission for Authorization of a Manual Food Stamp Transaction or Store and Forward Food Stamp Transaction following the denial of such Transaction by the CAS.

Reversal: The electronic reversal of the full amount of a prior Transaction. A partial Reversal can take place at an ATM due to an incomplete dispense.

Rules: These EBT Operating Rules, adopted on April 25, 1996, as amended thereafter from time to time.

Sales and Credit Draft: A paper draft used to initiate a Manual Food Stamp Transaction.

Scrip: A paper or token issued by an electronic hardware device located on the premises of a Merchant that is redeemable at Point of Sale locations on such Merchant's premises for U.S. currency or for goods or services.

Scrip Terminal: An electronic hardware device designated by an Acquirer to accept Cards that, when activated by a Cardholder through use of a Magnetic Stripe on a Card, is capable of automatically dispensing Scrip.

Security Compliance Review: A compliance review of security procedures performed pursuant to these Rules by each entity that handles encryption keys for Transactions.



Settlement: The movement of funds between an Issuer and an Acquirer in satisfaction of Transactions in accordance with these Rules.

Settlement Day: The calendar date on which funds are transferred for Settlement. The period between cut-off times established by an Issuer for Settlement.

Settlement Error: An auditable out-of-balance condition between any two Settlement endpoints that does not affect any Account. *(Amended December 1, 2000)*

Stand-Alone Balance Inquiry Terminal: A POS or POB Terminal that is not part of the checkout lane and which permits the Cardholder to check the balance in his or her Food Stamp Account and Cash Account. *(Amended August 28, 2006)*

Stand-In Processing: The process whereby a third party approves or denies Transactions in place of a CAS at times when the CAS is unable to process such Transactions.

State: Any State of the United States, the District of Columbia, any territory of the United States, Puerto Rico, Guam, American Samoa, the Trust Territory of the Pacific Islands, the Virgin Islands, and the Northern Mariana Islands. *(Amended May 21, 1998)*

Store and Forward Food Stamp Transaction: A Food Stamp Transaction that is electronically stored with an encrypted PIN by a POS Terminal Operator when the POS Terminal Operator is unable to communicate with a CAS, and that is later forwarded to the CAS.

Surcharge: A fee added to a Transaction by an Acquirer, Terminal Operator or Merchant for a Transaction initiated at a Terminal.

Switch: The computer hardware and software operated by or on behalf of a Network for the purpose of routing Transactions among Participants.

System Error: An auditable processing failure that results in the improper crediting or debiting of an Account or in the failure to credit or debit an Account. Human error in Transaction data entry at the POS does not constitute a System Error, but may be addressed under the relevant EBT Program if provided for by the Governmental Entity responsible for such EBT Program. *(Amended December 1, 2000)*

Telephone Authorization: The oral approval by a CAS over the telephone of a request for a Manual Food Stamp Transaction.

Telephone Authorization Code: A number or code provided by a CAS to a Merchant indicating the CAS's Telephone Authorization of a Food Stamp Transaction.

Terminal: An ATM, POS or POB Terminal.

Terminal Operator: An ATM Operator or POS Terminal Operator.

Third Party Provider Agreement: A written agreement between an Issuer, Designated Agent or Acquirer and a Third Party Service Provider pursuant to which the Third Party Service Provider confirms its agreement to be bound by and comply with these Rules, as such Rules may be amended from time to time.

Third Party Service Provider: An organization entity or individual, other than an Issuer or an Acquirer, that provides EBT services as an Independent Sales Organization, Encryption Support Service Provider, Network and/or Processor as described in Chapter 7 of these Rules.

Track 2: The magnetic medium on Cards as defined by ISO 7813 which contains the data to be transmitted to the CAS.



Transaction: An ATM, POS or POB Transaction initiated through the use of a Card or a Terminal pursuant to these Rules. *(Amended June 13, 1997 and August 28, 2006)*

Transaction Date: The calendar date on which a request for a funds transfer pursuant to a Transaction or a Balance Inquiry was initiated.

Transaction Record: An electronic record or hard copy report of each Transaction, including ATM Transactions, POS Transactions, POB Transactions, Correction Requests and Correction Responses and Reversals sent by an Acquirer or CAS. *(Amended November 15, 2001 and August 28, 2006)*

Transaction Request: An electronic message sent by an Acquirer to a CAS requesting that the CAS authorize a Transaction.

Transaction Response: An electronic message sent to the Acquirer by the CAS in response to a Transaction Request authorizing or denying a Transaction.

Transaction Time: The local time at which the Transaction is initiated at a Terminal.

TRSM (Tamper Resistant Security Module): A tamper resistant security module as referenced in ANSI X9.24-1992.

Withdrawal from Cash Account: A transaction initiated with a Card at an ATM whereby only U.S. currency is dispensed to a Cardholder from a Cash Account.

Throughout these Rules, where such meanings would be appropriate, the singular will be deemed to include the plural and vice versa.



CHAPTER ONE - ISSUER REQUIREMENTS

SECTION 1.1 Issuer

Each Issuer shall have primary responsibility and liability for performance of the obligations of an Issuer under these Rules, regardless of whether any such obligations, including the operation of a CAS, are performed by the Issuer or by a third party on behalf of the Issuer. No delegation of duties by an Issuer to a third party shall relieve such Issuer of its liability for performance of such duties hereunder. Each Issuer shall ensure that any activity performed by a third party on its behalf is performed in compliance with these Rules and hereby warrants such compliance to each other Participant. The obligations of each Issuer shall include the following:

- a. ***Issuer Agreement.*** Each Issuer shall enter into an Issuer Agreement with one or more Government Entities or Prime Contractors pursuant to which the Issuer shall agree to be bound by and comply with these Rules. These Rules do not restrict any other terms or conditions of the Issuer Agreement, provided that such terms and conditions do not conflict with these Rules.
- b. ***Issuer Participation Agreement.*** Each Issuer shall execute and deliver to NACHA a copy of the form of agreement attached as Appendix II.
- c. ***Card Issuance.*** Each Issuer shall ensure that its Cards and PINs are issued in accordance with these Rules, regardless of whether the distribution of Cards is performed directly by the Issuer or by a Government Entity, Prime Contractor or other third party.
- d. ***Transaction Processing.*** Each Issuer shall ensure that its CAS operates in accordance with these Rules.
- e. ***Settlement.*** Each Issuer is liable for and shall settle all Authorized Transactions in accordance with these Rules, notwithstanding any negligent, wrongful or fraudulent conduct of any Cardholder. *(Amended September 27, 1996)*
- f. ***Financial Responsibility.*** In order to promote the acceptance of Transactions by Merchants and Acquirers, each Issuer that is not a government entity shall:
 - (i) Provide to the appropriate Government Entities such evidence of the Issuer's ability to fulfill its settlement obligations under these Rules as is required under the Issuer Agreements between the Issuer and Government Entities and Prime Contractors. This evidence may be in the form of financial statements, bonds, guarantees or other assurances; and
 - (ii) Upon request, provide to relevant Acquirers such evidence of the responsibility of a Government Entity for the amount of Authorized Transactions as is provided for in the applicable Issuer or Prime Contractor contract with that Government Entity. This evidence may be in the form of the relevant contract, or commitments, statements or other assurances from the Government Entity. *(Amended November 15, 2001)*
- g. ***Acquirer Agreements.*** Each Issuer shall enter into Acquirer Agreements or cause its Designated Agent(s) to enter into Acquirer Agreements pursuant to which the Acquirer shall agree to be bound by and comply with these Rules, as such Rules may be amended from time to time. Each Acquirer Agreement shall acknowledge the ownership of the QUEST Mark by NACHA and NACHA's exclusive right to license the use of the QUEST Mark under these Rules. These Rules do not restrict any other terms or conditions of the Acquirer Agreement, provided that such terms and conditions do not conflict with these Rules. Each Issuer and Designated Agent must keep a copy of each of its Acquirer Agreements at its headquarters.
- h. ***Issuer as Acquirer.*** Each Issuer may act as an Acquirer, including as Acquirer of last resort if required under an Issuer Agreement or Applicable Law, and in such capacity shall be subject to the Rules governing the activities of Acquirers. As an Acquirer for a Full Service Merchant or Food Stamp Only Merchant, the Issuer shall be responsible for converting to an electronic format each Sales and Credit Draft initiated with a Card issued by another Issuer at such Merchant.



- i. **Designated Agent Agreement.** Each Issuer may enter into one or more Designated Agent Agreements, provided that such Issuer shall be liable for the acts and omissions of its Designated Agents pursuant to such Designated Agent Agreements. A Designated Agent may act on behalf of the Issuer to enter into Acquirer Agreements or Merchant Agreements or to enter into Designated Agent Agreements with other Networks. Each Designated Agent Agreement shall require the Designated Agent to comply with these Rules, as such Rules may be amended from time to time. These Rules do not restrict any other terms or conditions of the Designated Agent Agreement, provided that such terms and conditions do not conflict with these Rules. Each Issuer and Designated Agent must keep a copy of each of its Designated Agent Agreements at its headquarters. *(Amended June 13, 1997 and March 12, 2003)*
- j. **Processor Agreements.** The Issuer, or a Designated Agent on its behalf, shall enter into an agreement with each Processor directly connected to the CAS or to a Network that is directly connected to the CAS, pursuant to which agreement such Processor shall agree to be bound by and comply with these Rules, as such Rules may be amended from time to time. These Rules do not restrict any other terms or conditions of such agreement, provided that such terms and conditions do not conflict with these Rules. Each Issuer and Designated Agent must keep a copy of each of its Processor Agreements at its headquarters.
- k. **Interoperable Transactions.** Each Issuer is responsible for establishing telecommunications links, Transaction switching facilities and any other arrangements with other Issuers necessary for the routing of Interoperable Transactions to such other Issuers, for facilitating the Settlement of such Interoperable Transactions and for facilitating the handling of Correction Requests and Correction Responses. Each Issuer shall use good faith efforts to establish agreements with other Issuers on mutually agreeable terms and conditions for the exchange of Interoperable Transactions under the Rules. If Issuers are unable to reach such agreement through their own good faith efforts, the matter shall be submitted to mediation before a neutral mediator agreed between the parties or appointed by NACHA if the parties are unable to agree. Each Issuer shall absorb all of its own expenses in connection with the mediation and shall pay one half of the fees or costs related to the services of a neutral mediator. One of the more senior executives from each Issuer shall participate in such mediation, which shall take place in such neutral location and shall be of such duration as the parties shall agree in good faith. *(Amended January 30, 1997 and December 1, 2000)*
- l. **IIN Files.** Each Issuer shall be responsible for generating, updating and distributing IIN files of all Issuers to each Processor that is directly connected to the CAS.
- m. **Surcharge Notification.** Each Issuer that receives a notification from an Acquirer that such Acquirer or its Merchant or Terminal Operator intends to impose a Surcharge shall notify each other Issuer of such fact.
- n. **Applicable Law.** Each Issuer shall comply with all Applicable Laws with respect to its activities hereunder.

SECTION 1.2 Minimum CAS Performance Standards

- a. **Availability of a CAS.** Each CAS shall be available 99.9% of the CAS's scheduled up-time under the Issuer Agreement, twenty-four (24) hours per day, seven (7) days per week.
- b. **CAS Processing Time.** Each CAS must process and respond to a Transaction Request within two (2) seconds from the time such request is received by the CAS, 98% of the time, on a monthly average basis. These calculations do not include data transmission time between the CAS and the Acquirer.
- c. **Accuracy Standard.** No more than two (2) in every 10,000 Transactions processed by a CAS may lead to a Correction Request resulting from CAS error. *(Amended December 1, 2000)*
- d. **Interface.** Each CAS shall maintain the necessary computer hardware and software to interface directly with data processing facilities required to accommodate Transaction processing.



SECTION 1.3 Message Format

Each CAS shall use the ISO 8583 message format, modified for EBT, in a version mutually agreed to between the CAS and the party connected, for all Transactions. Each CAS shall process each Transaction as a single message financial Transaction, except for Preauthorized Transactions.

SECTION 1.4 Transaction Support

Each Issuer shall be liable for each Transaction Authorized by it or by a CAS on its behalf and shall settle for the full amount of the Transaction, if the Transaction was initiated in accordance with these Rules, regardless of whether the Issuer receives funding for the Transaction. The Issuer's liability to settle a Preauthorized Transaction is addressed in Section 1.6(e). Each CAS must verify the PIN for each Transaction for which a PIN is required under these Rules. Each Issuer may, if directed by its Government Entity in accordance with its Issuer Agreement, deny all Transaction Requests originating from a specific Acquirer or Merchant, and shall have no liability for such denials.

SECTION 1.5 ATM Transactions

Each CAS must support the following ATM Transactions that are initiated and transmitted to the CAS in accordance with these Rules:

- a. *Withdrawal from Cash Account.*
- b. *Balance Inquiry from Cash Account.*

SECTION 1.6 POS Cash Transactions

Each CAS that provides access to Cash Accounts under the QUEST Mark must support the following POS Cash Transactions that are initiated and transmitted to the CAS in accordance with these Rules:

- a. *Purchase Only from Cash Account.*
- b. *Purchase with Cashback from Cash Account.*
- c. *Balance Inquiry from Cash Account.*
- d. *Cash Only from Cash Account.*
- e. ***Preauthorized Transaction from Cash Account.*** Each CAS must support Preauthorization requests in an amount of \$40 or less. Each CAS must decline any request for Preauthorization on a Food Stamp Account; Preauthorized Transactions are not permitted on Food Stamp Accounts.

Each Issuer shall be liable for and must settle each properly Preauthorized Transaction in the amount of the Completion when the amount of the Completion, including any Surcharge otherwise permitted under these Rules, is less than or equal to the amount of the Preauthorization and the Completion is received by the Issuer's CAS within two hours of the CAS's response to the Preauthorization request. If the amount of the Completion is greater than the amount of the Preauthorization, then the Issuer is liable for and must settle only the amount of the Preauthorization. An Issuer is not liable for and is not required to settle any Transaction for which the Completion is not received in a timely manner. Notwithstanding the foregoing, each Issuer may, at its sole option and as permitted under its Issuer Agreement and Applicable Law, determine to pay a Transaction even if the Completion is received later than two hours after receipt of the Preauthorization request or for an amount greater than the amount of the Preauthorization if funds are available in the Cardholder's Account. The payment of one or more such Completion messages shall not create any obligation in the Issuer to pay any other such Completion that is not communicated in accordance with the requirements of these Rules.



- f. **Key entry of PAN Transactions.** Except as otherwise provided by these Rules, each CAS shall treat POS Cash Transactions for which the PAN is key-entered at the POS Terminal the same as other POS Cash Transactions. (Amended January 9, 1998)

SECTION 1.7 Food Stamp Transactions

Each CAS that provides access to Food Stamp Accounts under the QUEST Mark must support the following Food Stamp Transactions that are initiated and transmitted to the CAS in accordance with these Rules:

- a. **Food Stamp Purchase.** If a CAS denies a Food Stamp Purchase because there are insufficient funds available in the Cardholder's Account, the CAS must indicate that the Transaction was denied due to insufficient funds.
- b. **Balance Inquiry from Food Stamp Account.**
- c. **Food Stamp Merchandise Refunds.** Upon Authorization of a Food Stamp Merchandise Refund request, each CAS shall transmit a response communicating the Available Balance in the Cardholder's Food Stamp Account including the credit for the amount of the Food Stamp Merchandise Refund. A CAS may credit a Food Stamp Merchandise Refund only to the Cardholder's Food Stamp Account.
- d. **Manual Food Stamp Transactions.**
 - (i) **Voice Authorization System.** Each CAS must provide a telephone authorization system available to Food Stamp Merchants and Full Service Merchants twenty-four (24) hours per day, seven (7) days per week for the receipt of requests for Telephone Authorizations. If a Manual Food Stamp Transaction is Authorized pursuant to such system, the CAS shall provide to the Merchant a Telephone Authorization Code to place on the Sales or Credit Draft. If Telephone Authorization is provided within twenty-four (24) hours after a Merchant accepts a Manual Food Stamp Transaction without such Authorization, the Issuer shall treat such Transaction as Authorized. Notwithstanding the Authorization of a Manual Food Stamp Transaction, the CAS may return such Transaction when it is received if the Sales and Credit Draft or electronically converted message is not properly completed.
 - (ii) **Manual Sales and Credit Drafts.** If a CAS acts as the Acquirer with respect to a Manual Only Merchant, the CAS must support the processing and Settlement of Sales and Credit Drafts that are initiated and transmitted to the CAS in paper form by such Merchant in accordance with these Rules. (Amended January 30, 1997)
 - (iii) **Electronically Converted Sales and Credit Drafts.** Each CAS must support the processing and Settlement of Sales and Credit Drafts that have been converted to an electronic format acceptable to the CAS and that are initiated and transmitted to the CAS in accordance with these Rules.
 - (iv) **Manual Transactions without Authorization.** Each CAS must support Sales and Credit Drafts that are initiated and transmitted to the CAS in accordance with these Rules and for which a Telephone Authorization was not obtained by the Food Stamp Only Merchant or Full Service Merchant due to the Merchant's inability to contact the CAS. Each CAS shall communicate to the Merchant its Authorization or denial of the Transaction, and if the Transaction is Authorized, the Issuer shall settle the Transaction in accordance with these Rules.
- e. **Store and Forward Food Stamp Transactions.** Each CAS must support Store and Forward Food Stamp Transactions that are initiated and transmitted to the CAS in accordance with these Rules.
- f. **Resubmission of Denied Manual Food Stamp Transactions and Store and Forward Food Stamp Transactions.** If the CAS denies a Manual Food Stamp Transaction or Store and Forward Food Stamp Transaction due to an error in message format, the CAS shall support the Resubmission of such Transaction during the same calendar month in which the Transaction was originally initiated. The CAS shall not accept the Resubmission of a Transaction denied for invalid PIN or insufficient funds.



- g. **Key Entry of PAN Transactions.** Except as otherwise provided in these Rules, each CAS shall treat Food Stamp Transactions for which the PAN is key-entered at the POS Terminal the same as other Food Stamp Transactions.
- h. **Food Stamp and Full Service Merchants.** Each CAS shall authorize a Food Stamp Purchase only if it originated from a Merchant whose FSMC appears on the FSMC table provided by FCS. The CAS shall retain documentation evidencing its compliance with this provision. Each Issuer shall have no duty or obligation to determine the eligibility of items purchased by the Cardholder under the Food Stamp Program.

SECTION 1.8 Available Balance Return

Each CAS must include in its Transaction Response the Available Balance in the Cardholder's Account for each of the following:

- a. **Authorized Withdrawal from Cash Account;**
- b. **Authorized Food Stamp Purchase;**
- c. **Food Stamp Merchandise Refund; and**
- d. **Denial of a Food Stamp Purchase due to insufficient funds.**

Each CAS may, at its option, also include the Available Balance in the Transaction Response for other Transactions. If a Transaction is Authorized, the remaining Available Balance communicated shall include the effect of the debit or credit to the Cardholder's Account from the Transaction, including any Transaction fee to be charged to the Cardholder's Account.

SECTION 1.9 Error Correction

Each CAS shall support Correction Requests and Correction Responses in accordance with these Rules. (Amended December 1, 2000)

SECTION 1.10 Reversal

Each CAS shall support full Reversals from an ATM or POS Terminal and partial Reversals from an ATM that are initiated and transmitted in accordance with these Rules.

SECTION 1.11 Stand-In Authorization

Each Issuer, at its option, may arrange for a third party to provide Stand-In Processing for the Issuer's CAS during periods that the CAS is not operating. Each Issuer shall be liable for and shall settle each Transaction Authorized through Stand-In Processing to the same extent as if the Transaction had been directly Authorized by the CAS.

SECTION 1.12 Maintenance of Records

Each CAS shall maintain a record of all information communicated to it pertaining to its Cardholders' Transactions for a period of at least two (2) years or longer if required by Applicable Law or the Issuer Agreement. Each CAS must maintain records of Food Stamp Transactions for at least (3) three years or any longer period required by Applicable Law. These Rules do not require any specific mode or format for record keeping.

SECTION 1.13 Third Party Service Provider Registration Program

Each Issuer using the services of a Third Party Service Provider (a) must enter into a Third Party Provider Agreement with such Third Party Service Provider pursuant to which the Third Party Service Provider agrees to be bound by and



comply with these Rules, as such Rules may be amended from time to time, and (b) must comply with the provisions of Chapter 7.

SECTION 1.14 Investigation and Audit

If NACHA has reasonable cause to question the accuracy, timeliness, completeness or reliability of any activities undertaken by or on behalf of an Issuer under these Rules, or the compliance of the Issuer with these Rules, such Issuer shall provide to NACHA full and free access to all records and systems related to the issuance of Cards and the authorization, routing, processing and Settlement of Transactions, including records and systems of the Issuer's Third Party Service Providers, for the purpose of examination or auditing such performance and compliance. At NACHA's discretion, such examination or audit may be conducted, at the Issuer's expense, by (a) an outside auditor of the Issuer's choosing, (b) NACHA or (c) a third party retained by NACHA. If such examination or audit reveals any exception to the Issuer's compliance with these Rules, the Issuer shall promptly remedy such exception. To the extent feasible, NACHA shall coordinate any such examination or audit with and rely upon any comparable examination or audit performed by a Network. These Rules shall not limit the authority of a Government Entity to audit a Participant under any agreement or Applicable Law. The agreements between Participants that are required by these Rules may provide for additional audit requirements between such Participants.

SECTION 1.15 Disaster Contingency Information

Upon request, each CAS shall release to each Participant information reasonably necessary to allow such Participant to develop a disaster contingency plan which will work in concert with the disaster contingency plan of the CAS.

SECTION 1.16 PIN Issuance and Management

- a. **PIN Issuance.** Each Issuer shall ensure that a PIN is issued to each of its Cardholders for use in connection with his or her Card in accordance with the requirements of Chapter 9. Each PIN shall be made up of alphanumeric characters from four (4) to six (6) digits. The Issuer shall ensure that appropriate procedures are utilized to preserve the security and integrity of Cards and PINs during the process of physical issuance.
- b. **DES.** Each CAS shall use DES encryption for data communication purposes to protect a Cardholder's PIN.
- c. **Implementation of Cryptography.** Each CAS must implement cryptography for its PIN management operations so as to render the PIN unintelligible during transmission to anyone not possessing the encryption keys. The CAS shall translate and decrypt PINs for Transactions within a physically secure TRSM.

The CAS must ensure that all keys by which PINs are encrypted are generated in a secure manner. The management of encryption keys must meet the standards set by the ANSI X9.8-1982; X9.24-1992; X3.92-1987. At a minimum, all encryption keys must be subject to dual control, i.e., no single person shall have control over all parts of an encryption key.

If there is a known or suspected compromise of an encryption key, internal escalation procedures must be followed and the encryption key must immediately be changed.



CHAPTER TWO - CARD SPECIFICATIONS *(Amended October 8, 2002)*

SECTION 2.1 General

Each Issuer shall ensure that each of its Cards conforms to the standards and specifications prescribed in these Rules. Each Card must be usable in all Magnetic Stripe Readers. A single Card may provide a Cardholder with access to either a Food Stamp Account or a Cash Account, or to both types of Accounts. These Rules do not limit the number of Cards that can be issued to a single household or the number of Cardholders per Card, to the extent otherwise permissible under Applicable Law and any Issuer Agreement.

These Rules also do not restrict the issuance and use of a Card in part to access accounts that are not Food Stamp Accounts or Cash Accounts, provided that any such additional account access (a) shall not impair or interfere with the use of the Card to initiate Transactions under these Rules, (b) shall not detract from, incorporate or obscure through use of another service mark, directly or by association, the QUEST Mark, (c) shall be distinguished by and clearly attributable to a separate service mark or other identifier associated with such accounts and access services, and (d) shall be clearly explained to the Cardholder, including any ability to use the Card for other purposes when no Quest accessible benefits are available [(d) effective January 1, 2000.] An Issuer shall not assign the same personal identification number for such additional account access as the PIN used to initiate Transactions, unless security procedures comparable to those set forth in Chapter 9 are utilized for purposes of such additional account access. If such security procedures are not utilized and the Issuer provides for Cardholder selection of the personal identification number for such additional account access, the Issuer shall instruct each Cardholder to select a number other than his or her PIN. *(Amended April 14, 1999)*

These Rules also do not restrict the use of an alternative Government Entity (non-network) service mark to identify transactions on Accounts solely involving Cards issued by that Issuer at Terminals supported by Acquirers that have entered into direct agreements with that Issuer or one of its Designated Agents; such transactions shall not be subject to these Rules. Such use of an alternative Government Entity (non-network) service mark (a) shall not impair or interfere with the use of the Card to initiate Transactions under these Rules, (b) shall not detract from, incorporate or obscure, directly or by association, the QUEST Mark, (c) shall clearly distinguish for Cardholders transactions that are not subject to these Rules, and (d) effective January 1, 2000, shall be clearly explained to the Cardholder, including any ability to use the Card for other purposes when no Quest accessible benefits are available [(d) effective January 1, 2000.] The use of Network service marks on Cards is governed by Rule 12.3. *(Amended June 13, 1997 and [d] Amended April 14, 1999)*

If an Issuer issues cards bearing both the QUEST Mark and another service mark identifying one or more non-QUEST benefit programs pursuant to this Section, the Issuer may issue such QUEST Cards to individual recipients even if such individuals qualify only for non-QUEST benefit programs at the time of issuance. Such cards will be considered QUEST Cards for purposes of these Rules, but transactions initiated with such Cards shall be considered Transactions only when they access an Account associated with the QUEST program. *(Amended April 14, 1999)*

All benefits redeemable without restriction for physical currency must be included in the Cash Account. *(Amended April 14, 1999)*

SECTION 2.2 Card Standards

Each Card must comply with ANSI/ISO 7813-1990, Identification Cards - Financial Transaction Cards.

- a. **QUEST Mark.** Each Issuer shall ensure that the QUEST Mark is placed on all of its Cards in conformity with the Card design illustrated in the Quest Graphic Standards Manual.
- b. **PAN.** The PAN must be fully displayed on the face of the Card. The PAN may be embossed, laser engraved, indent printed or hot stamped on the Card.



- c. **Signature Panel or Signature Image.** Each Card must either have a signature panel that the Cardholder must sign upon receipt of the Card or display a photographic or digitally printed image of the Cardholder's signature. This signature panel or signature image may be on either the front or the back of the Card, unless otherwise restricted under the Issuer Agreement. These Rules do not require that the Cardholder's name be displayed on the face of the Card.

SECTION 2.3 Magnetic Stripe Encoding

- a. **Standards Compliance.** Each Card must comply with ISO, ANSI approved standards for Track 2 encoding. Each Card must be encoded according to ISO 7813, Identification Cards - Financial Transaction Cards. The maximum character count in Track 2 shall not exceed 40, including all control characters.
- b. **PAN.** Track 2 on each Card shall contain the PAN. Each Issuer, or Government Entity on behalf of an Issuer, shall obtain an IIN from the ABA. Each Issuer shall include the IIN as the first six digits of the PAN. The PAN must comply with ISO 7812, Identification Cards - Numbering System and Registration Procedures for Issuer Identifiers. (Amended September 27, 1996)
- c. **Expiration Date.** Each non-expiring Card shall use the "4912" convention encoded on Track 2. Each Card with a specific expiration date shall use a YYMM format on Track 2. Any such expiration date shall be later than the date of issuance of the Card, and shall not be later than twenty (20) years from the date of issuance.
- d. **Service Code Field.** The Service Code Field, as that term is used in ISO 7813, on Track 2 of each Card must be encoded with the designated numeric value of "120."
- e. **CAV Field/PIN Offset.** Each Card must have either or both of:
 - (i) a cryptographic value encoded on Track 2 in the discretionary data field to validate the Track 2 data contents; (Amended September 27, 1996) or
 - (ii) a PIN offset used to validate a PIN on Track 2.

SECTION 2.4 Card Conformity (AMENDED APRIL 14, 1999)

- a. All Cards must comply with Section 2.4(a) in order to initiate Transactions. For an EBT Program utilizing existing card stock, no later than six (6) months following the date an Issuer processes its first Transaction with respect to such EBT Program, all new and replacement Cards then issued with respect to such EBT Program shall bear the QUEST Mark and comply with the Card standards set forth in Sections 2.2, 2.3, and 2.4(b), (c), (d) and (e). No such grace period shall apply to an EBT Program that does not utilize existing card stock. No later than thirty-six (36) months following such date, the QUEST Mark shall appear on all of the Issuer's outstanding Cards and all such Cards shall comply with the Card standards set forth in Sections 2.2, 2.3, and 2.4(b), (c), (d) and (e). If Cards are issued on behalf of more than one Government Entity, the foregoing phase-in periods shall apply separately with respect to Cards issued on behalf of each such Government Entity.
- b. Notwithstanding the foregoing, if during such phase-in period the Cards do not conform to the ISO standards for PANs, and such Cards have identifying information that conflicts with that of another Card base that conforms to such ISO standards, the Issuer for the non-conforming Card base may be required to immediately reissue its Cards or may be suspended from processing Transactions.
- c. An Issuer for a Governmental Entity that has determined to participate in QUEST may issue Cards bearing the QUEST Mark without the ability to initiate Transactions for a period of one year from the first issuance of such Cards to the beginning of implementation of Transactions.



SECTION 2.5 Adhesive Material on Cards

No Issuer shall affix adhesive material to a Card that would interfere with the recognition of the QUEST Mark or interfere with the normal operation of any ATM or POS Terminal.



CHAPTER THREE - ACQUIRER AND TERMINAL OPERATOR REQUIREMENTS

SECTION 3.1 General Acquirer Requirements

Each Acquirer shall have primary responsibility and liability for performance of the obligations of an Acquirer under these Rules, regardless of whether any such obligations, including acting as Terminal Operator, are performed by the Acquirer or by a third party on behalf of the Acquirer. No delegation of duties by an Acquirer to a third party shall relieve such Acquirer of its liability for performance of such duties hereunder, and each Acquirer shall ensure that any activity performed by a third party on its behalf is performed in compliance with these Rules and hereby warrants such compliance to each other Participant. The duties of each Acquirer shall include the following:

- a. **Acquirer Agreement.** Each Acquirer shall enter into an Acquirer Agreement with an Issuer or its Designated Agent stating its agreement to comply with and be bound by these Rules, as such may be amended from time to time. Each Acquirer Agreement shall acknowledge the ownership of the QUEST Mark by NACHA and NACHA's exclusive right to license the use of the QUEST Mark under these Rules. These Rules do not restrict any other terms or conditions of the Acquirer Agreement, provided that such terms and conditions do not conflict with these Rules. Each Acquirer must keep a copy of each of its Acquirer Agreements at its headquarters. An Acquirer may, at its option, enter into Acquirer Agreements with more than one Issuer.
- b. **Transaction Processing.** Each Acquirer shall ensure that Terminals it owns, operates, controls, or for which it has signed an agreement to accept Transactions, shall operate and support Transactions in accordance with these Rules.
- c. **Settlement.** Each Acquirer shall settle all Authorized Transactions in accordance with these Rules.
- d. **ATM Acquirer.** Each ATM Acquirer shall have primary responsibility and liability for operating the telecommunications and processing system (including software and hardware) through which Transactions initiated at its ATMs, including sponsored ATMs, are processed and routed, directly or indirectly, to the appropriate Issuer.
- e. **POS Acquirer.** Each POS Acquirer shall have primary responsibility and liability for operating the telecommunications and processing system (including software and hardware) through which Transactions initiated at POS Terminals it owns, operates, controls or for which it has signed an Agreement to accept EBT Transactions, are processed and routed, directly or indirectly, to the appropriate Issuer. Each POS Acquirer also shall enter into Merchant Agreements in accordance with Chapter 4 and shall be jointly and severally liable with its Merchants for the compliance of such Merchants with these Rules.
- f. **Notice and Approval of Merchants.** Each Acquirer shall provide written notice to its Issuer of the identity of each Merchant with which it has entered into an agreement under these Rules, not less than three (3) Business Days prior to the initiation of the first Transaction by such Merchant. Each Issuer shall notify a Merchant or Acquirer if the Issuer determines at any time that the incidence of Cardholder complaints regarding a Merchant or an Affiliated Retailer is unsatisfactory. In assessing the performance of the Merchant or Affiliated Retailer, the Issuer may consider Cardholder allegations including, but not limited to, those:
 - (i) Transactions that were not made as indicated on the records furnished by the Merchant or Affiliated Retailer to the Issuer; or
 - (ii) Transactions that were in amounts that differed from those indicated on such records; or
 - (iii) Transactions that were fraudulent.

If any of these allegations are determined by the Issuer to be in excess of a level satisfactory to the Issuer, the Issuer may pursue any available remedies.



- g. **Authorized Merchants for Food Stamp Transactions.** Only a Merchant that has received authorization from FCS to participate in the Food Stamp EBT Program may accept Cards for Food Stamp Transactions. Each Acquirer for a Merchant that seeks such participation shall confirm with FCS or a Government Entity designated by FCS that the Merchant is authorized to accept Cards for Food Stamp Transactions, and shall be liable for the amount of any transaction completed at a Merchant for which it has not obtained such confirmation of FCS authorization as FCS may require from time to time. Each Acquirer shall ensure that it or its Terminal Operator does not process Food Stamp Transactions for a Merchant promptly following receipt of notice that the FCS authorization of such Merchant has been revoked, rescinded or otherwise eliminated.
- h. **Third Party Service Provider Registration Program.** Each Acquirer using the services of a Third Party Service Provider, including one acting as a Terminal Operator, must (a) enter into a Third Party Provider Agreement with such Third Party Service Provider pursuant to which the Third Party Service Provider agrees to be bound by and comply with these Rules, as such Rules may be amended from time to time, and (b) comply with the provisions of Chapter 7.
- i. **Investigation and Audit.** If NACHA has reasonable cause to question the accuracy, timeliness, completeness or reliability of any activities undertaken by or on behalf of an Acquirer under these Rules, or the compliance of the Acquirer with these Rules, such Acquirer shall provide to NACHA full and free access to all records and systems related to the routing, processing and Settlement of Transactions, including records and systems of the Acquirer's Merchants and Third Party Service Providers, for the purpose of examination of or auditing such performance and compliance. At NACHA's discretion, such examination or audit may be conducted, at the Acquirer's expense, by (a) an outside auditor of the Acquirer's choosing, (b) NACHA or (c) a third party retained by NACHA at the Acquirer's expense. If such examination or audit reveals any exception to the Acquirer's compliance with these Rules, the Acquirer shall promptly remedy such exception. To the extent feasible, NACHA shall coordinate any such examination or audit with and rely upon any comparable examination or audit performed by a Network. These Rules shall not limit the authority of a Government Entity to audit a Participant under any agreement or Applicable Law. The agreements between Participants that are required by these Rules may provide for additional audit requirements between such Participants.
- j. **Applicable Law.** Each Acquirer shall comply with all Applicable Laws with respect to its activities hereunder.
- k. **Notice of Termination.** If an Acquirer terminates a Merchant Agreement other than upon the expiration of the term of that agreement, the Acquirer shall notify its Issuer.
- l. **Terminal Participation.** These Rules do not require that any minimum number or percentage of an Acquirer's ATMs participate under the QUEST Mark.

SECTION 3.2 Display of QUEST Mark

- a. **Display.** Each Acquirer shall ensure that the QUEST Mark is displayed on each of its designated ATMs and POS Terminals in accordance with these Rules and the Quest Graphic Standards Manual wherever any other payment system acceptance mark is displayed, no later than forty-five (45) days after the Acquirer first processes a Transaction from that Terminal. As set forth in the Definitions Chapter of these Rules, references to ATMs and POS Terminals or Terminals generally include only terminals that are designated to accept Cards. *(Amended May 23, 2001)*
 - (i) **Merchant.** On behalf of its Acquirer, each Merchant shall display the QUEST Mark on all signs or decals at the Merchant's POS Terminals and storefront entrance door(s) and/or window(s) wherever any other payment system acceptance mark is displayed. A QUEST Mark does not have to be displayed on designated POS Terminals or storefront entrance door(s) and/or window(s) if no other payment system accept mark is displayed at these locations. Each Merchant may use the QUEST Mark solely to inform the public that Cards will be honored at the Merchant's place of business. Each Merchant shall display the QUEST Mark in conjunction with the appropriate icon designating the type of benefits accepted in accordance with the Quest Graphic Standards Manual. Each merchant that changes status between Cash Account Merchant, Food Stamp Only Merchant or Full Service Merchant categories shall promptly modify its use of the QUEST



Mark to comply with these Rules and the Quest Graphic Standards Manual. (*Amended September 27, 1996 and May 23, 2001*)

- (ii) **ATMs.** Each Acquirer shall display the QUEST Mark on or near each ATM solely to inform the public that Cards will be honored at the ATM.
- b. **Compliance.** All displays of the QUEST Mark by Acquirers, including by Merchants on behalf of Acquirers, by way of decals, signs, printed and broadcast materials or otherwise, must comply with these Rules and the Quest Graphic Standards Manual and must be used solely to indicate that Cards are accepted for payment and not to indicate endorsement of any goods or services other than the Transactions governed by these Rules.
- c. **Termination.** Upon termination of a Merchant Agreement for any reason, the Merchant shall cease to display the QUEST Mark, shall not in any way use the QUEST Mark, and shall promptly either return to the Acquirer or destroy any materials displaying the QUEST Mark, unless the Merchant shall have entered into a new Merchant Agreement. Upon termination of its Acquirer Agreement for any reason, an Acquirer shall cease to display the QUEST Mark, shall not in any way use the QUEST Mark, and shall promptly either return to NACHA or destroy any materials displaying the QUEST Mark, unless the Acquirer shall have entered into a new Acquirer Agreement.

SECTION 3.3 Rules for Surcharges

An Acquirer may impose a Surcharge only with respect to an authorized and completed Transaction of the following type: Withdrawal from Cash Account, Purchase Only from Cash Account or Purchase with Cashback from Cash Account. No other fee may be imposed on a Cardholder by an Acquirer, Terminal Operator or Merchant as a condition to accepting a card. (*Amended January 25, 2000*)

Each Acquirer must ensure that the following requirements are met prior to permitting a Surcharge to be imposed at any of its Terminals:

- a. **Notice.** Each Acquirer must notify its Issuer of any Surcharge that it, or its Terminal Operator(s) or Merchant(s), intends to impose with respect to Transactions.
- b. **Terminal Requirements for Surcharges.** No Surcharge may be imposed with respect to an ATM Transaction unless the Cardholder is given prior on-screen notice:
 - (i) that such Surcharge will be applied;
 - (ii) of the amount or percentage of such Surcharge;
 - (iii) that the Cardholder has the option to continue or cancel the Transaction; and
 - (iv) of the name of the entity imposing the Surcharge, if the Terminal is capable of doing so.
- c. **Fee Notice Requirement for Surcharges.** Each Acquirer must ensure that a notice of any permitted Surcharge is posted on or near each Terminal to which such Surcharge applies in a location that is clearly visible and conspicuous to the Cardholder while using the Terminal. The notice must be approved by NACHA after consultation with the Acquirer and its Issuer, and shall bear the heading "Fee Notice" and meet the following minimum requirements or comparable requirements of a Network in which such Terminal participates:
 - (i) The size of the notice must be a minimum of (A) 4" x 4" at an ATM or (B) 1 2" x 4" at a POS Terminal unless incompatible with the size of the PIN Pad;
 - (ii) At a POS Terminal, the notice shall be attached to the PIN Pad unless the size of the PIN Pad makes this infeasible, in which case:
 - A. The heading "Fee Notice" must be set in a minimum of 14 point type; and



- B. The text must be set in a minimum of 10-point type.
- (iii) At an ATM, the heading "Fee Notice" must be set in a minimum of 18 point type and the text must be a minimum of 14 point type.
- d. **Fee Notice Text.** The text of the notice must identify the entity imposing the Surcharge and must contain the specific amount or percentage of the Surcharge. The Notice should read as follows unless alternative language identifying the entity imposing the Surcharge and the amount of the Surcharge is required by a Network in which the Terminal participants:
- (Full name of the entity that imposed the Surcharge, or, if the Terminal is located on a Merchant's premises and the Merchant so elects, the phrase "This Merchant") charges a fee of \$x.xx (X%) for performing this Transaction. This fee is added to the amount of your Transaction and is in addition to any fees that may be charged by the entity that issued your Card.
- e. **Reserved.** (Amended January 25, 2000)
- f. **Surcharges on a Partial Dispense.** If a Surcharge is based on a percentage of the Transaction amount, but only a portion of the funds for the Transaction are actually dispensed, the Terminal Operator must process a Correction Request to make the Surcharge proportionate to the amount actually dispensed. (Amended December 1, 2000)
- g. **Surcharge on a Reversal.** Any on-line Reversal of a complete Transaction must include as a part of the on-line Reversal a Reversal of any Surcharge associated with such Transaction.
- h. **Surcharge Receipt Requirement.** The amount of any Surcharge levied on the Cardholder must be listed as a separate item and identified either by the word "Fee" preceded by an acronym or other word or symbol identifying the entity levying the Surcharge or, if a Merchant's name appears on the receipt and the Merchant so elects, by the phrase "Merchant Fee," or if the ATM Acquirer's or owner's name appears on the receipt and that entity so elects, by the phrase "Terminal Fee."
- i. **Audit Record.** Each Terminal Operator for a Terminal where Surcharges are imposed shall maintain a separate reference in the audit record of each Surcharge imposed at such Terminal.

SECTION 3.4 Chained Transactions

No Acquirer shall permit a Chained Transaction at its Terminals unless the Transaction takes place at a Terminal that retains the Card in the Terminal for the duration of the Transaction session.

SECTION 3.5 Transaction Restrictions

Each ATM Acquirer shall not impose minimum Transaction amount limitations at its ATMs greater than \$20.00 per Transaction or maximum Transaction amount limitations less than \$200.00 per Transaction.

SECTION 3.6 Food Stamp Merchandise Refunds

Each Acquirer for a Food Stamp Only Merchant or Full Service Merchant shall be liable to the Issuer for each Merchandise Return Transaction authorized by or on behalf of the Issuer and shall settle for the full amount of such Transaction.

SECTION 3. Food Stamp Exception Processing

Each Acquirer and its respective Merchants shall bear the risk of denial, for any reason, of a Store and Forward Food Stamp Transaction or Manual Food Stamp Transaction for which Telephone Authorization was not received.



SECTION 3.8 Maintenance of Records

Each Acquirer or Terminal Operator on behalf of the Acquirer, shall maintain a record of each Transaction communicated to or by it for a period of two (2) years or such longer period of time as may be required under Applicable Law.

GENERAL TERMINAL OPERATOR REQUIREMENTS FOR ATMs AND POS TERMINALS

SECTION 3.9 Agreements

Each Terminal Operator that is not an Acquirer shall enter into a Third Party Provider Agreement with an Acquirer pursuant to which such Terminal Operator agrees to be bound by and comply with these Rules, as such Rules may be amended from time to time.

SECTION 3.10 Interface

Each Terminal Operator shall maintain the necessary computer hardware and software to interface either directly with a CAS or with a Third Party Service Provider to obtain access to one or more CAs.

SECTION 3.11 General Operating Standards

- a. ***Required Data Transmission.*** Terminals must transmit all information electronically as specified in these Rules.
- b. ***Track 2 Transmission.*** The entire unaltered contents of Track 2 must be transmitted to the CAS.
- c. ***Message Format.*** Each Terminal Operator shall use the ISO 8583 message format, modified for EBT in a version mutually agreed to between the Terminal Operator and its CAS, for all Transactions. Each Terminal Operator shall process each Transaction as a single message financial Transaction, except for Preauthorized Transactions.
- d. ***Modification of Transactions.*** No Terminal Operator may modify or alter a Transaction message except to correct a technical error in message format.

SECTION 3.12 Terminal Standards

Each Terminal Operator shall ensure that its Terminals have the following physical characteristics:

- a. ***Magnetic Stripe Reader.*** Each Terminal must have a Magnetic Stripe Reader that is used to initiate Transactions, except as otherwise provided in these Rules for certain POS Transactions. For a POS Terminal the Magnetic Stripe Reader must be at, or in immediate proximity to, the Point of Sale where a Card is accepted.
- b. ***Keyboard.*** Each Terminal must have an alphanumeric keyboard necessary for the completion of Transactions. Each Terminal keyboard must be capable of performing actions, functions, and data entry according to ANSI standards. Each Terminal must lock the keyboard and prevent additional Transactions, other than a Cancellation, from being initiated while a Transaction is being processed. The keyboard conversion from letters to numbers shall be as follows:

Alphabetic Character	Numeric Equivalent
QZ	1
ABC	2
DEF	3
GHI	4
JKL	5
MNO	6
PRS	7
TUV	8
WXY	9
(Not applicable)	0



- c. **Data Entry Keypad.** Each Terminal Operator shall provide a data entry keypad or appropriate alternative to enable the entry of alphanumeric data necessary for Transactions, including entry of PINs having from 4 to 6 characters. The alphabetic characters and their corresponding numeric equivalent shall be consistent with the keyboard format specified in these Rules.
- d. **Cancel Key.** Each Terminal must have a cancel function to enable a Cardholder to cancel a Transaction when an error has been made or when the Cardholder wishes to stop the Transaction prior to Authorization, and must otherwise support Cancellations.
- e. **Printed Documentation.** Each Terminal must have a journal printer or other capability to print records of Transactions, including, at a minimum, the information, other than Available Balance, provided on the Transaction receipt and, for Transactions that are denied, the denial reason communicated by the CAS.
- f. **Receipt Printer.** Upon completion of an Authorized Transaction, other than a Balance Inquiry, each ATM and POS Terminal must make available to the Cardholder a receipt that complies with Applicable Law and contains the following information: *(Amended October 8, 1998)*
 - (i) the final four digits only of the Card number or, solely at an ATM that allows the Cardholder the option of not receiving a receipt for each Transaction, either the final four digits of, or the entire, Card number; *(Amended October 8, 1998)*
 - (ii) information that would satisfy the receipt requirements of Regulation E, 12 C.F.R. Section 205.9, if such regulation were otherwise applicable to the Transaction; and
 - (iii) the amount of any Surcharge levied on the Cardholder in accordance with these Rules and Applicable Law, listed as a separate item in accordance with Section 3.3(h).
- g. **Time-Out Requirements.** Each Terminal Operator shall ensure that its Terminals wait a reasonable time from the sending of a Transaction Request for a response before terminating the Transaction due to the failure to receive a timely response. This period of time must account for reasonable time for the CAS to process the request, Switch timers and reasonable telecommunications time for the transmission of the Transaction Request and Transaction Response.

SECTION 3.13 Routing of Transactions

Each Terminal Operator shall establish a direct or indirect telecommunications connection for the routing of Transactions to the CAS for its Acquirer's Issuer, or to a Network or Processor directly or indirectly connected to the CAS.

SECTION 3.14 Transactions at Scrip Terminals

Scrip Terminals are considered to be POS Terminals for purposes of these Rules, except with respect to the following special conditions on the use of Scrip Terminals to effectuate Transactions:

- a. No Terminal Operator may utilize a Scrip Terminal to initiate a Food Stamp Transaction.
- b. Each Terminal Operator shall clearly and conspicuously post the following information at or near each of its Scrip Terminals:
 - (i) The location(s) or place(s) of redemption for the Scrip.
 - (ii) The days and hours of operation of such location(s).



- (iii) Any time limit within which the Scrip must be redeemed.
 - (iv) Any policy regarding lost or stolen Scrip and refunds for unused Scrip.
 - (v) Any restrictions, including daily Transaction limits, imposed by the Terminal Operator or Merchant on the number or value of Transactions for the purchase or redemption of the Scrip.
 - (vi) Notification that the Cardholder's account will be debited when the Transaction is completed, regardless of whether the Scrip is redeemed.
 - (vii) Any other restrictions on the issuance or redemption of the Scrip.
- c. Each Terminal Operator shall clearly and conspicuously print on the Cardholder's receipt or Scrip voucher any expiration date for redemption of the Scrip issued.

SECTION 3.15 Key Entry of PAN Transactions

If a POS Terminal is unable to read the Magnetic Stripe of a Card, a POS Terminal Operator, on behalf of one or more Acquirers and Merchants, may permit the manual entry of the PAN into the Terminal in order to process a POS Transaction; provided, however, that the Cardholder must be present and must enter the PIN himself or herself. Provided, further, that the Card must be present to initiate a Transaction. The POS Terminal Operator must identify each such Transaction as key-entered in the Transaction message. Key entry of the PAN is not permitted at ATMs. *(Amended January 9, 1998 and February 2, 2001)*

SECTION 3.16 Use of PIN and Magnetic Stripe Reader

Each original Transaction must be initiated by swiping, dipping or inserting a Card through a Magnetic Stripe Reader and by the Cardholder keying in the PIN at the ATM or at the PIN Pad located at or in proximity to the POS Terminal; except as otherwise expressly provided herein. The Card must be present to initiate a Transaction. *(Amended February 2, 2001)*

SECTION 3.17 IIN Files

Each Terminal Operator that uses a routing table for routing acquired Transactions shall, within seven (7) calendar days of receiving an IIN routing table update, modify its routing tables to reflect the updated routing information.

SECTION 3.18 PIN Confidentiality and Security

Each Terminal Operator shall ensure the following with respect to each Transaction it processes:

- a. upon entry into a PIN Pad, each PIN must be encrypted using DES;
- b. initial PIN encryption must be performed within either a "Physically Secure" or a "Logically Protected" TRSM and must utilize a corresponding key management technique, as specified in Section 4.1 of ANSI X9.24-1992, and as listed below:

Physically Secure TRSM

- 1. Fixed Transaction Keys

- 2. Master Keys/

Transaction Keys Unique Key per Transaction

- 3. Non-Reversibly Transformed

- 4. Derived Unique Key per Transaction

**Logically Protected TRSM**

1. Non-Reversibly Transformed
2. Derived Unique Key per Unique Key per Transaction

- c. the PIN must remain encrypted until it reaches the CAS;
- d. any translation of the PIN by a Terminal Operator, including any translation at the Acquirer's central processing computer, must be performed within a Physically Secure TRSM, without the use of software; and
- e. all keys by which PINs are encrypted must be generated in a secure manner and management of encryption keys must meet the standards as set by the ANSI X98.8-1982; X9.24-1992; and X3.92-1987. At a minimum, all encryption keys must be subject to dual control, i.e. no single person shall have control over all parts of any encryption key. If there is a known or suspected compromise of an encryption key, internal escalation procedures must be followed and the encryption key must immediately be changed.

SECTION 3.19 Confidentiality

No Terminal Operator shall reveal to any third party any information regarding a specific Transaction or series of Transactions involving any one Cardholder without such Cardholder's prior written consent, except:

- a. to each Participant involved in or necessary to effect the Transaction or resolve any alleged error regarding a Transaction;
- b. to any other person who is a party to the Transaction or is necessary to effect the Transaction;
- c. to its auditors;
- d. as required by these Rules; or
- e. as required by Applicable Law.

SECTION 3.20 [Reserved]**SECTION 3.21 Transaction Record Retention**

Each Terminal Operator shall retain prompt access to records for all Transaction activity for a minimum period of seven (7) calendar days. Such records shall be in a retrievable form on a media and format as required by the Acquirer's Issuer. Each Terminal Operator shall deliver such records to any Issuer or CAS involved in the Transaction requesting them within seven (7) Business Days' receipt of an electronic or telefacsimile transmission of a request for such records. Each Terminal Operator shall certify as to its ability to comply with the requirements of this Rule at the time it qualifies to process Transactions.

Each Terminal Operator shall participate in periodic tests of its ability to comply with the requirements of this Rule no more frequently than annually and shall correct any noncompliance identified by such test or by audit as soon as reasonably possible. Each Issuer or Acquirer may conduct an annual audit of each of its Terminal Operators' ability to retain and deliver the foregoing information on magnetic tape or other agreed to medium and shall provide at least six (6) weeks written notice of such test to each Terminal Operator required to participate therein.

ATM OPERATOR REQUIREMENTS

In addition to the general obligations of all Terminal Operators, each ATM Operator shall comply with the provisions of Sections 3.22, 3.23, 3.24, 3.25 and 3.26.



SECTION 3.22 ATM Transactions

Each ATM Operator must support each of the following ATM Transactions:

- a. **Withdrawal from Cash Account.** This Transaction may be supported by the existing checking account withdrawal function and key. The Terminal Operator must print the remaining Available Balance communicated by the CAS on the ATM receipt if the ATM is physically capable of printing such Available Balance.
- b. **Balance Inquiry from Cash Account.** This Transaction can be supported by the existing checking account balance inquiry function and key.
- c. **Correction Requests and Correction Responses.** (Amended December 1, 2000)
- d. **Reversal.** Each ATM Operator must be able to initiate Reversals and partial Reversals at the ATMs it drives.

SECTION 3.23 ATM Terminal Operating Standards

In addition to the standards identified for all Terminals, ATMs must have the following physical characteristics:

- a. **Display.** Each ATM must enable the Cardholder to view data entered into the Terminal or received in response to a Transaction. The PIN keyed in by the Cardholder must not be displayed.
- b. **Action Key.** Each ATM must have an action key to enable a Cardholder to select the function shown on the display or printed on the key.
- c. **Denial Message Content.** Each ATM must have the capability of printing or displaying for the Cardholder the following (or similar) responses or corresponding codes in connection with the associated Transaction denial message:
 - (i) invalid PIN;
 - (ii) invalid Transaction;
 - (iii) NSF (non-sufficient funds);
 - (iv) invalid Account;
 - (v) failure to receive a timely response; and
 - (vi) system malfunction.

The ATM Operator must provide an appropriate message to the Cardholder in any instance where the attempted Transaction is denied. If a specific reason cannot be provided for the rejection, the message shall refer the Cardholder to the Issuer.

SECTION 3.24 Authorization of Transactions

No ATM Operator may dispense cash at an ATM without receiving an on-line Authorization from a CAS. Each ATM Operator must request Authorization of a Transaction notwithstanding the fact that the Card used to initiate the Transaction is past its expiration date.

SECTION 3.25 Cameras



These Rules do not require cameras at ATM locations. If an ATM Acquirer does have cameras at such locations, pictures obtained with such cameras with respect to a disputed Transaction shall be provided to a requesting Issuer within seven (7) Business Days of the Acquirer's receipt of a request from the Issuer. Such pictures shall be provided and used at the sole expense of the Issuer at rates generally applicable with respect to comparable requests in commercial systems.

SECTION 3.26 Customer Service

Each ATM Operator shall respond to requests for customer assistance from Cardholders in the same manner that such ATM Operator would respond to any other commercial debit customer. For matters other than general information, each ATM Operator shall direct the Cardholder to the Issuer for that Card.

REQUIREMENTS FOR ALL POS TERMINAL OPERATORS

In addition to the general obligations of all Terminal Operators, each POS Terminal Operator shall comply with the provisions of Sections 3.27, 3.28, 3.29 and 3.30.

SECTION 3.27 Correction Requests

Each POS Terminal Operator must support the following:

- a. ***Correction Requests.***
- b. ***Correction Responses.***
- c. ***Reversals.*** Each POS Terminal Operator must support Reversals, including a Reversal due to a Cardholder's attempted cancellation of a POS Transaction following the release of the Transaction Request by the POS Terminal Operator. *(Amended November 15, 2001)*

SECTION 3.28 Transaction Restrictions

A POS Terminal Operator may not impose either minimum or maximum POS Transaction limitations on any Cardholder. Notwithstanding the foregoing, limitations on the amount of the cash portion of a Cashback Transaction are not prohibited.

SECTION 3.29 Authorization of Transactions

Each POS Terminal Operator must request authorization of a Transaction even if the Card used to initiate the Transaction is past its expiration date, except with respect to Manual Food Stamp Transactions for which a Telephone Authorization cannot be obtained and Store and Forward Food Stamp Transactions.

SECTION 3.30 POS Terminal Operating Standards

In addition to ensuring compliance with the requirements for all Terminals, each POS Terminal Operator must ensure that each POS Terminal it operates has:

- a. ***Connectivity.*** An on-line connection to the system for Transaction processing and routing, whether operated by the Acquirer or the POS Terminal Operator, or an immediate dial-up connection to that system.
- b. ***PIN Pad.*** At, or in immediate proximity to, any Point of Sale where a Card is accepted, an operating PIN Pad with an alphanumeric keyboard that meets the standards set forth in these Rules. The PIN Pad must be positioned in such a way as to afford the Cardholder reasonable privacy while entering his or her PIN and conducting a POS Transaction. Each PIN must be encrypted at the POS Terminal or in the PIN Pad if it is separate from the POS Terminal.



- c. ***Denial Message Content.*** Each POS Terminal must have the capability of printing or displaying for the cardholder the following (or similar) responses or corresponding codes in connection with the associated Transaction denial message:
 - (i) invalid PIN; or
 - (ii) other denial.

POS TERMINAL OPERATOR REQUIREMENTS FOR POS CASH TRANSACTIONS

In addition to the general obligations of all Terminal Operators and of all POS Terminal Operators, each POS Terminal Operator for a Cash Account Merchant or Full Service Merchant shall comply with the provisions of Sections 3.3 1, 3.3 2, 3.3 3, 3.3 4 and 3.3 5.

SECTION 3.31 POS Transactions

Each POS Terminal Operator for a Cash Account Merchant or a Full Service Merchant must support Purchase Only from Cash Account Transactions. This Transaction may be supported by the standard debit function at a POS Terminal.

SECTION 3.32 Optional POS Transactions

At its option, each POS Terminal Operator for a Cash Account Merchant or a Full Service Merchant may support the following Transactions:

- a. ***Purchase with Cashback from Cash Account.*** This Transaction may be supported by the existing debit function at a POS Terminal. These Rules do not place any limit on the amount of the cashback portion of a POS Transaction.
- b. ***Balance Inquiry from Cash Account.*** This Transaction may be supported by the existing checking account Balance Inquiry function and key.
- c. ***Cash Only from Cash Account.*** This Transaction may be supported by the existing debit function at the POS Terminal. These Rules do not place any limit on the amount of a Cash Only from Cash Account Transaction.
- d. ***Preauthorized Transaction from Cash Account.*** A Preauthorized Transaction is a two-part Transaction which consists of a Preauthorization request and a Completion. Each POS Terminal Operator supporting Preauthorized Transactions shall comply with the following requirements:
 - (i) ***Request*** - Each Preauthorization request transmitted to the CAS must be initiated through the use of a Magnetic Stripe Reader and a PIN entered by the Cardholder and must be for \$40.00 or less.
 - (ii) ***Completion*** - Each POS Terminal Operator must transmit a Completion to the CAS when the Cardholder completes the purchase and the final Transaction amount is entered. Each Completion must be sent within two hours after the Preauthorization request is sent. The Completion must be in an amount less than or equal to the amount of the Preauthorization response provided by the CAS.
 - (iii) ***Exceeded Time Limit/Exceeds Amount*** - If the POS Terminal Operator sends a Completion more than two hours after it sent the corresponding Preauthorization request, the Issuer shall have no liability for such Transaction. The Issuer, in its sole discretion, may accept a Completion in accordance with the provisions of Chapter I notwithstanding that it was not timely presented. The Issuer also shall have no liability for a Transaction if the amount of the Completion is in excess of the amount of the Preauthorization. The Issuer, in its sole discretion, may accept a Completion in accordance with the provisions of Chapter I notwithstanding that the amount of the Completion exceeds the amount of the Preauthorization.



SECTION 3.33 Refunds on Cash Account Transactions

A POS Terminal Operator may not process an electronic refund to a Cash Account with respect to a previously Authorized Transaction. A refund associated with a POS Cash Transaction must be handled by the Merchant in the same manner as the Merchant would handle a refund with respect to a cash purchase.

SECTION 3.34 Store and Forward Transactions and Resubmissions

Store and Forward Transactions (excluding Preauthorized Transactions) and Resubmissions of previously denied Transactions are not permitted with respect to POS Cash Transactions.

SECTION 3.35 Cashback Reporting

Effective January 1, 1998, each POS Terminal Operator that processes Cashback Transactions shall transmit, for each such Cashback Transaction, the amount of cash given to a Cardholder in the Transaction message to the CAS. Following January 1, 1998, no POS Terminal Operator may initiate a Cashback Transaction without complying with this Rule.

REQUIREMENTS FOR POS TERMINAL OPERATORS PROCESSING FOOD STAMP TRANSACTIONS

In addition to the general obligations of all Terminal Operators and of all POS Terminal Operators, each POS Terminal Operator for a Food Stamp Only Merchant or a Full Service Merchant shall comply with the provisions of Sections 3.36, 3.37 and 3.38.

SECTION 3.36 Food Stamp Transactions

Each POS Terminal Operator for a Food Stamp Only Merchant or Full Service Merchant must support the following Food Stamp Transactions:

- a. ***Food Stamp Purchase.*** A Food Stamp Purchase may be initiated only at a POS Terminal located on the premises of a Food Stamp Only Merchant or Full Service Merchant and may not include any return of cash to the Cardholder. Upon completion of an Authorized Food Stamp Purchase or a Food Stamp Transaction declined for insufficient funds, the POS Terminal Operator must print the Available Balance communicated by the CAS on the receipt.
- b. ***Food Stamp Merchandise Refund Transaction.*** Each Food Stamp Merchandise Refund may be processed only with the Card that initiated the original Transaction and to the Food Stamp Account from which funds were debited. Each Food Stamp Merchandise Refund request must be initiated through the use of a PIN and a Magnetic Stripe Reader or as a Manual Food Stamp Transaction. No POS Terminal Operator may process a Food Stamp Merchandise Refund request (i) in an amount that exceeds the original Transaction amount, or (ii) for a Merchant other than the Merchant at which the original Transaction was completed. No Merchant may provide a Food Stamp Merchandise Refund in cash. The POS Terminal Operator must print on the receipt for a Food Stamp Merchandise Refund Transaction the Available Balance communicated by the CAS.

SECTION 3.37 Optional Food Stamp Transactions

(Amended January 9, 1998)

Each POS Terminal Operator that supports Food Stamp Transactions may, at its option, also support the following Transactions:



- a. ***Balance Inquiry from Food Stamp Account.***
- b. ***Manual Food Stamp Transactions.*** Each POS Terminal Operator for a Food Stamp Only Merchant or Full Service Merchant that accepts Manual Food Stamp Transactions must accept Sales and Credit Drafts and convert these drafts to electronic messages for submission to the CAS. Each converted Sales and Credit Draft must be received by the CAS in an electronic format acceptable to the CAS no later than fifteen (15) calendar days from the date of the Transaction Authorization.
- c. ***Store and Forward Food Stamp Transactions.*** If at any time, a POS Terminal Operator is unable electronically to communicate with a CAS or any entity providing Stand-In Authorization for the CAS because of a technical malfunction, the POS Terminal Operator may electronically store for up to twenty-four (24) hours and forward a Food Stamp Transaction, provided that the Cardholder's PIN is stored only in an encrypted format. The Transaction must be forwarded within twenty-four (24) hours of the original initiation of the Transaction, provided that this period shall be extended in twenty-four (24) hour increments if the POS Terminal Operator continues to be unable to communicate with the CAS or any entity providing Stand-In Processing for the CAS during each such twenty-four (24) hour period. Each Store and Forward Food Stamp Transaction is conducted at the risk and liability of the Acquirer and the Merchant. Any allocation of liability between the Acquirer and the Merchant shall be governed by the Merchant Agreement.
- d. ***Resubmission of Denied Manual Food Stamp Transactions and Store and Forward Food Stamp Transactions.*** A POS Terminal Operator may not resubmit any Transaction for which a denial has been received due to:
 - (i) an invalid PIN (For Store and Forward Food Stamp Transactions only); or
 - (ii) insufficient funds in the Cardholder's Account. If a Manual Food Stamp Transaction or Store and Forward Food Stamp Transaction is denied by the CAS due to an error in message format, the Terminal Operator may correct the problem that led to denial of the Transaction and resubmit such corrected Transaction for Authorization and payment by the CAS. Such Resubmission shall be made as promptly as possible following the receipt of such denial message, but in no event later than the last calendar day of the month in which the Transaction was originally initiated.

SECTION 3.38 Food Stamp Merchant Code

For each Food Stamp Transaction, the POS Terminal Operator must transmit the FSMC as part of the Transaction Message.



CHAPTER FOUR - MERCHANT AGREEMENT REQUIREMENTS

SECTION 4.1 General

- a. Each Merchant that wishes to display, or allow its Affiliated Retailers to display, the QUEST Mark and to honor Cards must enter a Merchant Agreement with an Acquirer. Each Merchant Agreement, to the extent permitted under Applicable Law, must contain the substance of the provisions relating to Merchants in these Rules and shall obligate the Merchant to comply with all applicable policies of these Rules, as such Rules may be amended from time to time. If a Merchant acts as a POS Terminal Operator, the Merchant Agreement shall provide that the Merchant will comply with each provision of these Rules applicable to a POS Terminal Operator. Since these Rules may be amended from time to time, the Acquirer shall be responsible for effecting any necessary and appropriate amendments to its Merchant Agreement. The Merchant Agreement may, in addition, contain such other terms and conditions as may be mutually agreed upon between the Merchant and the Acquirer; provided, however, that such additional terms and conditions may not conflict with any provisions contained in these Rules. In the event of any such inconsistency or conflict, these Rules shall govern.
- b. Each Acquirer that enters a Merchant Agreement shall be jointly and severally liable with the Merchant for each of the Merchant's obligations set forth in these Rules, including any Rules applicable to the Merchant acting as a POS Terminal Operator.
- c. All Merchant forms (including Merchant applications and Merchant Agreements) must clearly state the Acquirer's name and location in letter size consistent with the rest of the Merchant Agreement printing and in such a manner that the Acquirer's name can be readily discerned by the Merchant.
- d. Each Merchant Agreement must be signed by both the Acquirer and the Merchant and kept on file by the Acquirer and the Merchant at their respective headquarters.

SECTION 4.2 Acceptance of Cards

Each Full Service Merchant and Cash Account Merchant shall promptly honor each valid Card when such Card is presented by a Cardholder with a valid PIN for the purpose of engaging in a Cash Account Transaction. Each Full Service Merchant and Food Stamp Only Merchant shall promptly honor each valid Card when such Card is presented by a Cardholder with a valid PIN for the purpose of engaging in a Food Stamp Transaction.

SECTION 4.3 Requirement of PIN/Cardholder Signature

Each Merchant shall require that the Cardholder enter his or her PIN at, or in proximity to, the Point of Sale when initiating a POS Transaction, except as provided in these Rules. Whenever the PIN can be validated by either the CAS or a third party performing Stand-In Processing on behalf of the CAS, the Merchant shall ensure that the Cardholder is not required to present a signature or any other form of identification unless the Merchant has grounds to suspect fraud. Each Merchant must obtain the Cardholder's signature if technical problems prevent the Cardholder from entering his or her PIN and the Merchant elects to use a Sales and Credit Draft. The Merchant may also request additional identification if it has grounds to suspect fraud.

SECTION 4.4 Return of Cards

Each Merchant may return to a Cardholder a Card inadvertently left at a Merchant location only if the Cardholder provides positive identification. If the Cardholder does not pick up the Card within forty-eight (48) hours of its discovery by the Merchant or does not provide positive identification, the Merchant must notify the Issuer and then destroy the Card.



SECTION 4.5 Confiscation of Cards

No Merchant shall be required to confiscate a Card at the Point of Sale for any reason.

SECTION 4.6 Display of QUEST Mark

On behalf of its Acquirer, each Merchant shall display the QUEST Mark in accordance with the provisions of Section 11, Chapter 11, and the Quest Graphic Standards Manual.

SECTION 4.7 Manual Only Merchants

Each Manual Only Merchant may accept Manual Food Stamp Transactions in accordance with the provisions governing such Transactions only under agreement with an Acquirer that processes or arranges for the processing of the Sales and Credit Drafts of such Manual Only Merchant.

SECTION 4.8 Manual Food Stamp Transactions

Each Food Stamp Only Merchant or Full Service Merchant may support Manual Food Stamp Transactions in accordance with these Rules, and the Merchant Agreement. (Amended January 30, 1997)

- a. ***Conditions.*** If, at any time, a Merchant or its POS Terminal Operator is unable to electronically communicate with a CAS or any entity providing Stand-In Processing for the CAS, because of a technical malfunction, the Merchant may process a Manual Food Stamp Transaction.
- b. ***Telephone Authorization.*** If the conditions in the preceding paragraph for a Manual Food Stamp Transaction have been met, the Merchant shall attempt to obtain a Telephone Authorization for the Transaction. For each Sales and Credit Draft, the Merchant must make a telephone call to the CAS and receive from the CAS a Telephone Authorization for the amount of the Transaction and a Food Stamp Authorization Code, which the Merchant must record on the Sales and Credit Draft. If the Merchant does not receive Telephone Authorization for a Manual Food Stamp Transaction, the Transaction is conducted at the Merchant's risk and liability, and the Acquirer will not receive payment if there are insufficient funds in the Cardholder's Account. The Merchant must call within twenty-four (24) hours of accepting the Transaction to attempt to obtain Telephone Authorization. If the CAS provides Telephone Authorization within such twenty-four (24) hour period, the Transaction shall be treated as Authorized.
- c. ***Manual Sales and Credit Drafts.*** Each Merchant processing Manual Food Stamp Transactions must ensure that a Sales and Credit Draft is completed for each such Transaction containing the following information:
 - (i) an imprint of the Card or a manually entered PAN;
 - (ii) Transaction date;
 - (iii) time;
 - (iv) dollar amount;
 - (v) voucher number;
 - (vi) Telephone Authorization Code;
 - (vii) Transaction type;
 - (viii) Terminal number (if any);
 - (ix) street address
 - (x) one of the following: FSMC, Merchant ID, or Merchant trade name, city and State.

When such Sales and Credit Draft is converted to an electronic message for transmission to the CAS, the electronic message for each Transaction must comply with ANSI X9, Draft Standards for Trial Use - Financial Services EBT Processor Interface Technical Specifications or any successor or modified standard acceptable to the CAS and must contain:

- (i) the PAN;



- (ii) Transaction date;
- (iii) dollar amount;
- (iv) voucher number;
- (v) Telephone Authorization Code;
- (vi) Transaction type;
- (vii) Terminal number if any;
- (viii) FSMC;
- (ix) Acquirer ID; and
- (x) Merchant trade name, street address, city and State.

- d. **Cardholder Signature.** The Cardholder must sign the Sales and Credit Draft, and the Merchant must compare the signature on the Card to the signature on the Sales and Credit Draft and may submit the Sales and Credit Draft only if the signatures appear to be the same.

SECTION 4.9 Confidentiality

No Merchant shall reveal to any third party any information regarding a specific Transaction or series of Transactions involving any one Cardholder without such Cardholder's prior written consent, except:

- a. to each Participant involved in or necessary to effect the Transaction or resolve any alleged error regarding a Transaction;
- b. to any other person who is a party to the Transaction or is necessary to effect the Transaction;
- c. to its auditors;
- d. as required by these Rules; or
- e. as required by Applicable Law.

SECTION 4.10 Customer Service

Each Merchant shall respond to requests for customer assistance from Cardholders in the same manner that such Merchant would respond to any other commercial customer. For matters other than general information, a Merchant shall direct the Cardholder to the Issuer for that Card.

SECTION 4.11 Merchant Qualification Standards

- a. **Minimum Requirements.** Prior to entering into a Merchant Agreement, each Acquirer must ascertain that the prospective Merchant is financially responsible from available records, independent reports and other appropriate means. Such information may also be obtained by credit reports, personal and/or business financial statements, income tax returns, or such other information as is available to, and deemed appropriate by, the Acquirer. The Depository Institution that agrees with a Government Entity or Prime Contractor to act as Acquirer of last resort with respect to Food Stamp Only Merchants is not subject to this paragraph (a) with respect to such Merchants.
- b. **Inspection.** To the extent possible the Acquirer shall conduct an investigation of the Merchant including, whenever feasible, an inspection of the Merchant's premises.
- c. **Documentation of Investigation.** Any investigation must be well documented and all documents related to the investigation must be kept on file at the Acquirer's place of business for a minimum of two (2) years following termination of the Merchant Agreement.

SECTION 4.12 Merchant Participation



Each Merchant Agreement shall provide the Acquirer with the authority to terminate the Merchant Agreement or suspend processing for the Merchant if properly directed to do so by a Government Entity. Each Merchant Agreement for a Food Stamp Only Merchant or a Full Service Merchant shall provide that the Merchant will be liable to the Issuer for the amount of any transaction that the Issuer authorizes as a Food Stamp Transaction at a time when the Merchant is not eligible to accept Food Stamp Transactions under FCS regulations. Each Merchant Agreement shall require the Merchant to provide prompt notice to the Acquirer if FCS revokes, rescinds or otherwise eliminates the Merchant's authority to accept Food Stamp Transactions.

SECTION 4.13 Third Party Service Provider Registration Program

Each Merchant using the services of a Third Party Service Provider (a) must enter into a Third Party Provider Agreement with such Third Party Service Provider pursuant to which the Third Party Service Provider agrees to be bound by and comply with these Rules, as such Rules may be amended from time to time, and (b) must comply with the provisions of Chapter 7.

SECTION 4.14 Security Compliance Review

MERCHANTS WHICH DRIVE TERMINALS, PERFORM ENCRYPTION SUPPORT SERVICES OR PROCESS TRANSACTIONS FOR THEIR OWN STORE LOCATIONS ONLY ARE NOT REQUIRED TO REGISTER AS THIRD PARTY SERVICE PROVIDERS; HOWEVER, THEY MUST COMPLETE A SECURITY COMPLIANCE REVIEW.

SECTION 4.15 Authorization of Transactions

Each Merchant must request Authorization of a Transaction even if the Card used to initiate the Transaction is past its expiration date, except with respect to Manual Food Stamp Transactions for which a Telephone Authorization cannot be obtained and Store and Forward Food Stamp Transactions.

SECTION 4.16 Affiliated Retailer Performance

Except where otherwise specifically provided in these Rules, each Merchant shall ensure that each of its Affiliated Retailers complies with these Rules to the same extent as if such Affiliated Retailer were a Merchant.

SECTION 4.17 Mandatory Transactions

A Merchant that accepts Cards for POS Cash Transactions must support Purchase Only from Cash Account Transactions and any related Correction Requests and Correction Responses. A Merchant that accepts Cards for Food Stamp Transactions must support Food Stamp Purchase and Food Stamp Merchandise Refund Transactions and any related Correction Requests and Correction Responses. Other Transactions are at the Merchant's option. *(Amended December 1, 2000)*



CHAPTER FIVE - ERROR RESOLUTION *(Amended November 15, 2001)*

SECTION 5.1 General

- a. **Cooperation.** Each Participant involved in a Transaction error, whether a System Error, Settlement Error or otherwise, shall cooperate in good faith in attempts to resolve such error, regardless of whether the error resolution procedures of this Chapter apply. If an Acquirer initiates a System Error Correction Request in good faith outside of the time lines provided by this Chapter, nothing in this Chapter shall preclude such claim from being addressed under the relevant EBT Program if provided for by the Governmental Entity responsible for such EBT Program. *(Amended June 17, 2005)*
- b. **Consistency with FNS Regulations.** No provision of this Chapter 5 should be read to require any Participant to take any action inconsistent with FNS Regulations. *(Amended June 17, 2005)*
- c. **Issuer Obligations.** An Issuer may not reject an Acquirer's Correction Request because of limitations on Account access under Applicable Law or the Issuer Agreement, except as expressly provided herein.
- d. **No Modifications at POS.** A Merchant may not modify an amount originally entered at the point of sale. The preceding sentence does not preclude a Merchant from modifying an erroneous amount entered on a Sales and Credit Draft if the Cardholder is present and specifically approves the modification.
- e. **Notice of Correction Requests and Responses.** Notice of a Correction Request or Correction Response shall be deemed to have been given:
 - (i) With respect to an entry into an automated adjustment system or other form of electronic communication, such as email, on the day the Correction Request or Correction Response is sent
 - (ii) With respect to a faxed communication, on the day Correction Request or Correction Response is sent
 - (iii) With respect to a communication sent by overnight delivery service, on the Business Day following the day that the Correction Request or Correction Response is sent
 - (iv) With respect to a communication sent by U.S. mail, on Business Day such communication is received
- f. **Holds on Accounts.** Nothing in these Rules shall affect the right, authority or obligation of an Issuer under any Issuer Agreement or Applicable Law to place a hold on an Account pending payment of a Correction Request.

SECTION 5.2 Acquirer-Initiated Corrections for Cash Transactions

Each Acquirer must promptly balance and reconcile its Terminals and accounts, and must initiate a Correction Request for Cash Transactions promptly upon discovery of a System Error or Settlement Error.

- a. **Credit to Issuer (Cash Transactions).** Examples of errors for which Correction Requests should be issued to credit an Issuer include: duplicate Transactions and ATM under-dispense.
 - (i) **Time Lines**
 - A. **Acquirer Request.** Each Acquirer must provide notice of a System Error Correction Request for Cash Transactions within six (6) Business Days of discovery of a System Error requiring credit to a Cash Account, or as promptly as possible thereafter if the Acquirer in good faith, is unable to provide notice within such time frame. Each Acquirer must provide notice of a Settlement Error Correction Request to credit an Issuer within twenty (20) Business Days of the original Transaction Date, or as promptly



as possible thereafter if the Acquirer, in good faith, is unable to provide notice within such time frame.

- B. Issuer Response.** No response is required other than settlement of the Correction Request as provided below.

(ii) Documentation

- A. Acquirer Request.** Each Correction Request by an Acquirer to credit an Issuer in respect of a Cash Transaction must contain at least the following information:

- I. Transaction identification or trace number
- II. Transaction amount
- III. Transaction Date and Transaction Time
- IV. Terminal identification number
- V. Cardholder PAN
- VI. Explanation of the alleged error sufficient to allow the Cardholder of the Correction Request to evaluate the claim
- VII. Contact information for communications regarding the Correction Request
- VIII. Listing of any accompanying documentation
- IX. If the Correction Request relates to an earlier erroneous Correction Request, the date of the earlier Correction Request and any other information reasonably necessary to identify the earlier Correction Request.

- B. Issuer Response.** No response is required other than settlement of the Correction Request as provided below. However, if the Issuer rejects the Correction Request, the Correction Response must contain a reasonable explanation of the basis for rejection (e.g., duplicate Correction Request). No additional documentation is required.

(iii) Follow-up

- A. Approval/No Response.** The amount of the Correction Request must be included in the Settlement for correction items and credited to the Cardholder's Cash Account within four (4) Business Days following notice of a System Error Correction Request. The amount of the Correction Request must be included in the Settlement for correction items within ten (10) Business Days following notice of a Settlement Error Correction Request. In each case, the Acquirer must pay such amount.

- B. Denial.** If the Issuer issues a Correction Response rejecting a credit (e.g., on the basis of a prior or duplicate correction), no further action is required of the Issuer or Acquirer.

- b. Debit to Issuer (Cash Transactions).** Examples of errors for which Correction Requests should be issued to debit an Issuer include: erroneous reversal, ATM over-dispense and prior correction credit provided to Issuer in error.

(i) Time Lines



- A. **Acquirer Request.** Each Acquirer must provide notice of a System Error Correction Request to debit an Issuer for a Cash Transaction (a) within six (6) Business Days of the original Transaction Date, or (b) if the Correction Request is to reverse or adjust a prior correction credit to the Issuer, within six (6) Business Days of the date of such earlier Correction Request. Correction Requests for System Errors initiated after that period may be automatically rejected. Each Acquirer must provide notice of a Settlement Error Correction Request to debit an Issuer for a Cash Transaction within twenty (20) Business Days of the original Transaction Date, or as promptly as possible thereafter if the Acquirer, in good faith, is unable to provide notice within such time frame. Each Issuer must make a good faith effort to process late Correction Requests for Settlement Errors.
- B. **Issuer Response for Transactions NOT Subject to Fair Hearing Requirements.** The procedures in this Subsection (B) apply if an Acquirer's Correction Request relates to a Cash Transaction that is NOT subject to State Fair Hearing procedures prior to the charging of a Correction Request to a Cardholder's Cash Account. Each Issuer must issue its Correction Response for System Errors promptly upon determining that either (i) that it rejects the Correction Request or (ii) that it accepts the Correction Request and there are sufficient funds available to satisfy such Correction Request. The Issuer shall accept or reject a Correction Request for a System Error by the Initial Issuer Response Cut-Off unless it determines that the Correction Request is valid but there are insufficient funds in the Cardholder's Cash Account with which to satisfy such Correction Request. If there are insufficient funds to pay an otherwise valid System Error Correction Request, the Issuer thereafter shall daily review whether sufficient funds have become available in the Cardholder's Cash Account, giving first priority to payment of the Correction Request out of any funds in or added to the Cardholder's Cash Account, and shall issue its System Error Correction Response the next Business Day following the availability of sufficient funds in the Cardholder's Cash Account. If sufficient funds do not become available in the Cardholder's Cash Account by the close of business on the last calendar day of the month following the Correction Request, the Issuer shall notify the Acquirer of its Correction Response rejecting the Correction Request for insufficient funds within two (2) Business Days. If information comes to the attention of the Issuer after the Initial Issuer Response Cut-Off that justifies rejection of a Correction Request, the Issuer may, notwithstanding the foregoing, issue a Correction Response rejecting the Correction Request at any time prior to settlement of the Correction Request. Each Issuer must issue its Correction Response to Settlement Error Correction Requests within ten (10) Business Days of notice of the Correction Request, and may not reject such Correction Request for insufficient funds.
- C. **Issuer Response for Transactions Subject to Fair Hearing Requirements.** The procedures in this Subsection (C) apply if an Acquirer's Correction Request relates to a Cash Transaction that IS subject to State Fair Hearing procedures prior to the charging of a Correction Request to a Cardholder's Cash Account. Each Issuer shall make a preliminary determination whether to accept or reject a System Error Correction Request by the Initial Issuer Response Cut-Off.
 - I. **Rejection.** If the Issuer determines to reject a System Error Correction Request, it shall notify the Acquirer by the Initial Issuer Response Cut-Off. If information comes to the attention of the Issuer after the Initial Issuer Response Cut-Off that justifies rejection of a Correction Request, the Issuer may, notwithstanding the preceding sentence, issue a Correction Response rejecting the Correction Request at any time prior to settlement of the Correction Request.
 - II. **Acceptance.** If the Issuer makes a preliminary determination to accept a System Error Correction Request, it shall provide such notice to the Cardholder as may be required by Applicable Law.
 - (a) **No Hearing Request.** If the Cardholder does not request a Fair Hearing within the period applicable to Food Stamp Transactions and there are sufficient funds available in the Cash Account to fully satisfy the System Error Correction Request, the Issuer shall issue its Correction Response the next Business Day. If the Cardholder does not request a Fair Hearing within the period applicable to Food Stamp Transactions and there are insufficient funds available in the Cash Account to fully satisfy the Correction Request,



the Issuer thereafter shall daily review whether sufficient funds have become available in the Cardholder's Cash Account, giving first priority to payment of the Correction Request out of any funds in or added to the Cardholder's Cash Account, and shall issue its System Error Correction Response the next Business Day following the availability of sufficient funds in the Cardholder's Cash Account. If sufficient funds do not become available in the Cardholder's Cash Account by the close of business on the last calendar day of the month following the Correction Request, the Issuer shall notify the Acquirer of its Correction Response rejecting the Correction Request for insufficient funds within two (2) Business Days. If information comes to the attention of the Issuer after the Initial Issuer Response Cut-Off that justifies rejection of a Correction Request, the Issuer may, notwithstanding the foregoing, issue a Correction Response rejecting the Correction Request at any time prior to settlement of the Correction Request.

- (b) **Hearing Request.** If the Cardholder requests a Fair Hearing within the period applicable to Food Stamp Transactions, the Issuer shall provide a Correction Response that rejects the Correction Request on the basis of the Fair Hearing request.

(ii) Documentation

- A. **Acquirer Request.** Each Correction Request by an Acquirer to debit an Issuer in respect of a Cash Transaction must contain at least the following information:
- I. Transaction identification or trace number
 - II. Transaction amount
 - III. Transaction Date and Transaction Time
 - IV. Terminal identification number
 - V. Cardholder PAN
 - VI. Explanation of the alleged error sufficient to allow the Cardholder of the Correction Request to evaluate the claim
 - VII. Contact information for communications regarding the Correction Request
 - VIII. Listing of any accompanying documentation
 - IX. A copy of the audit tape or Terminal journal and ATM balancing sheets, upon request only
 - X. If the Correction Request relates to an earlier erroneous Correction Request, the date of the earlier Correction Request and any other information reasonably necessary to identify the earlier Correction Request, and, upon request only, a copy of such earlier Correction Request.

- B. **Issuer Response.** If the Issuer rejects the Correction Request, the Correction Response must contain:
- I. a reasonable explanation of the basis for rejection (e.g., failure by Acquirer to provide all required information, duplicate Correction Request, or unverifiable PAN)
 - II. documents (including electronic records) reasonably supporting such rejection, such as a Transaction record of a reversal of the underlying Transaction, upon request only.

(iii) Follow-up

**A. *Timely Correction Response Received***

- I. **Approval.** If the Issuer accepts the Correction Request and (i) there are sufficient funds in the Cardholder's Cash Account to satisfy such Correction Request by the Initial Issuer Response Cut-Off, (ii) sufficient funds become available before the close of business on the last calendar day of the month following the Correction Request or (iii) the Correction Request relates to a Settlement Error, the Issuer shall include the correction in the Settlement of correction items within the next three (3) Business Days.
 - II. **Denial.** If the Issuer rejects the Correction Request, it must notify the Acquirer in accordance with the time limits and documentation requirements above. If there is a dispute regarding the validity of the Issuer's rejection of a Correction Request, the parties to any such dispute shall take all steps reasonably practicable to resolve such dispute by mutual agreement within thirty (30) calendar days of notice of the Issuer's Correction Response.
- B. **No Timely Correction Response Received.** If the Issuer fails to provide a timely Correction Response or payment of a Correction Request in accordance with the procedures above, the Issuer shall be responsible for settling the Correction Request regardless of the availability of funds in the Cardholder's Cash Account.

SECTION 5.3 Acquirer-Initiated Corrections for Food Stamps

Each Acquirer must promptly balance and reconcile its POS Terminals and accounts, and must initiate a Correction Request for Food Stamp Transactions promptly upon discovery of a System Error or Settlement Error.

- a. **Credit to Issuer (Food Stamp Transactions).** Examples of errors for which Correction Requests should be issued to credit an Issuer include: duplicate Transactions.

(i) **Time Lines**

- A. **Acquirer Request.** Each Acquirer must provide notice of a System Error Correction Request for Food Stamp Transactions within six (6) Business Days of discovery of a System Error requiring credit to a Food Stamp Account, or as promptly as possible thereafter if the Acquirer in good faith, is unable to provide notice within such time frame. Each Acquirer must provide notice of a Settlement Error Correction Request to credit an Issuer within twenty (20) Business Days of the original Transaction Date, or as promptly as possible thereafter if the Acquirer, in good faith, is unable to provide notice within such time frame.
- B. **Issuer Response.** No response is required other than settlement of the Correction Request as provided below.

(ii) **Documentation**

- A. **Acquirer Request.** Each Correction Request to credit an Issuer in respect of a Food Stamp Transaction must contain at least the following information:
 - I. Transaction identification or trace number
 - II. Transaction amount
 - III. Transaction Date and Transaction Time
 - IV. Terminal identification number



- V. Merchant FNS number
 - VI. Cardholder PAN
 - VII. Explanation of the alleged error sufficient to allow the Cardholder of the Correction Request to evaluate the claim
 - VIII. Contact information for communications regarding the Correction Request
 - IX. Listing of any accompanying documentation
 - X. If the Correction Request relates to an earlier erroneous Correction Request, the date of the earlier Correction Request and any other information reasonably necessary to identify the earlier Correction Request.
- B.** ***Issuer Response.*** No response is required other than settlement of the Correction Request as provided below. However, if the Issuer rejects the Correction Request, the Correction Response must contain a reasonable explanation of the basis for rejection (e.g., duplicate Correction Request). No additional documentation is required.

(iii) Follow-up

- A.** ***Approval/No Response.*** The amount of the Correction Request must be included in the Settlement for correction items and credited to the Cardholder's Food Stamp Account within four (4) Business Days following notice of a System Error Correction Request. The amount of the Correction Request must be included in the Settlement for correction items within ten (10) Business Days following notice of a Settlement Error Correction Request. In each case, the Acquirer must pay such amount.
 - B.** ***Denial.*** If the Issuer issues a Correction Response rejecting a credit (e.g., on the basis of a prior or duplicate correction), no further action is required of the Issuer or Acquirer.
- b. Debit to Issuer (Food Stamp Transactions).** Examples of errors for which Correction Requests should be issued to debit an Issuer include: erroneous reversal or prior correction credit provided to Issuer in error.

(i) Time Lines

- A.** ***Acquirer Request.*** Each Acquirer must provide notice of a System Error Correction Request to debit an Issuer for a Food Stamp Transaction (a) within six (6) Business Days of the original Transaction Date or (b) if the Correction Request is to reverse or adjust a prior correction credit to the Issuer, within six (6) Business Days of date of such earlier Correction Request. Correction Requests for System Errors initiated after that period may be automatically rejected. Each Acquirer must provide notice of a Settlement Error Correction Request to debit an Issuer within twenty (20) Business Days of the original Transaction Date, or as promptly as possible thereafter if the Acquirer, in good faith, is unable to provide notice within such time frame. Each Issuer must make a good faith effort to process late Correction Requests for Settlement Errors.
- B.** ***Issuer Response.*** Each Issuer shall make a preliminary determination whether to accept or reject a System Error Correction Request by the Initial Issuer Response Cut-Off. Each Issuer must issue its Correction Response to Settlement Error Correction Requests within ten (10) Business Days of notice of the Correction Request, and may not reject such Correction Request for insufficient funds.
 - I.** ***Rejection.*** If the Issuer determines to reject a System Error Correction Request, it shall notify the Acquirer by the Initial Issuer Response Cut-Off. If information comes to the attention of the Issuer after the Initial Issuer Response Cut-Off that justifies rejection of a Correction



Request, the Issuer may, notwithstanding the preceding sentence, issue a Correction Response rejecting the Correction Request at any time prior to settlement of the Correction Request. Correction Requests for Settlement Errors may not be rejected for insufficient funds.

- II. **Acceptance.** If the Issuer makes a preliminary determination to accept a System Error Correction Request, it shall provide such notice to the Cardholder as may be required by Applicable Law.
- (a) **No Hearing Request.** If the Cardholder does not request a Fair Hearing within the period required by Applicable Law and there are sufficient funds available in the Food Stamp Account to fully satisfy the System Error Correction Request, the Issuer shall issue its Correction Response the next Business Day. If the Cardholder does not request a Fair Hearing within the period required by Applicable Law and there are insufficient funds available in the Food Stamp Account to fully satisfy the Correction Request, the Issuer thereafter shall daily review whether sufficient funds have become available in the Cardholder's Food Stamp Account, giving first priority to payment of the Correction Request out of any funds in or added to the Cardholder's Food Stamp Account, and shall issue its System Error Correction Response the next Business Day following the availability of sufficient funds in the Cardholder's Food Stamp Account. If sufficient funds do not become available in the Cardholder's Food Stamp Account by the close of business on the last calendar day of the month following the Correction Request, the Issuer shall notify the Acquirer of its Correction Response rejecting the Correction Request for insufficient funds within two (2) Business Days. If information comes to the attention of the Issuer after the Initial Issuer Response Cut-Off that justifies rejection of a Correction Request, the Issuer may, notwithstanding the foregoing, issue a Correction Response rejecting the Correction Request at any time prior to settlement of the Correction Request.
- (b) **Hearing Request.** If the Cardholder requests a Fair Hearing within the period required by Applicable Law, the Issuer shall provide a Correction Response that rejects the Correction Request on the basis of the Fair Hearing request.

(ii) Documentation

- A. **Acquirer Request.** Each Acquirer Correction Request to debit an Issuer in respect of a Food Stamp Transaction must contain at least the following information:
- I. Transaction identification or trace number
- II. Transaction amount
- III. Transaction Date and
Transaction Time
- IV. Terminal identification number
- V. Merchant FNS number
- VI. Cardholder PAN
- VII. Explanation of the alleged error sufficient to allow the Cardholder of the Correction Request to evaluate the claim
- VIII. Contact information for communications regarding the Correction Request



-
- IX. Listing of any accompanying documentation
 - X. A copy of the audit tape or Terminal journal, upon request only
 - XI. For a Manual Food Stamp Transaction B upon request only, a copy of the Sales and Credit Draft
 - XII. If the Correction Request relates to an earlier erroneous Correction Request, the date of the earlier Correction Request and any other information reasonably necessary to identify the earlier Correction Request, and, upon request only, a copy of such earlier Correction Request
- B.** ***Issuer Response.*** If the Issuer rejects the Correction Request, the Correction Response must contain:
- I. a reasonable explanation of the basis for rejection (e.g., failure by Acquirer to provide all required information, duplicate Correction Request, or unverifiable PAN)
 - II. documents (including electronic records) reasonably supporting such rejection, such as a Transaction record of a reversal of the underlying Transaction, upon request only.

(iii) Follow-up

- A. *Timely Correction Response Received***
 - I. ***Approval.*** If the Issuer issues a Correction Response accepting the Correction Request, the Issuer shall include the correction in the Settlement of correction items within the next three (3) Business Days following notice of such Correction Response.
 - II. ***Denial.*** If the Issuer rejects the Correction Request, it must notify the Acquirer in accordance with the time limits and documentation requirements above. If there is a dispute regarding the validity of the Issuer's rejection of a Correction Request, the parties to any such dispute shall take all steps reasonably practicable to resolve such dispute by mutual agreement within thirty (30) calendar days of notice of the Issuer's Correction Response.
- B. *No Timely Correction Response Received.*** If the Issuer fails to provide a timely Correction Response or payment of a Correction Request in accordance with the procedures above, the Issuer shall be responsible for settling the Correction Request regardless of the availability of funds in the Cardholder's Food Stamp Account.

SECTION 5.4 Issuer-Initiated Corrections for Cash Transactions

Each Issuer must promptly balance and reconcile its accounts, and must initiate Correction Requests for Cash Transactions promptly upon discovery of a System Error or Settlement Error.

- a. *Debit to Acquirer (Cash Transactions).*** Examples of errors for which Correction Requests should be issued to debit an Acquirer include: duplicate Transaction and ATM misdispense.

(i) Time Lines

- A. *Issuer Request.*** Each Issuer must make a good faith effort to initiate System Error Correction Requests for debit to an Acquirer in respect of a Cash Transaction (a) within ten (10) Business Days of the original Transaction Date, or (b) if the Correction Request is to reverse or adjust a prior correction credit to the Acquirer, within ten (10) Business Days of date of such earlier Correction Request, unless the Correction Request is in response to a Cardholder dispute. Each Issuer must initiate a Correction Request promptly in response to a Cardholder dispute received up to ninety (90) calendar days after the Transaction Date or, if the Correction Request is to reverse or adjust a prior



correction credit to the Acquirer, up to ninety (90) calendar days from the date of such earlier Correction Request. Each Issuer must provide notice of a Settlement Error Correction Request to debit an Acquirer within twenty (20) Business Days of the original Transaction Date, or as promptly as possible thereafter if the Issuer, in good faith, is unable to provide notice within such time frame. Acquirers must make a good faith effort to process late Correction Requests for Settlement Errors.

- B. Acquirer Response.** Each Acquirer must issue a Correction Response within twenty (20) calendar days of notice of a System Error Correction Request for a Cash Transaction. Each Acquirer must issue its Correction Response to Settlement Error Correction Requests within ten (10) Business Days of notice of the Correction Request, and may not reject such Correction Request for insufficient funds.

(ii) Documentation Requirements

- A. Issuer Request.** Each Issuer Correction Request to debit an Acquirer in respect of a Cash Transaction must contain at least the following information:

- I. Transaction identification or trace number
- II. Transaction amount
- III. Transaction Date and Transaction Time
- IV. Terminal identification number
- V. Cardholder PAN
- VI. Explanation of the alleged error sufficient to allow the Cardholder of the Correction Request to evaluate the claim
- VII. Contact information for communications regarding the Correction Request
- VIII. Listing of any accompanying documentation
- IX. For a Correction Request involving a Cardholder dispute -- any documentation provided by the Cardholder, upon request only
- X. If the Correction Request relates to an earlier erroneous Correction Request, the date of the earlier Correction Request and any other information reasonably necessary to identify the earlier Correction Request, and, upon request only, a copy of such earlier Correction Request.

- B. Acquirer Response.** No documentation is required for approval of a Correction Request. If the Acquirer rejects the Correction Request, the Correction Response must contain:

- I. a reasonable explanation of the basis for rejection (e.g., failure of Issuer to provide required information or Transaction verified by Terminal records)
- II. documents (including electronic records) supporting such rejection, such as a Terminal journal record or audit tape showing the completed Transaction and, upon request, the ATM balancing sheet. *(Amended May 30, 2002)*

(iii) Follow-up



-
- A. **No Timely Correction Response Received.** If the Acquirer does not respond within the foregoing timeframes, the Issuer may include the amount of the Correction Request in the Settlement for correction items for any of the next three (3) Business Days and the Acquirer must pay such amount.
 - B. **Timely Correction Response Received**
 - I. **Approval.** If the Acquirer's Correction Response confirms that a debit should be issued, the Issuer may include the agreed amount in the Settlement for correction items within the three (3) Business Days next following notice of the Correction Response and the Acquirer must pay such amount.
 - II. **Denial.** If the Acquirer rejects the Correction Request, it must notify the Issuer in accordance with the time limits and documentation requirements above. If there is a dispute regarding the validity of the Acquirer's rejection of a Correction Request, the parties to any such dispute shall take all steps reasonably practicable to resolve such dispute by mutual agreement within thirty (30) calendar days of notice of the Acquirer's Correction Response.
 - b. **Credit to Acquirer (Cash Transactions).** Examples of errors for which Correction Requests should be issued to credit an Acquirer include: erroneous reversal.
 - (i) **Time Lines**
 - A. **Issuer Request for Transactions NOT Subject to Fair Hearing Requirements.** The procedures in this Subsection (A) apply if an Issuer's Correction Request relates to a Cash Transaction that is NOT subject to State Fair Hearing procedures prior to the charging of a Correction Request to a Cardholder's Cash Account. Each Issuer must initiate System Error Correction Requests for credit to an Acquirer in respect of a Cash Transaction within ten (10) Business Days of the original Transaction Date, unless (a) a later credit is authorized by the Cardholder, or (b) there are not sufficient funds available in the Cardholder's Cash Account to satisfy the Correction Request. If there are not sufficient funds available in the Cardholder's Cash Account to satisfy the System Error Correction Request during such ten (10) Business Day period, the Issuer thereafter shall daily review whether sufficient funds have become available in the Cardholder's Cash Account, giving first priority to payment of the Correction Request out of any funds in or added to the Cardholder's Cash Account, and shall issue its System Error Correction Request the next Business Day following the availability of sufficient funds in the Cardholder's Cash Account. If sufficient funds do not become available, the Issuer is not required to initiate a System Error Correction Request. Each Issuer must provide notice of a Settlement Error Correction Request to credit an Acquirer within twenty (20) Business Days of the original Transaction Date, or as promptly as possible thereafter if the Issuer, in good faith, is unable to provide notice within such time frame.
 - B. **Issuer Request for Transactions Subject to Fair Hearing Requirements.** The procedures in this Subsection (B) apply if an Issuer's Correction Request relates to a Cash Transaction that IS subject to State Fair Hearing procedures prior to the charging of a Correction Request to a Cardholder's Cash Account. If an Issuer discovers a System Error that requires a debit to the Cardholder's Cash Account, the Issuer shall provide such notice to the Cardholder as may be required by Applicable Law.
 - I. **No Hearing Request.** If the Cardholder does not request a Fair Hearing within the period applicable to Food Stamp Transactions and there are sufficient funds available in the Cash Account to fully satisfy the hold, the Issuer shall issue its System Error Correction Request the next Business Day. If the Cardholder does not request a Fair Hearing within such period and there are insufficient funds available in the Cash Account to fully satisfy the Correction Request, the Issuer thereafter shall daily review whether sufficient funds have become available in the Cardholder's Cash Account, giving first priority to payment of the Correction Request out of any funds in or added to the Cardholder's Cash Account, and shall issue its System Error Correction



Request the next Business Day following the availability of sufficient funds in the Cardholder's Cash Account. If sufficient funds do not become available, the Issuer shall not initiate a Correction Request.

- II. **Hearing Request.** If the Cardholder requests a Fair Hearing within the period applicable to Food Stamp Transactions, the Issuer shall not initiate a Correction Request.
- C. **Acquirer Response.** No response is required other than settlement of the Correction Request as provided below.

(ii) Documentation Requirements

- A. **Issuer Request.** Each Issuer Correction Request to credit an Acquirer in respect of a Cash Transaction must contain at least the following information:
 - I. Transaction identification or trace number
 - II. Transaction amount
 - III. Transaction Date and Transaction Time
 - IV. Terminal identification number
 - V. Cardholder PAN
 - VI. Explanation of the alleged error sufficient to allow the Cardholder of the Correction Request to evaluate the claim
 - VII. Contact information for communications regarding the Correction Request
 - VIII. Listing of any accompanying documentation
 - IX. If the Correction Request relates to an earlier erroneous Correction Request, the date of the earlier Correction Request and any other information reasonably necessary to identify the earlier Correction Request.
- B. **Acquirer Response.** No documentation is required for approval of a Correction Request. If the Acquirer rejects the Correction Request, the Correction Response must contain a reasonable explanation of the basis for rejection (e.g., duplicate correction). No additional documentation is required.

(iii) Follow-up

- A. **Approval.** The Issuer must credit the amount of the Correction Request to the Acquirer in the Settlement for correction items within the next three (3) Business Days following notice of the Correction Request.
- B. **Denial.** If the Acquirer rejects the Correction Request, no further action is necessary.

SECTION 5.5 Issuer-Initiated Corrections for Food Stamp Transactions



Each Issuer must promptly balance and reconcile its accounts, and must initiate Correction Requests for Food Stamp Transactions promptly upon discovery of a System Error or Settlement Error.

- a. **Debit to Acquirer (Food Stamp Transactions).** Examples of errors for which Correction Requests should be issued to debit an Acquirer include: unauthorized Manual Food Stamp Transaction or duplicate Transaction.

(i) **Time Lines**

- A. **Issuer Initiation.** Each Issuer must initiate Correction Requests within four (4) Business Days of discovery, or receipt of notice of a Cardholder claim with the timeframe required by Applicable law, of a System Error that requires a credit to a Food Stamp Account. Issuers must provide notice of a Settlement Error Correction Request to debit an Acquirer within twenty (20) Business Days of the original Transaction Date, or as promptly as possible thereafter if the Issuer, in good faith, is unable to provide notice within such time frame. Acquirers must make a good faith effort to process late Correction Requests for Settlement Errors.
- B. **Acquirer Response.** Each Acquirer must issue a Correction Response to a System Error Correction Request for a Food Stamp Transaction within five (5) Business Days. Each Acquirer must issue its Correction Response to Settlement Error Correction Requests within ten (10) Business Days of notice of the Correction Request, and may not reject such Correction Request for insufficient funds.

(ii) **Documentation Requirements**

- A. **Issuer Request.** Each Issuer Correction Request to debit an Acquirer in respect of a Food Stamp Transaction must contain at least the following information:
- I. Transaction identification or trace number
 - II. Transaction amount
 - III. Transaction Date and Transaction Time
 - IV. Terminal identification number
 - V. Cardholder PAN
 - VI. Explanation of the alleged error sufficient to allow the Cardholder of the Correction Request to evaluate the claim
 - VII. Contact information for communications regarding the Correction Request
 - VIII. Listing of any accompanying documentation
 - IX. If pursuant to a Cardholder dispute, the date the dispute was received
 - X. For duplicate Transactions - the Transaction number or trace number for both transactions
 - XI. For a failed Food Stamp Merchandise Refund B a copy of the receipt evidencing return of merchandise for Food Stamp credit, Transaction Date, Transaction Time and Transaction identification or trace number for both the original Food Stamp Transaction and the Food Stamp Merchandise Refund



XII. If the Correction Request relates to an earlier erroneous Correction Request, the date of the earlier Correction Request and any other information reasonably necessary to identify the earlier Correction Request, and, upon request only, a copy of such earlier Correction Request.

B. Acquirer Response. No documentation is required for approval of a Correction Request. If the Acquirer rejects the Correction Request, the Correction Response must contain:

- I. a reasonable explanation of the basis for rejection (e.g., Correction Request directed to incorrect Acquirer, duplicate Correction Request, Correction Request does not contain required information, Food Stamp Merchandise Refund already issued, or miskeyed Telephone Authorization Code); and
- II. upon request only, documents (including electronic records) supporting such rejection, such as (i) Terminal journal record of showing completed Transaction, or (ii) copy of the Sales and Credit Draft for a Manual Food Stamp Transaction.

(iii) Follow-up

A. No Timely Correction Response Received. If the Acquirer does not respond within the foregoing timeframes, the Issuer may include the amount of the Correction Request in the Settlement for correction items within the three (3) Business Days next following the expiration of the Acquirer's time to respond and the Acquirer must pay such amount.

B. Timely Correction Response Received

- I. **Approval.** If the Acquirer's Correction Response confirms that a debit should be issued, the Issuer may include the agreed amount in the Settlement for correction items within the next three (3) Business Days following notice of the Correction Response and the Acquirer must pay such amount.
- II. **Denial.** If the Acquirer rejects the Correction Request, it must notify the Issuer in accordance with the time limits and documentation requirements above. If there is a dispute regarding the validity of the Acquirer's rejection of a Correction Request, the parties to any such dispute shall take all steps reasonably practicable to resolve such dispute by mutual agreement within thirty (30) calendar days of notice of the Acquirer's Correction Response.

b. Credit to Acquirer (Food Stamp Transactions). Examples of errors for which Correction Requests should be issued to credit an Acquirer include: erroneous reversal.

(i) Time Lines

A. Issuer Initiation. Each Issuer must provide notice of a Settlement Error Correction Request to credit an Acquirer within twenty (20) Business Days of the original Transaction Date, or as promptly as possible thereafter if the Issuer, in good faith, is unable to provide notice within such time frame. If an Issuer discovers a System Error that requires a debit to the Cardholder's Food Stamp Account, the Issuer shall provide such notice to the Cardholder as may be required by Applicable Law.

- I. **No Hearing Request.** If the Cardholder does not request a Fair Hearing within the period required by Applicable Law and there are sufficient funds available in the Food Stamp Account to fully satisfy the hold, the Issuer shall issue its System Error Correction Request the next Business Day. If the Cardholder does not request a Fair Hearing within the period required by Applicable Law and there are insufficient funds available in the Food Stamp Account to fully satisfy the Correction Request, the Issuer thereafter shall daily review whether sufficient funds have become available in the Cardholder's Food Stamp Account, giving first priority to payment of the Correction Request out of any funds in or added to the Cardholder's Food



Stamp Account, and shall issue its System Error Correction Request the next Business Day following the availability of sufficient funds in the Cardholder's Food Stamp Account. If sufficient funds do not become available, the Issuer shall not initiate a Correction Request.

- II. **Hearing Request.** If the Cardholder requests a Fair Hearing within the period required by Applicable Law, the Issuer shall not initiate a Correction Request.

- B. **Acquirer Response.** No response is required other than settlement of the Correction Request as provided below.

(ii) **Documentation Requirements**

- A. **Issuer Request.** Each Issuer Correction Request to credit an Acquirer in respect of a Food Stamp Transaction must contain at least the following information:

- I. Transaction identification or trace number
- II. Transaction amount
- III. Transaction Date and Transaction Time
- IV. Terminal identification number
- V. Cardholder PAN
- VI. Explanation of the alleged error sufficient to allow the Cardholder of the Correction Request to evaluate the claim
- VII. Contact information for communications regarding the Correction Request
- VIII. Listing of any accompanying documentation
- IX. If the Correction Request relates to an earlier erroneous Correction Request, the date of the earlier Correction Request and any other information reasonably necessary to identify the earlier Correction Request.

- B. **Acquirer Response.** No documentation is required for approval of the Correction Request. If the Acquirer rejects the Correction Request, the Correction Response must contain a reasonable explanation of the basis for rejection (e.g., duplicate correction). No additional documentation is required.

(iii) **Follow-up**

- A. **Approval.** The Issuer must credit the amount of the Correction Request to the Acquirer in the Settlement for correction items within the three (3) Business Days next following notice of the Correction Request.
- B. **Denial.** If the Acquirer rejects the Correction Request, no further action is necessary.

SECTION 5.6 Fair Hearing Corrections

All Fair Hearing Correction Requests shall be handled in accordance with this Section 5.6 rather than Section 5.3 or 5.5. Each Issuer shall initiate a Fair Hearing Correction Request when instructed by the appropriate Government Entity as the result of (i) a Fair Hearing held pursuant to Applicable Law or (ii) of late notice of a Fair Hearing request that was



delayed by the Cardholder for good cause, as defined by Applicable Law. Before initiating such Fair Hearing Correction Request, the Issuer shall confirm the accuracy and validity of such request. All references to the Cardholder's Account in this Section mean the Cash Account or Food Stamp Account that was the subject of the Fair Hearing.

- a. **Debit to Acquirer (Fair Hearing Correction Request).** If an Issuer had previously paid the amount of a Transaction or Correction Request to an Acquirer and the Issuer is required to credit such amount in whole or in part to the Cardholder's Account, the Issuer may initiate a Correction Request to debit the Acquirer in accordance with instructions from the appropriate Government Entity.

(i) **Time Lines**

- A. **Issuer Initiation.** Each Issuer must issue Fair Hearing Correction Requests within the timeframe permitted under Applicable Law.
- B. **Acquirer Response.** Each Acquirer must issue a Correction Response within five (5) Business Days of receipt of the Correction Request.

(ii) **Documentation Requirements**

- A. **Issuer Request.** The Issuer shall include at least the following information when initiating a Fair Hearing Correction Request.
- I. Original transaction identification or trace number
 - II. Original transaction amount
 - III. Original transaction Date and Transaction Time
 - IV. Original terminal identification number
 - V. Cardholder PAN
 - VI. Amount of the Fair Hearing Correction Request
 - VII. Copy of the administrative or judicial order relating to the Fair Hearing Correction Request, upon request only
 - VIII. Contact information for communications regarding the Fair Hearing Correction Request
 - IX. Listing of any accompanying documentation
- B. **Acquirer Response.** No documentation is required for approval of a Correction Request. The Acquirer may reject the Fair Hearing Correction Request only for the reason of an error in identification of either the Acquirer or the Merchant. The Acquirer must provide sufficient documentation to support its rejection by reason of an error in identification.

(iii) **Follow-up**

A. **Timely Correction Response by Acquirer**

- I. **Approval.** If the Acquirer issues a Correction Response accepting the Correction Request, the Issuer shall settle the Correction Request within the next three (3) Business Days and the Acquirer must pay such amount.



- II. ***Denial.*** If the Acquirer issues a Correction Response rejecting the Correction Request, it must do so in accordance within the time limits and documentation requirements above. If there is a dispute regarding the validity of the Acquirer's rejection of a Correction Request, the parties to any such dispute shall take all steps reasonably practicable to resolve such dispute by mutual agreement within thirty (30) calendar days of notice of the Acquirer's Correction Response.
- B. ***No Timely Correction Response by Acquirer.*** If the Acquirer does not respond within the foregoing timeframes, the Issuer shall settle the Correction Request within the next three (3) Business Days and the Acquirer must pay such amount.
- b. ***Credit to Acquirer (Fair Hearing Correction Request).*** If the Issuer had not previously paid the amount of the Correction Request to the Acquirer and the Fair Hearing determines that the Correction Request was correct, in whole or in part, the Issuer shall initiate a Correction Request to credit the Acquirer in accordance with instructions from the appropriate Government Entity.

(i) ***Time Lines***

- A. ***Issuer Initiation.*** Each Issuer must issue Fair Hearing Correction Requests within the three (3) Business Days after funds become available in the appropriate Account to satisfy the Fair Hearing Correction Request in accordance with Applicable Law. If sufficient funds are not available at the time of notice from the appropriate Government Entity, the Issuer thereafter shall daily review whether sufficient funds have become available in the Cardholder's appropriate Account, giving first priority to payment of the Correction Request out of any funds in or added to the Cardholder's Account, and shall issue its Fair Hearing Correction Request the next Business Day following the availability of sufficient funds in the Cardholder's Account. If sufficient funds do not become available, the Issuer shall not initiate a Fair Hearing Correction Request and shall notify the Acquirer and Government Entity that the Fair Hearing Correction Request cannot be satisfied due to insufficient funds.
- B. ***Acquirer Response.*** No response is required other than settlement of the Correction Request as provided below.

(ii) ***Documentation Requirements***

- A. ***Issuer Request.*** The Issuer shall include at least the following information when initiating a Fair Hearing Correction Request.
 - I. Original transaction identification or trace number
 - II. Original transaction amount
 - III. Original transaction Date and Transaction Time
 - IV. Original terminal identification number
 - V. Cardholder PAN
 - VI. The amount of the Fair Hearing Correction Request



VII. Copy of the administrative or judicial order relating to the Fair Hearing Correction Request, upon request only

VIII. Contact information for communications regarding the Correction Request

IX. Listing of any accompanying documentation

B. **Acquirer Response.** No documentation is required for approval of the Fair Hearing Correction Request. If the Acquirer rejects the Fair Hearing Correction Request, the Correction Response must contain a reasonable explanation of the basis for rejection.

(iii) **Follow-up**

A. **Approval or Failure to Respond.** The Issuer shall settle the Fair Hearing Correction Request within three (3) Business Days of initiating such Correction Request, unless the Correction Request is denied.

B. **Denial.** If the Acquirer rejects the Correction Request, no further action is necessary.

SECTION 5.7 Availability of Records

Sections 5.2, 5.3, 5.4, 5.5 and 5.6 govern the provision of Transaction-related records in connection with Correction Requests and Correction Responses. All requests for documentation in connection with Sections 5.2, 5.3, 5.4, 5.5 and 5.6 should be honored as promptly as possible to facilitate the ability of requesting party to respond within the time frames provided under those Sections. This Section 5.7 governs the provision of Transaction-related records in the event such records are required outside of such processes.

- a. Acquirers shall provide Transaction-related records within 20 calendar days of receipt of a request, if the request is received within 30 calendar days of the Transaction Date.
- b. Acquirers shall provide Transaction-related records within 45 calendar days of receipt of a request if the request is received between 31 and 180 calendar days of the Transaction Date.
- c. Issuers must promptly respond to requests for Transaction-related records received up to 180 calendar days from the Transaction Date.
- d. Notwithstanding the foregoing, Issuers and Acquirers shall provide Transaction-related records as may be required for any Fair Hearings held pursuant to Applicable Law.



CHAPTER SIX - SETTLEMENT

SECTION 6.1 End of Day Cut-off and Processing

Each Issuer must designate a standard daily cut-off time for Transaction processing by Acquirers that have entered into Acquirer Agreements with that Issuer or its Designated Agent(s); provided, however, that such cut-off time may not be earlier than 12:00 noon local time at any Terminal accepting Transactions for such an Acquirer. Transactions performed during a Business Day prior to the standard cut-off time shall be settled by the Issuer to the Acquirer on the next Business Day. (Example 1: Transactions performed after Wednesday Business Day cut-off time and before Thursday Business Day cut-off time shall be settled to Acquirers on Friday Business Day; Example 2: Transactions performed after Thursday Business Day cut-off time and before Sunday cut-off time shall be settled to Acquirers on Monday Business Day). Merchants and Acquirers that establish their own cut-off times which are different from their Issuer's cut-off time must maintain appropriate suspense accounts for such purposes. (Amended December 29, 2000)

SECTION 6.2 Settlement Payments

Settlement shall be on a net basis among Issuers and Acquirers. Each Issuer must initiate Settlement payments to its Acquirers in a net credit position through ACH transfers or Federal Reserve Wire Transfers each Settlement Day in a timely manner to ensure receipt of Settlement payments by the Acquirers on the next Business Day.

- a. ***Network Settlement.*** Transactions routed by Acquirers through a Network shall be settled in accordance with such Network's normal Settlement procedures.
- b. ***Settlement of Interoperable Transactions.*** Each Issuer shall arrange with each other Issuer for the net Settlement of Interoperable Transactions each Business Day.
- c. ***Processors as Endpoints.*** These Rules do not prohibit Processors from acting as agents of Acquirers for purposes of Settlement and reconciliation.

SECTION 6.3 Government Reimbursement

Each Issuer shall be liable for Settlement of Transactions it authorizes each Settlement Day regardless of when or whether the Issuer receives payment in respect of such Transactions from a Government Entity.

SECTION 6.4 Beneficial Ownership of Funds

Each Issuer that is not a Government Entity that receives funds directly or indirectly from a Government Entity for the purpose of settling for Authorized Transactions under these Rules shall have no equitable or beneficial interest in such funds and holds such funds in trust so that such funds shall not be considered to be property of the Issuer, assets of the Issuer or property of the estate of the Issuer or used to satisfy the creditors of the Issuer in the event that the Issuer becomes insolvent. Any such funds that are due and payable to Acquirers or their Agents under these Rules shall be paid to Acquirers or their agents. Any such funds that are not due and payable to Acquirers or their agents under these Rules shall be due and payable to the Government Entity from which they were received and shall be returned to that Government Entity. For the purpose of this section, an agent shall be defined as a Processor, Designated Agent or Network that acts on behalf of Acquirer for settlement and reconciliation purposes. (Amended October 8, 2002 and November 10, 2004)

SECTION 6.5 Settlement Reports

Promptly following the cut-off time each Settlement Day, each Issuer shall make available to each Acquirer, directly or through a Processor for such Acquirer, such settlement reports and/or data files as shall be reasonably required for such Acquirer's reconciliation of the day's Settlement.



CHAPTER SEVEN - THIRD PARTY SERVICE PROVIDER REQUIREMENTS

SECTION 7.1 Third Party Service Provider Agreements

Each Third Party Service Provider shall enter into a Third Party Provider Agreement stating its agreement to comply with and be bound by these Rules, as such may be amended from time to time. These Rules do not restrict any other terms or conditions of the Third Party Provider Agreement, provided that such terms and conditions do not conflict with these Rules, and do not relieve the Third Party Service Provider from any registration, certification or other requirement imposed by a Network in which such Third Party Service Provider participates. Each Issuer, Designated Agent or Acquirer entering into a Third Party Provider Agreement must keep a copy of each of its Third Party Provider Agreements at its headquarters. Each Issuer and Acquirer entering, directly or through a Designated Agent, into a Third Party Provider Agreement shall be jointly and severally liable for the performance or failure to perform by the Third Party Service Provider of any of the duties of such Issuer or Acquirer hereunder.

SECTION 7.2 Registration

Each Issuer, Designated Agent or Acquirer shall provide to NACHA a list of the Third Party Service Providers with which it has entered into a Third Party Provider Agreement.

SECTION 7.3 Requirements for All Third Party Service Providers

Each Third Party Service Provider Agreement shall be executed by an officer of an Issuer, Designated Agent or Acquirer and shall contain the substance of the following provisions.

- a. ***Capacity.*** Each Third Party Service Provider acting on behalf of any Issuer, Designated Agent or Acquirer, shall comply with the Rules applicable to such Issuer, Designated Agent or Acquirer, in the provision of its services.
- b. ***Security Requirements.*** Each Third Party Service Provider must meet all applicable security requirements under Chapter 9.
- c. ***Subcontracting.*** A Third Party Service Provider may not subcontract its services, except that a Designated Agent of an Issuer may enter into an agreement with a Network for such Network to also act as Designated Agent of the Issuer. *(Amended September 27, 1996)*
- d. ***Acquirer-Controlled Functions.*** If the Third Party Provider Agreement is with an Acquirer, the following functions are to be controlled by the Acquirer:
 - (i) approval and review of Merchants and execution of Merchant Agreements
 - (ii) establishment of Terminal encryption and placement procedures
 - (iii) Settlement with Merchants
- e. ***Agreement Termination.*** Each Third Party Provider Agreement shall be terminable for a violation of these Rules.
- f. ***Audits.*** If NACHA or the Issuer or Acquirer for a Third Party Service Provider has reasonable cause to question the accuracy, timeliness, completeness or reliability of any activities undertaken by the Third Party Service Provider under these rules or the compliance of the Third Party Service Provider with these Rules, such Third Party Service Provider shall provide to the Acquirer, NACHA and its Issuer or Acquirer full and free access to all records and systems related to its performance under its Third Party Provider Agreement for the purpose of examination or



auditing such performance and compliance. At NACHA's discretion, such examination or audit may be conducted, at the Third Party Service Provider's expense by (a) an outside auditor of the Third Party Service Provider's choosing, (b) NACHA or (c) a third party retained by NACHA. If such examination or audit reveals any exception to the Third Party Service Provider's compliance with these Rules, the Third Party Service Provider shall promptly remedy such exception. To the extent feasible, NACHA shall coordinate any such examination or audit with and rely upon any comparable examination or audit performed by a Network. These Rules shall not limit the authority of a Government Entity to audit a Participant under any agreement or Applicable law. The agreements between Participants that are required by these Rules may provide for additional audit requirements between such Participants.

- g. **Settlement Funds.** No Third Party Service Provider, other than a Network, may be a party to Settlement or receive Settlement funds other than through an Issuer or Acquirer, provided that a Processor may act as an agent of one or more Acquirers for purposes of Settlement and reconciliation.
- h. **Protection of the QUEST Mark.** Only Issuers and Acquirers are licensed to use the Quest Mark pursuant to Chapter 11 of these Rules. A Third Party Service Provider may utilize the QUEST Mark on behalf of an Issuer or Acquirer solely in accordance with the standards regarding the use of the QUEST Mark in Chapter 11 and may not misrepresent any aspect of the handling of Transactions hereunder, including the pricing of such Transactions. No Third Party Provider may represent or imply that NACHA endorses its products or services or that it is other than a contractor or representative of its Issuer or Acquirer for purposes of its activities under these Rules. *(Amended December 16, 2008)*

SECTION 7.4 Government Entities as Third Party Service Providers

If a Government Entity engages in Merchant solicitation, sales or servicing, other than approval of Merchants to participate in an EBT Program, or acts as an ESSP, such Government Entity shall enter into a Third Party Provider Agreement that contains the substance of Subsections 7.3(b) and 7.3(h).

SECTION 7.5 ISO Agreements

Each Acquirer and Processor that enters into an agreement with an independent sales organization for the purpose of merchant sales and servicing shall include the substance of the following provisions in each such agreement:

- a. Employees, agents or other representatives of the independent sales organization must clearly and accurately identify themselves and the independent sales organization in any oral or written communication with retailers and merchants. Such individuals and entities may not state, suggest or imply that they are representatives of QUEST®, NACHA, any governmental entity or any Issuer. *(Amended December 16, 2008)*
- b. Employees, agents or other representatives of the independent sales organization may not state, suggest or imply that they are or represent the only authorized company able to provide any EBT-related services, that any merchant or retailer will be foreclosed from accepting EBT transactions if such merchant or retailer does not enter into an agreement or arrangement with the independent sales organization or that there is any time limit within which such merchant or retailer must arrange to be able to accept EBT transactions.
- c. Employees, agents or other representatives of the independent sales organization must clearly, completely and accurately describe in writing to each merchant or retailer such independent sales organization's plans for installation of terminals, training of the merchant or retailer's employees, maintenance options, terminal lease or purchase costs and transaction fees.
- d. Each independent sales organization shall provide to each retailer, prior to entering into an agreement with such retailer, a written disclosure of official contact information for the EBT Program for the State in which the retailer is located as provided by the Issuer for that State.



- e. Each independent sales organization shall provide the following written statement in a clear and conspicuous manner to each merchant or retailer prior to the merchant or retailer entering into an agreement with such independent sales organization for EBT related products or services: "I am a representative of [insert company name]. I am NOT a representative of Quest®, NACHA, any governmental entity or any Issuer. You have a right to receive, review and keep a written description of the services that we offer and the prices for those services. You have a right to compare that information to the products and services that can be provided by other companies."
(Amended December 16, 2008)

This amendment shall apply to all agreements between Acquirers or Processors and ISOs that are entered or renewed more than 60 days after approval of this amendment by NACHA. With respect to all other agreements between Acquirers and Processors and ISOs, this amendment shall take effect 12 months after approval by NACHA and shall require amendment of the pre-existing agreements. *(Amended May 9, 2000 and December 16, 2008)*



CHAPTER EIGHT - ARBITRATION AND GRIEVANCE PROCEDURES, ASSESSMENTS

SECTION 8.1 Filing a Complaint

Each Participant shall cooperate with each other Participant in attempting to resolve complaints or disputes regarding Transactions or compliance with these Rules. If such efforts are unsuccessful a Participant that is party to a complaint or dispute (the "complainant") may initiate an arbitration proceeding by filing a complaint with NACHA stating that all reasonable attempts to reconcile the difference have failed and requesting arbitration under these Rules. NACHA may itself initiate a complaint on its own behalf or on behalf of other Participants. A complaint shall contain the following:

- a. ***Identification of Parties.*** The names, addresses and telephone numbers of the complainant and the other party or parties involved in the dispute (each, a "respondent").
- b. ***Summary of Facts.*** A summary of the facts of the dispute as well as the Section(s) of the Rules violated. The summary shall also include information permitting identification of the particular Transaction(s) and the sequence of events involved, and the precise nature of the violation(s).
- c. ***Statement of Damages.*** A statement of the dollar amount of damages claimed by the complainant and an explanation of how damages in the amount claimed resulted from the violation(s) asserted. An arbitration claim under this Chapter shall be processed only if the amount of the damages claimed is \$100 or more.
- d. ***Additional Documents and Fees.*** The complaint shall be accompanied by the following:
 - (i) copies of the documents available to the complainant necessary to resolve the dispute, and of any written communications by the complainant and the respondent relating to the violations asserted; and
 - (ii) a \$250 non-refundable application fee to be used for administrative expenses.
- e. ***Authorization for Submitting a Claim.*** The complaint shall be signed by an officer of the complainant and be submitted to NACHA within one (1) year of the violations asserted.
- f. ***Complaints Involving Multiple Participants.*** If the complainant is involved in related disputes with more than one Participant, a separate complaint shall be filed with respect to each such Participant.

NACHA may reject any complaint which does not meet the requirements of this Section 8.1.

SECTION 8.2 Classification of Disputes

- a. ***Complaints with Damages of Less than \$10,000 (Arbitration Procedure A).*** All complaints in which the amount of damages claimed is \$100 or more but less than \$10,000 shall be processed under Arbitration Procedure A set forth in these Rules. Under Arbitration Procedure A:
 - (i) Arbitration is not mandatory. Before the complaint is filed, both parties must agree to submit the dispute to binding arbitration. If both parties so agree, one of them shall submit a complaint to NACHA, as set forth in Section 8.1, which complies with the requirements of that Section;
 - (ii) A hearing shall not be held;
 - (iii) One arbitrator shall decide the case; and
 - (iv) The arbitrator's stipend shall be 3% of the arbitrator's decision with a \$100 minimum stipend.



b. **Complaints with Damages of \$10,000 or More (Arbitration Procedure B).** All complaints in which the amount of damages claimed is \$10,000 and above shall be processed under Arbitration Procedure B set forth in these Rules. Under Arbitration Procedure B:

- (i) Arbitration is not mandatory. Before the complaint is filed, both parties must agree to submit the dispute to binding arbitration. If both parties so agree, one of them shall submit a complaint to NACHA, as set forth in Section 8.1, which complies with the requirements of that Section;
- (ii) A hearing shall be held unless the parties otherwise agree and so notify NACHA at the time the complaint is filed. If the parties do so otherwise agree, the procedures set forth in Section 8.2(a) (Arbitration Procedure A) rather than as provided for in this Section 8.2(b) (Arbitration Procedure B) shall be followed;
- (iii) At its discretion, a party may be represented at the hearing by legal counsel;
- (iv) Three arbitrators shall decide the case; and
- (v) The stipend for each arbitrator shall be set according to the following scale:

Amount of Claim	Stipend per Arbitrator
\$10,000 to \$40,000	\$300 plus 2% of excess over \$10,000
\$40,001 and up	\$900 plus 1/2% of excess over \$40,001

SECTION 8.3 Selection of Arbitrators

NACHA shall maintain a list of arbitrators to serve as the pool from which arbitrators will be selected in accordance with the procedures set forth below. Each such arbitrator must have at least five (5) years of experience in a position with responsibility for electronic payments processing. (Amended December 16, 2008)

a. **Arbitration Procedure A.** For claims subject to Arbitration Procedure A, arbitrators will be selected by the following method:

- (i) NACHA shall mail each party the same list of five (5) arbitrators from among those nominated as provided herein who are not affiliated with either party to the dispute;
- (ii) Each party shall be given ten (10) days from the date the list is mailed to review the list, delete two (2) names, and mail or deliver the remaining names to NACHA;
- (iii) NACHA shall then compare the two lists and select one (1) arbitrator not deleted from either list to decide the case; and
- (iv) If either list is not returned within the time limit specified above, NACHA shall then select the arbitrator to decide the case from among the names not deleted on the list returned, or, if neither list is returned within the time limit, from among the names on the lists as mailed to each party.

b. **Arbitration Procedure B.** For claims subject to Arbitration Procedure B, arbitrators will be selected by the following method:

- (i) NACHA shall mail each party the same list of ten (10) arbitrators from among those nominated as provided herein who are not affiliated with either party to the dispute;



- (ii) Each party will have ten (10) days from the date the list is mailed to review the list, delete three (3) names, and mail or deliver the remaining names to NACHA;
- (iii) NACHA shall then compare the two lists and select three (3) arbitrators not deleted from either list to decide the case; and
- (iv) If either list is not returned within the time limit specified above, NACHA shall then select the arbitrators to decide the case from among the names not deleted on the list returned, or, if neither list is returned within that time limit, from among the names on the list as mailed to each party.

SECTION 8.4 Presentation of the Case and the Decision

- a. ***Arbitration Procedure A.*** Cases subject to Arbitration Procedure A will be presented and the decisions reached according to the following requirements:
 - (i) After a party has received notification of the selection of the arbitrator, it will have fourteen (14) days to submit to the arbitrator in writing, with a copy to the other party, for consideration in such proceeding any matter it deems appropriate;
 - (ii) In the event the respondent, in the judgment of the arbitrator, fails to cooperate in the proceeding within fourteen (14) days of a request for information by the arbitrator, the facts as stated in the complaint shall be assumed to be true for purposes of the arbitration;
 - (iii) Once the arbitrator has received all information he or she deems relevant or necessary, the arbitrator shall have thirty (30) days to render his or her decision. The amount of the award of damages may not exceed the amount of damages claimed in the complaint;
 - (iv) The arbitrator may adopt such rules and procedures with respect to evidence and other procedural and substantive matters as he or she may deem appropriate; provided, however, such rules and procedures shall not be inconsistent with these Rules;
 - (v) The decision of the arbitrator shall be based upon these Rules insofar as they are applicable;
 - (vi) Neither party shall initiate contact with the arbitrator concerning the subject matter of the dispute unless the other party is present;
 - (vii) The arbitrator shall be entitled to recover all of the arbitrator's stipend from the party determined by the arbitrator to have been at fault in the dispute; and
 - (viii) The arbitrator shall pay his or her expenses and each party shall pay its own expenses, including attorneys' fees, in connection with the arbitration.
- b. ***Arbitration Procedure B.*** Cases subject to Arbitration Procedure B will be presented and the decisions reached according to the following requirements:
 - (i) If a hearing is to be held, the arbitrators shall set a hearing date which shall not be less than ninety (90) days after each party has received notification of the selection of the arbitrators;
 - (ii) NACHA shall provide both parties with at least thirty (30) days prior notice of the hearing;
 - (iii) Following the hearing, the arbitrators shall have thirty (30) days to render their decision to the parties to the dispute. The amount of the award of damages may not exceed the amount of damages claimed in the complaint;



- (iv) The arbitrators may adopt such rules and procedures with respect to evidence and other procedural and substantive matters as they may deem appropriate; provided, however, such rules and procedures shall not be inconsistent with these Rules;
- (v) The decision of the arbitrators shall be based upon these Rules insofar as they are applicable;
- (vi) Neither party shall initiate contact with any arbitrator concerning the subject matter of the dispute unless the other party is present;
- (vii) Each party shall pay its own expenses, including attorneys' fees, in connection with the arbitration; and
- (viii) The arbitrators shall be entitled to recover all of their travel and other expenses in connection with the arbitration and the arbitrators' stipend from the party determined by the arbitrators to be a fault in the dispute.

SECTION 8.5 Payment and Appeal

a. ***Arbitration Procedure A.*** Payments of awards and appeals of decisions will be subject to the following requirements:

- (i) The party against which such amount has been assessed shall have fourteen (14) days after receiving notice of the decision in which to pay the damage award or other amount assessed against it as provided in these Rules;
- (ii) The arbitrator's decision shall be final and binding on the parties to the dispute, and judgment thereon may be entered in any court having jurisdiction. Except to the extent such a prohibition is unlawful under the laws of the State in which the party against which damages have been awarded by the arbitrator is domiciled, such decision shall not be appealable to the courts.

b. ***Arbitration Procedure B.*** Payments of awards and appeals of decisions will be subject to the following requirements:

- (i) In the absence of an appeal to the courts, the party against which such amount has been assessed shall have fourteen (14) days after receiving notice of the decision in which to pay the damage award or other amount assessed against it as provided in these Rules;
- (ii) The arbitrators' decision shall be binding on the parties to the dispute, and judgment thereon may be entered by any court having jurisdiction. Except to the extent the parties have entered into an enforceable agreement to the contrary, either party may appeal the arbitrators' decision to the courts. In the absence of such an appeal, the arbitrators' decision shall be final.



CHAPTER NINE - SECURITY

SECTION 9.1 Compliance

Each Issuer and Acquirer is responsible for ensuring that it and each entity acting on its behalf complies with the requirements in this Chapter.

SECTION 9.2 General Issuer Requirements

Each Issuer shall comply with the following requirements for PIN management and security and shall ensure that each entity acting on its behalf complies with such requirements:

- a. **PIN Issuance.** Each Issuer may designate the PIN for each Card or may permit Cardholder selection, as permitted under the Issuer Agreement, in either case in a secure and confidential manner. Each Issuer may reissue a Card with the same PIN only if it has reason to believe that the PIN has not been compromised. The Issuer shall not put any data on a Card from which it is possible to deduct the PIN without further knowledge of any cryptographic keys.
- b. **PIN Confidentiality.** Each Issuer must ensure the confidentiality and security of the PIN during generation, issuance, storage, and verification.
- c. **PIN Verification.** Each CAS must verify the authenticity of each PIN communicated to it.
- d. **PIN Mailing.** Each Issuer shall not mail a Card and PIN advice in the same envelope, nor shall it mail a Card and PIN so that both would likely be received on the same day.
- e. **Cardholder Education.** Each Issuer must advise Cardholders about the importance of the PIN, PIN security and Card security.

SECTION 9.3 General Acquirer and Merchant Requirements

Each Acquirer shall comply with the following requirements for PIN management and security and shall ensure that each entity acting on its behalf, including any Terminal Operator, complies with such requirements:

- a. **PIN Security.** Each Acquirer shall ensure that ATMs and POS Terminals it owns, operates, controls or that accepts EBT Transactions by virtue of an agreement with such Acquirers, accept and securely encrypt PINs of 4 to 6 characters in length.
- b. **PIN Disclosure.** Each Acquirer and Merchant must instruct its employees that they are prohibited from requesting the Cardholder to disclose their PIN.
- c. **PIN Encryption Translation and Key Management.** Each Acquirer must accept and translate encrypted PINs for interchange of Transactions. Each Acquirer must perform key management as described within this Chapter.
- d. **PIN Storage Requirements.** PIN storage procedures must comply with Section 3.3 of ANSI Standard X9.8-1993. It is recommended that PINs never be stored, except with respect to Store and Forward Food Stamp Transactions. If stored, PINs must be encrypted under a unique PIN encryption key not used for any other purpose. Access to stored, encrypted PINs must be strictly controlled.

SECTION 9.4 PIN Entry

Each Acquirer must ensure compliance with the following security requirements for PIN entry at Terminals owned, operated or controlled by the Acquirer or for which the Acquirer is otherwise responsible under these Rules:



- a. **PIN Entry Order.** The first digit entered to the PIN Pad shall be the high-order digit (far left). The last digit to be entered shall be low-order (far right). Each PIN Pad must accept PINs with a variable length of four (4) to six (6) digits.
- b. **Completion Function.** Each ATM and POS Terminal must have both an enter key function in order to indicate the completion of a variable length PIN and a clear key or other function to allow the Cardholder to clear the PIN entry when an error has been made.
- c. **Non-Display of PIN.** The value of the entered PIN must not be displayed in plain text or be disclosed by audible feedback. The clear text value of the entered PIN must never be printed, electronically recorded or written to software.

SECTION 9.5 Secure Cryptographic Devices

Each Acquirer must ensure that its systems and equipment, including systems and equipment owned or operated by a third party on behalf of the Acquirer, comply with each of the following security measures regarding secure cryptographic devices. All cryptographic functions must be performed in secure cryptographic devices in which all clear text keys and PINs are physically protected against disclosure and modification. In order for an ATM, POS Terminal, or PIN Pad to qualify as a secure cryptographic device, it must meet the criteria of Section 3.18. For a Host Security Module to qualify as a secure cryptographic device, it must meet the following criteria:

- a. **Encryption.** The PIN must be encrypted using DES within the device.
- b. **Erasure.** Penetration of the device must cause immediate erasure of all PINs, cryptographic keys and all useful residue of PINs and keys contained within the device.

SECTION 9.6 PIN Transmission Requirements

Each Issuer and Acquirer shall ensure that it and each entity acting on its behalf complies with the following security requirements for PIN transmission whenever the PIN is electronically transmitted outside of a secure cryptographic device:

- a. **Reversible Encryption.** The PIN must be reversible encrypted using DEA.
- b. **Security Module.** A hardware security module must be used to perform all PIN translations.
- c. **Unique Cryptographic Keys.** All cryptographic keys relating to PIN security must be unique between each pair of communication zones of such keys; in their clear text form, these keys must reside solely within security modules and it must be impossible for any person to determine any such keys.
- d. **PIN in Unenciphered Mode.** If the PIN is to occur in the unenciphered form in any node, it shall be in a secure cryptographic device. Each secure cryptographic device shall be uniquely identifiable at the interface with connected network zones up to the authorization system of the Issuer.
- e. **Recipherment.** The Transaction PIN shall never be visible in the clear in the Acquirer central computing facility. In the event recipherment is necessary at this level, this function must be performed in a separate secure cryptographic device.
- f. **Dynamic Key Exchange.** Dynamic exchange of keys is required between the first level connection and the Switch.

SECTION 9.7 Encrypted PIN Block Format



Each Issuer and Acquirer shall ensure compliance with the following security requirements for encrypted PIN block format.

- a. **Formation of PIN Block.** The clear text PIN block and the PAN must be X'ORED together to form the standard ANSI PIN block as specified in [ANSI Standard X9.8-1995](#). The ANSI PIN block format specifies the number, position, and function of bits within a 64-bit block used as input to the DEA algorithm operating in electronic code book (ECB) mode (i.e., 64 bits in, 64 bits out). The 64-bit output of the DEA algorithm is transmitted in its entirety.
- b. **Double-Length Key.** It is recommended that a double-length (112 bits plus parity) key be used for PIN encryption, as follows:
 - (i) Encrypt the PIN block with the left half of the double-length key;
 - (ii) Decrypt this result with the right half of the double-length key; and
 - (iii) Encrypt this result using the left half of the double-length key.
- c. **Rejection of PIN Block.** Any interchange node having access to the clear text PIN block must reject the encrypted PIN block if, during encryption, reformatting, re-encryption or PIN verification, any of the following conditions are found:
 - (i) control field is not 0000 (binary);
 - (ii) PIN length entered field value is less than 4 or greater than 12; or
 - (iii) a PIN digit has a value greater than 9.
- d. **PIN Block Key Change.** The PIN block key must be changed between the first level connection and the CAS at least every 24 hours.

SECTION 9.8 Key Management

To ensure the highest level of key security, controls must exist to minimize the risk of cryptographic keys being compromised during creation, transmission, loading, storage, administration and destruction.

- a. **Key Creation Requirements.** Each key and each key component must be generated by a random or pseudo-random process.
- b. **Zone Encryption.** Where two organizations share a key to encrypt PINs communicated between them, that key must be unique to those two organizations and must not be given to any other organization. This technique of using keys unique for communication between organizations is referred to as zone encryption and is required under these Rules.
 - (i) **Zones.** A zone must start and terminate at a physically secure device. A zone begins at a device that encrypts the PIN in the zone's DES key(s) and continues through the communications facilities used to transmit the Transaction. A zone ends when the encrypted PIN is decrypted using the same DES key(s). The security of zone encryption, and the ability to change keys used within a zone without affecting other zones, is dependent upon using unique DES keys for each zone.
 - (ii) **Unique ZCMK.** Each pair of communicating organizations must have a unique zone control master key (ZCMK). All keys transmitted between the two organizations must be encrypted under this ZCMK. Such keys include unique PIN encryption keys, which are used to encrypt and decrypt PINs transmitted between the two organizations.

- (iii) **One Cryptographic Function.** Each encryption key may be used for only one cryptographic function; however, a variant of a PIN encryption key may be used for a different cryptographic function from that of the original key.
 - (iv) **Physically Secure Device.** Each Participant which processes Transactions must use a physically secure device to translate encrypted PIN blocks and other encrypted data from one zone encryption key to another.
- c. **Protection of Keys from Disclosure.** Any cryptographic key must only exist in the following forms:
- (i) **Encryption.** Encrypted using a key-encrypting key.
 - (ii) **Security of Devices.** In a physically secure device.
 - (iii) **Separation of Components.** In clear form, in at least two (2) separate components, where each component must be protected under the techniques of split knowledge and dual control. The resulting key shall be a function of all key components. Key components shall be stored in such a way that unauthorized access has a high probability of being detected. Key components must never be in the physical possession of a person when that person is or ever has been similarly entrusted with any other component of the same key.
- d. **Access.** No one person shall have the capability to access or ascertain any clear text secret key.
- e. **Detection of Secret Keys.** The system shall prevent and detect:
- (i) attempted disclosure of any secret key;
 - (ii) attempted use of a secret key for anything other than its intended purpose; and
 - (iii) unauthorized modification, substitution, deletion or insertion of any secret key.
- f. **Protection Against Key Substitution.**
- (i) **Substitution.** Each Issuer and Acquirer must prevent the unauthorized substitution of one stored key for another, whether encrypted or unencrypted.
 - (ii) **Alternative Measures.** When it is not feasible to physically or cryptographically prevent the substitution of one encrypted stored key for another, (1) it should not be feasible to ascertain clear text and corresponding cipher text encrypted under the key-encryption key, and (2) if the compromise of any key is known or suspected, both the key in question and its key encryption key must be changed.
- g. **Limiting the Effects of a Key Compromise.** The following are required to prevent the compromise of the key or keys in one cryptographic device from compromising any other cryptographic device:
- (i) **Location of Keys.** Any key-encrypting key, and any key used to encrypt a Transaction PIN in other than a PIN Pad, must be known only at two locations: the location where the key or PIN is encrypted and the location where it is decrypted.
 - (ii) **Knowledge of Keys.** Any key used to encrypt a Transaction PIN in a PIN Pad must be known only in that device and in security modules at the minimum number of facilities consistent with effective system operations. (This is to allow, for example, a POS Terminal to interface with more than one Acquirer.)
 - (iii) **Key Value.** No cryptographic keys other than those cryptographic keys used in conjunction with the operation of a Terminal by a Terminal Operator shall, except by chance, be equal to any other cryptographic key. Except by chance, the variant of a key, the irreversible transformation of a key, or keys encrypted under a key, knowledge of one cryptographic key must provide no information about any other cryptographic key.



- (iv) **Irreversible Transformation.** The irreversible transformation of a key must be used only at the same level in a key hierarchy as the original key or the level immediately below that of the original key.
 - (v) **Key Variant.** A key shall be used for only one function. The variant of a key may be used only in those devices that possessed the original key. In a unique key per Transaction scheme, a single key may be used for different security functions in the same Transaction, provided it can be shown that no misuse is possible in a given implementation.
- h. **Key Replacement.** A cryptographic key must be replaced with a new key whenever the compromise of the original key is known or suspected. The replacement key must not be a variant of the original key, nor an irreversible transformation of the original key. A compromised cryptographic key must be replaced with a new key within a reasonable time.

SECTION 9.9 Key Management Between Issuers, Acquirers and Merchants

Issuers, Acquirers and Merchants must use one of the following methods for changing keys and for establishing keys that are not encrypted under any other key:

- a. **Separation of Functions.** Two or more trusted employees may each enter a key component into the ATM, POS Terminal or PIN Pad. The ATM, POS Terminal or PIN Pad generates the key, e.g., XORing the components. No one person shall have knowledge of more than one component. The key may be similarly entered into the Issuer's, Acquirer's or Merchant's security module or may be generated by the device and printed, as with a secure PIN mailer, for use by trusted employees.
- b. **Key Conveyance.** A physical secure key-transfer device may be used to convey keys from the Acquirer's or Merchant's security module to the receiving security module, ATM, POS Terminal or PIN Pad. The device is first electronically loaded with keys by connection to the generating security module. The device is then connected to the receiving security module, ATM, POS Terminal or PIN Pad and will electronically transfer one or more keys into the security module, ATM, POS Terminal or PIN Pad. No key may be displayed or otherwise disclosed during a transfer process. The key must be erased from the conveyance device immediately after transfer to a security module, ATM, POS Terminal or PIN Pad. Such a device must be loaded and unloaded under dual control to ensure that the device input or output is not tapped to disclose a transferred key.
- c. **Key Transfers.** The Issuer's Acquirer's or Merchant's security module, or the security module of a Third Party Service Provider, may be used to directly and electronically transfer keys into ATMs, POS Terminals or PIN Pads. The above security requirements for key transfers to and from a key-transfer device apply to this "direct connect" technique as well. When a Third Party Service Provider's security module is used, information concerning the keys thus loaded must be conveyed to the receiving security module in such a way that this information cannot be compromised.

SECTION 9.10 Procedures

Each Participant, as applicable, shall implement appropriate procedures to prevent unauthorized personalization of security equipment, replacement of hardware or software, key generation and initial key loading. Each Issuer and Acquirer is responsible for maintaining up-to-date records regarding any Third Party Service Providers that manufacture or install secure cryptographic devices or load secure cryptographic devices with the initial keys.

SECTION 9.11 Separation

The security of processing Cards shall not be influenced or affected by the simultaneous processing of cards pertaining to other card schemes. In particular it shall be ensured that messages cannot be misrouted to any destination other than the intended one. To this end it is strongly recommended that only one party establishes a cryptographic key relationship with the PIN Pad so that when leaving a PIN Pad, an enciphered PIN is always routed to the same secure cryptographic device under control of the acquiring Network.



SECTION 9.12 Clearing and Reconciliation Data

If a Terminal has a removable storage medium and the data is not protected by encipherment, then only the minimum data necessary for clearing and reconciliation shall be stored. With the exception of the Card sequence number, sensitive data elements residing in the discretionary data field in Track 2, such as the CAV, shall not be recorded in the clearing and reconciliation data.

SECTION 9.13 Data Site Security

Each Issuer and Acquirer shall ensure that all data sites incorporate the following items into security procedures:

- a. data sites shall be secured 24 hours, 365 days a year;
- b. employee access to the data site shall be controlled by an electronic access system;
- c. employee access to departments within the data site shall be controlled by the electronic access system;
- d. guests, including vendors, shall be required to sign in and shall be assigned a temporary guest badge for identification;
- e. guests, including vendor service personnel, shall be escorted at all times;
- f. tapes, disks, and other storage media shall be kept in a secure access controlled environment when not being utilized by computer operations;
- g. no storage media shall leave the data site without prior management authorization;
- h. programming personnel, including contractors, shall be restricted from sensitive storage media unless prior management approval is obtained; and
- i. sensitive output shall be shredded prior to disposal.

SECTION 9.14 System Access Control Software

Each Issuer and Acquirer shall ensure that system access control software is utilized and has the following capabilities:

- a. all personnel requiring access to the system must be established within the system;
- b. access to files, data bases, Transactions, programs and executable code shall be restricted to personnel with a job description need for access;
- c. the system shall identify and verify individual access by the input of both a logon ID and password;
- d. the system must support a "blind password" display to ensure password information is not obtained from a Terminal display screen;
- e. data site procedures must be in place to ensure passwords are changed, at a minimum, every thirty (30) calendar days;
- f. data site procedures must be in place to ensure old passwords are not reissued within three (3) password change cycles;
- g. the system shall support a lock-out threshold if excessive invalid access attempts are input;



- h. production personnel shall be restricted from accessing both the development systems and the test systems and associated data;
- i. development personnel shall be restricted from accessing both the production systems and test systems and associated data; and
- j. test personnel shall be restricted from accessing the development systems and the production systems and associated data.

SECTION 9.15 Security Compliance Review

- a. ***Participants Subject to a Security Compliance Review.*** Each Issuer, Acquirer, Processor, Network, or Third Party Service Provider that handles Transactions, PINs, encryption keys, or encryption hardware or software used for encryption must perform, at its own expense, a Security Compliance Review that is verified by a qualified internal or external auditor to ensure that such Participant is in compliance with the security provisions of these Rules. If a Security Compliance Review is being conducted by an internal auditor, the auditor must not have general responsibility for electronic funds transfers for the Participant. Each Issuer is responsible for conducting its own Security Compliance Review and ensuring that any Processor, Third Party Service Provider or Network with which it has an agreement under these Rules conducts a Security Compliance Review. Each Acquirer is responsible for conducting its own Security Compliance Review and for ensuring that any Processor or Third Party Service Provider (including ESSPs and Independent Sales Organizations) that handles Transactions, Cards, PINs, encryption keys, or encryption hardware or software and with which it has an agreement under these Rules conducts a Security Compliance Review. For purposes of the provisions in this Section, a Processor shall include a Merchant that drives its own Terminals.
- b. ***Forms.*** For each Participant that completes a Security Compliance Review, an officer of the Participant who does not have operational responsibility related to the subjects covered in the Security Compliance Review shall complete and execute a Security Compliance Review either on the American Banker's Association (ABA) form "PIN Security Compliance Guideline or TG-3 or on a comparable security review form provided to a Network as a requirement for participation in such Network. For purposes of designation of eligible security review forms only, a "Network" includes one that has not entered an agreement to process Transactions. (Amended January 9, 1998)
- c. ***Timing of Security Compliance Review.*** Each new Participant described in paragraph (a) above shall complete a Security Compliance Review at least forty-five (45) calendar days prior to processing Transactions or handling PINs, encryption keys or encryption hardware or software. Thereafter, each such Participant shall complete a Security Compliance Review at least every third calendar year. An Issuer or NACHA may request that an Acquirer, Processor, Network or Third Party Service Provider complete a Security Compliance Review at an earlier date if there is cause to believe that such Participant is not in compliance with the security standards set forth in these Rules. NACHA or another Issuer may request that an Issuer complete a Security Compliance Review at an earlier date if there is cause to believe that such Issuer is not in compliance with the security standards set forth in these Rules. Any Security Compliance Review initiated in response to an identified security concern must be completed as soon as reasonably possible. At any time that a Participant subject to this Section makes a substantive change in its operations that affects security procedures, it must complete a new Security Compliance Review within forty-five (45) days of the change.
- d. ***Security Compliance Certification Statements.*** Each Participant described in paragraph (a) above must complete a Security Compliance Review certification statement, as attached hereto in Appendix III or on a comparable form filed with a Network, each calendar year in which it does not complete a Security Compliance Review. A Security Compliance Review certification statement is a certification by an officer of the Participant that there has been no substantive change in the operations that are the subject of the Security Compliance Review since the last Security Compliance Review. (Amended January 9, 1998)
- e. ***Security Exceptions and Record Retention.*** If the answer to any question on the Security Compliance Review form is other than "yes" (or otherwise indicates the Participant's inability to perform the security procedures



pursuant to these Rules), the Participant shall, at its own expense, complete the Security Compliance Review Statement and Exception Form(s), as attached hereto in Appendix III (or comparable forms filed with a Network), which must be certified by its internal auditor or an outside auditor. Each Participant that is obligated to complete a Security Compliance Review Statement and Exception Form (or comparable form filed with a Network) must also indicate the date by which any security exception noted will be remedied, and shall file with the entity that received its original Security Compliance Review Statement and Exception Form (or comparable form filed with a Network) a certification of the removal of such exception promptly upon the completion of any corrective action. The work papers, files and other information compiled during the completion of the Security Compliance Review shall be maintained by each Participant, or its outside auditor, for a period of three (3) years from the submission date of the Security Compliance Review. (Amended January 9, 1998)

- f. **Filing of Forms.** Each Security Compliance Review form, Security Compliance Review certification statement and Security Compliance Review Statement and Exception Form (or comparable Network forms) completed by a Participant other than an Issuer or CAS shall be delivered to the Participant's choice of the Issuer for that Participant or a Network acting as Designated Agent for the Issuer. Each Issuer shall deliver to NACHA, or cause any Network acting as Designated Agent to deliver (i) the Security Compliance Review form, Security Compliance Review certification statement and Security Compliance Review Statement and Exception Form (or comparable Network forms) for itself and its CAS, and (ii) a listing of all Participants that have filed the above forms with it or its Designated Agents, including a separate listing of each Participant that has filed a Security Compliance Review Statement and Exception Form (or comparable Network form) and the dates by which the Participant has indicated that any security exceptions will be remedied.
- g. **Confidentiality of Forms.** NACHA and each Issuer and Network receiving Security Compliance Review forms, Security Compliance Review certification statements or Security Compliance Review Statement and Exception Forms (or comparable Network forms) shall treat such materials as strictly confidential and shall disclose such materials only to such persons as are reasonably required to evaluate such materials and address any security issues raised by such materials.
- h. **Network Security Procedures.** These Rules are intended to accommodate and supplement Network security compliance review procedures, and do not in any way supersede such procedures. NACHA and each Network shall cooperate in utilizing such procedures to address security issues. A Network Security Compliance Review that is comparable to the Security Compliance Review under these Rules may be used to satisfy the requirements of this Section.



CHAPTER TEN - LIABILITIES AND INDEMNIFICATION

SECTION 10.1 Indemnification and Hold Harmless by Issuers

Each Issuer shall indemnify and hold harmless each other Participant against any and all claims, losses, costs, damages, liabilities or expenses (including reasonable attorneys' fees) that are incurred as a result of a Transaction, attempted Transaction or other transaction initiated with a card purporting to be a Card but which was not properly issued by or on behalf of the Issuer and that arise out of:

- a. The Authorization or denial of Authorization of a Transaction whether done by the Issuer's CAS or by a third party providing Stand-In Processing;
- b. Malfunction of or failure to operate the CAS (unless such malfunction was caused by the party claiming indemnification);
- c. Unauthorized access being obtained to the systems utilized to process, route and authorize Transactions from any point under the ownership or control of the Issuer or the CAS;
- d. The failure of the Issuer or the CAS to comply, as to any Transaction, with any Applicable Law;
- e. The negligence or fraudulent conduct of the Issuer; (*Amended September 27, 1996*) and
- f. The failure of the Issuer to comply with these Rules.

SECTION 10.2 Indemnification and Hold Harmless by Acquirers

Each Acquirer shall indemnify and hold harmless each other Participant against any and all claims, losses, costs, damages, liabilities or expenses (including reasonable attorneys' fees) that are incurred as a result of a Transaction or attempted Transaction and that arise out of:

- a. Personal injury or tangible property damage suffered or incurred by any person and caused, directly or indirectly, in whole or in part, by the placement, location, operation, condition, servicing or use of a Terminal owned, operated or controlled by an Acquirer or for which an Acquirer is otherwise responsible under these Rules or located on the premises of a Merchant with which the indemnifying Acquirer has a Merchant Agreement;
- b. Malfunction of or failure to operate the Acquirer's system for processing and routing Transactions, whether such system is operated by the Acquirer or a third party on its behalf (unless such malfunction was caused by the party claiming indemnification);
- c. Unauthorized access being obtained to the systems utilized to process, route and authorize Transactions from any point between and including the Terminal or Point of Sale through the Acquirer's system for processing and routing Transactions, whether such system is operated by the Acquirer or a third party on its behalf;
- d. The failure of the Acquirer or any Third Party Service Provider (including Terminal Operators) or Merchant with which the Acquirer has a Third Party Provider Agreement or Merchant Agreement, respectively, to comply, as to any Transaction, with any Applicable Law;
- e. The negligence or fraudulent conduct of the Acquirer, or any Third Party Service Provider (including Terminal Operators) or Merchant with which the Acquirer has a Third Party Provider Agreement or Merchant Agreement, respectively;
- f. The failure of the Acquirer or any Third Party Service Provider (including Terminal Operators) or Merchants with which the Acquirer has a Third Party Provider Agreement or Merchant Agreement to comply with these Rules;



- g. The completion by the Acquirer, its Terminal Operator or its Merchants of any Transaction denied by, or on behalf of, an Issuer; and
- h. Any agreement by a Merchant of the Acquirer with, or obligation of such Merchant to, a Cardholder with respect to the sale or lease of goods or services by means of a Transaction.

SECTION 10.3 Indemnification and Hold Harmless by Processors

Each Processor other than a Network, including each CAS and Terminal Operator, shall indemnify and hold harmless each other Participant against any and all claims, losses, costs, damages, liabilities or expenses (including reasonable attorneys' fees) that are incurred as a result of a Transaction or attempted Transaction and that arise out of:

- a. The Authorization or denial of Authorization of a Transaction by such Processor operating a CAS;
- b. Malfunction of or failure to operate the CAS, Acquirer's or Network's system for processing and routing Transactions (unless such malfunction was caused by the party claiming indemnification);
- c. Unauthorized access being obtained to the systems utilized to process, route and authorize Transactions from any point in such system that is under the ownership or control of such Processor;
- d. The failure of the Processor to comply, as to any Transaction, with any Applicable Law;
- e. The negligence or fraudulent conduct of the Processor;
- f. The failure of the Processor to comply with these Rules; and
- g. The Completion by the Processor of any Transaction denied by, or on behalf of, an Issuer.

SECTION 10.4 Liability of Networks

The liability of each Network acting in its capacity as such and not as a CAS or Terminal Operator shall be governed by such Network's rules and regulations governing the processing and routing of transactions through such Network, regardless of whether such Rules specifically reference Transactions under these Rules. If a Network operates as a CAS or Terminal Operator, it shall be treated as a Processor for purposes of Section 10.3 above.

SECTION 10.5 Liability of NACHA (Amended December 16, 2008)

NACHA, and each of their members when acting in such capacity, shall have no liability or duty of indemnity for their respective participation in drafting, updating and enforcing these Rules and otherwise performing the functions allocated to each of them hereunder.



CHAPTER ELEVEN – LICENSING OF THE QUEST MARK

SECTION 11.1 The QUEST Mark *(Amended December 16, 2008)*

NACHA is the owner of the QUEST Mark, consisting of the "Quest" word mark and the Design Mark as illustrated in the Quest Graphic Standards Manual, and such other marks as may be adopted by NACHA for use in connection with EBT Programs from time to time. The protection of the QUEST Mark is vital to all Participants to identify the nature and quality of EBT services being supplied. It is an essential responsibility of all Participants to maintain the nature and quality of services identified by the QUEST Mark, consistent with the standards established by these Rules and the Quest Graphic Standards Manual.

SECTION 11.2 License to Use the QUEST Mark

- a. NACHA hereby grants to each Issuer and Acquirer a nonexclusive, nontransferable license to use the QUEST Mark solely within the States, solely in connection with the promotion and rendering of services by each Issuer and Acquirer in connection with designated EBT Programs with the right to enter into sublicense only with Merchants with which they have entered into Merchant Agreements and for the sole purpose of facilitating the participation of such Merchants in such EBT Programs. Any other use of the QUEST Mark is prohibited without the prior express written approval of NACHA. *(Amended May 21, 1998)*
- b. Each Issuer and Acquirer acknowledges NACHA's sole ownership of the QUEST Mark, agrees that it will do nothing inconsistent with such ownership and that all use of the QUEST Mark by such Issuer or Acquirer shall inure to the benefit of and be on behalf of NACHA. No Issuer or Acquirer may use any of the QUEST Mark in its corporate name, trade name, fictitious name or trade address.
- c. Each Issuer and Acquirer agrees that all use of the QUEST Mark, as well as the nature and quality of all goods produced, services rendered and printed materials published by such Issuer or Acquirer in connection with the QUEST Mark shall conform to the standards set by and be under the control of NACHA, which standards are established and maintained by these Rules and the Quest Graphic Standards Manual; both as amended from time to time.
- d. Each Issuer and Acquirer agrees to cooperate with NACHA in maintaining NACHA's control of such nature and quality, to permit reasonable inspection of such Issuer or Acquirer's operations, and to supply NACHA with specimens of such Issuer's or Acquirer's use of the QUEST Mark upon request.
- e. Each Issuer and Acquirer shall cooperate with NACHA in executing any and all documents or in doing or refraining from doing such acts as may be reasonably necessary to enable NACHA to protect the QUEST Mark.
- f. Each Issuer and Acquirer agrees to notify NACHA promptly of any infringement, potential infringement or improper use of the QUEST Mark that shall come to such Issuer's or Acquirer's notice. NACHA shall have the sole right to engage in infringement, opposition, cancellation or unfair competition proceedings involving the QUEST Mark.
- g. Each Issuer and Acquirer agrees that it shall not state or imply that any service offered under the QUEST Mark is exclusively offered by such Issuer or Acquirer.
- h. Each Issuer and Acquirer agrees to indemnify NACHA against all claims, liabilities, losses and expenses arising from such Issuer's or Acquirer's use of the QUEST Mark.
- i. The license granted to each Issuer and Acquirer under this Section shall become effective as of the date of each Issuer's or Acquirer's first use of the QUEST Mark as an Issuer or Acquirer under these Rules, and the term shall be unlimited so long as such Issuer or Acquirer is an Issuer or Acquirer in good standing and will terminate



automatically upon expiration or termination of such Issuer's Issuer Participation Agreement or such Acquirer's Acquirer Agreement, unless such party shall have in effect another such agreement at the time of such termination.

- j. Upon termination of the license granted under Section 11.2(a), each Issuer and Acquirer agrees to cease all use of the QUEST Mark as provided in Chapter 12 of these Rules.
- k. The right to use the QUEST Mark in any form or manner will be granted only to Issuers and Acquirers, and the QUEST Mark may not be used in any form or manner until an Issuer has executed and delivered an Issuer Participation Agreement as provided in Section 1.1(b) and an Acquirer has executed an Acquirer Agreement and certified to its Issuer its ability to properly process Transactions.
- l. Each Merchant which has entered into a Merchant Agreement with an Acquirer pursuant to these Rules shall, on behalf of such Acquirer, have the right to display the QUEST Mark on decals, signs, printed and broadcast materials solely to indicate acceptance of Cards for payment. Any such display shall be in accordance with the Quest Graphic Standards Manual.
- m. No material displaying the QUEST Mark shall contain any matter that would tend to denigrate the QUEST Mark.
- n. Any use and/or display of the QUEST Mark by any Issuer or Acquirer or any of an Acquirer's Merchants not in compliance with the requirements of this Chapter and the Quest Graphic Standards Manual is actionable by NACHA under these Rules and may lead to termination or suspension of the Issuer's or Acquirer's right to process Transactions or other appropriate action if such use is not terminated and satisfactory evidence of such termination is not given to NACHA promptly after notice to cease any such use.
- o. The right to use the QUEST Mark cannot be sublicensed, other than as specified in Section 11.2(a), or assigned, whether by sale, consolidation, merger, amalgamation, operation of law, or otherwise, except with the express prior written consent of NACHA. Any attempted sublicense beyond that expressly permitted above, or assignment without the express written consent of NACHA, shall be void and of no effect. No sublicense permitted under these Rules shall extend beyond the time limitations of the license to the Issuer or Acquirer under these Rules.

SECTION 11.3 Use of QUEST Mark on Cards

The QUEST Mark shall be placed on all Cards in conformity with the design illustrated in the Quest Graphic Standards Manual.

SECTION 11.4 Responsibility for Use of the QUEST Mark

Any Issuer and Acquirer or Merchant permitted by NACHA to use the QUEST Mark shall obtain no interest in the QUEST Mark, except the right to use it in accordance with the requirements of this Chapter and the Quest Graphic Standards Manual. In addition, with respect to the QUEST Mark, each Issuer, Acquirer and Merchant shall:

- a. Whenever and however incurred, bear all costs and expense of, and full responsibility with respect to, and all liability for, its own use and, for Acquirers, its Merchants' use and any removal from use of the QUEST Mark;
- b. Comply strictly with all specifications, directives and requirements concerning copyright, patent, trademark or service mark use, as from time to time an Issuer or Acquirer may be advised of by NACHA; and
- c. At any time required by NACHA, at such Issuer and Acquirer's sole expense, remove from use the QUEST Mark and, where applicable, surrender to NACHA any depiction of the QUEST Mark in any signs, decals, advertisements, promotional material and any other written materials.

SECTION 11.5 License to Use and Reproduce Written Materials



NACHA hereby grants to each Issuer and Acquirer a personal, nontransferable, nonexclusive right and license to reproduce, on the conditions set out hereinafter, written materials, advertisements and other like promotional materials as may be hereafter from time to time created by or for NACHA for use in conjunction with the EBT Programs under the QUEST Mark. NACHA hereby further grants to each Issuer and Acquirer a similar right and license to utilize and distribute such materials in connection with such Issuer or Acquirer's participation and promotion of the EBT Programs using the QUEST Mark.

Each Issuer and Acquirer agrees that it will conform all of its use of such materials to the quality and content of the specimens which may from time to time be submitted to Issuer and Acquirer by NACHA; in that connection each Issuer and Acquirer agrees to always use the QUEST Mark in the authorized form set out in these Rules and the Quest Graphic Standards Manual. Each Issuer and Acquirer further agrees to use a proper copyright notice on all such materials in the precise form and content as such copyright notice is set out in any such materials submitted to Issuer and Acquirer by NACHA.

Should any Issuer and Acquirer fail to include in any such reproduced material a copyright notice, in conformance with such notice appearing on any specimens of such materials submitted by NACHA, or should any Issuer and Acquirer fail to include a copyright notice on other material to be disseminated by such Issuer or Acquirer upon receipt of instructions from NACHA to do so, and should any such failure result in loss of copyright or other damage to NACHA, such Issuer or Acquirer hereby agrees to compensate NACHA fully for any loss or damage occasioned by its failure to include an appropriate copyright notice on any such materials.

SECTION 11.6 Nonmember Guidelines for the Usage of the QUEST Mark

- a. It is the responsibility of each Issuer and Acquirer to ensure that any use of the QUEST Mark by its registered Third Party Service Providers and Merchants complies with the specifications described in this Chapter of the Rules and the Quest Graphic Standards Manual.
- b. Each Acquirer must ensure that all solicitation materials distributed by its registered Third Party Service Providers comply with the following guidelines:
 - (i) The Third Party Service Provider must be clearly identified as a representative of the Acquirer.
 - (ii) All solicitation materials must clearly disclose that any Merchant Agreement resulting from the solicitation will be between the Acquirer and the individual Merchant.
- c. All Third Party Service Providers are prohibited from using the QUEST Mark on their letterhead, stationery or business cards.



CHAPTER TWELVE - MISCELLANEOUS

SECTION 12.1 Termination

- a. **General.** Each Issuer or Acquirer that voluntarily terminates its processing of Transactions shall provide advance written notice to NACHA and shall continue to be bound by these Rules with respect to matters occurring prior to such termination, and shall continue to be liable with respect to Transactions initiated prior to such termination, including Correction Requests and Correction Responses of such Transactions. *(Amended December 1, 2000)*
- b. **Issuers.**
 - (i) **New Issuer.** Upon termination of an Issuer Participation Agreement, each terminated Issuer shall promptly cease use of the QUEST Mark, except as necessary to facilitate the transition to a successor Issuer.
 - (ii) **Withdrawal from Quest.** If a Government Entity determines that Cards issued on its behalf should cease participation under the QUEST Mark, the Issuer of such Cards shall cease issuing Cards or documentation bearing the QUEST Mark immediately upon its cessation of Transaction processing for such Government Entity, and, within twenty-four (24) months of such cessation, shall issue replacement cards that do not bear the QUEST Mark for all its outstanding Cards for such Government Entity.
- c. **Acquirers.** If an Acquirer's Acquirer Agreement is terminated, voluntarily or involuntarily, and such Acquirer does not have in effect another Acquirer Agreement, the terminated Acquirer shall promptly take all necessary action to cease all use of the QUEST Mark and shall promptly take all necessary action to cause its Merchants to cease all use of the QUEST Mark, unless such Merchants have entered into Merchant Agreements with other Acquirers. If a terminated Acquirer fails to take such action, NACHA may take such action itself at the expense of the Acquirer, after providing at least three (3) calendar days' notice of its intention to do so to the Acquirer.

SECTION 12.2 Amendment of the Rules

These Rules may be amended from time to time by a vote of the Board of Directors of NACHA in accordance with the NACHA by-laws. NACHA shall distribute notice of any proposed amendment of these Rules to the Registered State Representatives. If at the time of such notice there are at least 20 Registered State Representatives and sixty percent (60%) or more of such Registered State Representatives object to the adoption of such amendment in a writing delivered to the designated NACHA contact within thirty (30) days of the date of such notice, the proposed amendment shall not become effective. *(Amended December 16, 2008)*

SECTION 12.3 Placement of a Non-Quest Mark on a Card with a QUEST Mark

The use of the Quest Card at a Quest Terminal to access an Account shall be treated as a Quest Transaction subject to these Rules unless both the Quest Card and the Quest Terminal also bear the service mark of a Network and each of the following apply: (i) The Issuer has entered into an agreement with such Network for the Network to process transactions involving Accounts as transactions subject to Network Rules, (ii) the Issuer is authorized pursuant to its Issuer Agreement to enter into such agreement, and (iii) the Terminal Operator routes such transaction to the Network switch. *(Amended June 13, 1997)*

If a Government Entity determines that Cards issued on its behalf shall bear both the QUEST Mark and a Non-Quest Mark, prior notice to and coordination with NACHA shall be performed, to assure satisfaction of the requirements of the Rules as they relate to the QUEST Mark. *(Amended December 16, 2008)*

SECTION 12.4 Variances

Any Participant may seek a variance from compliance with one or more provisions of these Rules by written application to NACHA. A variance should be requested only when special circumstances warrant exemption of the specific



Participant that would not otherwise be applicable to other Participants. A variance of these Rules may be granted only by a vote of the Board of Directors of NACHA in accordance with the NACHA by-laws. NACHA shall distribute notice of any proposed variance from these Rules to the Registered State Representatives. If at the time of such notice there are at least 20 Registered State Representatives and sixty percent (60%) or more of such Registered State Representatives object to the adoption of such variance in a writing delivered to the designated NACHA contact within thirty (30) days of the date of such notice, the proposed variance shall not become effective. *(Amended December 16, 2008)*

SECTION 12.5 Fees

The Rules do not address and shall not address any transaction, processing, interchange, gateway or other fee of any kind related to Quest Transactions. *(Amended January 30, 1997 and October 8, 2002)*

SECTION 12.6 Registered State Representative *(Amended December 16, 2008)*

If a State Government Entity agrees to adopt the Quest® Operating Rules for its EBT Program, such Government Entity may appoint a Registered State Representative by providing written notice to the designated NACHA contact, provided that only one Registered State Representative may be appointed for any such participating Quest® State. Such Registered State Representative may be replaced or removed by such Government Entity at any time upon provision of written notice to the designated NACHA contact.



APPENDIX II

*(Amended January 30, 1997 and March 12, 2003)***FORM OF
ISSUER PARTICIPATION AGREEMENT**

This **Issuer Participation Agreement** (this "Agreement") is entered into as of _____, 199____, by and between _____, a _____ ("Issuer"), and the National Automated Clearing House Association ("NACHA"), a Delaware non-profit corporation, to permit Issuer to participate in an interstate system for the electronic distribution of electronic benefits under the "QUEST®" service mark, as set forth in the Quest Graphic Standards Manual (the "Mark"). Accordingly, the parties agree as follows:

1. Capitalized terms not otherwise defined herein shall have the meanings assigned in the Quest Operating Rules attached hereto, as such rules may be amended from time to time in accordance with their terms (the "Rules").
2. Issuer shall be bound by and comply with each provision of the Rules applicable to an Issuer. If Issuer acts in any capacity in addition to acting as Issuer, including acting as an Acquirer under these Rules, Issuer shall be bound by and comply with each provision of the Rules applicable to an entity acting in such capacity. Issuer may use an alternative service mark on the Cards pursuant to the Rules governing such use.
3. Issuer acknowledges that NACHA is the sole owner of the Mark and such other marks as may be adopted for use under the Rules from time to time. Issuer acknowledges that NACHA has the exclusive right to license the use of the Mark and that all use of the Mark shall inure to the benefit of NACHA. Issuer's promotion of the Mark shall be on a best efforts basis, including the marketing of Quest and signage of the QUEST Mark in accordance with the Rules and as may be required by the Issuer Agreements. Issuer agrees to abide by the terms of the nonexclusive, nontransferable license for use of the Mark contained in the Rules. Issuer shall notify NACHA of any potentially infringing use, and shall cooperate with NACHA in protecting the Mark and the quality of services provided under the Mark, at no expense to Issuer, except to the extent arising out of Issuer's improper use of the Mark or violation of the Rules or this Agreement. There shall be no fee payable to NACHA for the use of the Mark.
4. Issuer hereby represents and warrants that it has established, or will establish prior to issuing Cards bearing the QUEST Mark, telecommunications connections and computer switching facilities that will enable Interoperable Transactions to be exchanged between Issuer and its Acquirers and each other Issuer that has entered into an Issuer Participation Agreement with NACHA as of the date hereof and the Acquirers of such Issuers. Issuer's responsibility to establish arrangements with future Issuers is separately addressed in the Rules.
5. Subject to Issuer's obligations under its Issuer Agreement, Issuer may terminate this Agreement, in accordance with the Rules, upon written notice to NACHA.

IN WITNESS OF THE FOREGOING, each of the parties has caused this Agreement to be executed and delivered by its duly authorized officers.

ISSUER

By: _____

Title: _____

**NATIONAL AUTOMATED CLEARING
HOUSE ASSOCIATION**

By: _____

Title: _____



APPENDIX III

EBT SECURITY COMPLIANCE REVIEW

3.1 SECURITY COMPLIANCE CERTIFICATION FORM (Amended October 8, 1998)

EBT SECURITY COMPLIANCE CERTIFICATION FOR:

_____ (Name of EBT Participant)

I, _____, do hereby certify that:

(1) (Check One)

I am an internal auditor for _____ (the "Participant") and I have no operational responsibility for matters referenced in the Security Compliance Review.

I am an independent auditor, employed by _____ and hired by _____ (the "Participant") to complete the Security Compliance Review Form on its behalf.

(2) Pursuant to the Quest® Operating Rules Section 9.15, I have conducted my audit of the Participant in accordance with generally accepted auditing standards and have examined such records, documents, procedures, facilities and operations as I have deemed reasonably necessary to form the basis for this certification.

(3) Based on my review of the foregoing, I have completed on _____, 19____ a Security Compliance Review for the Participant and I have answered "Yes" to all questions contained therein except those questions specifically referenced in the Compliance Exception Forms attached hereto. I hereby certify that the Participant is in compliance with the requirements described in each respective section of the Security Compliance Review referenced in Section 9.15(b), except those sections of the Security Compliance Review specifically referenced in the Compliance Exception Forms attached hereto.

(4) I will maintain in my records the Security Compliance Review and all working papers related thereto for a period of three (3) years from the date of this Compliance Certification.

(5) Participant uses the following processors for the handling of EBT Transactions:

By: _____
(Auditor)



APPENDIX III

3.2 AUDIT EXCEPTION FORM (*Amended January 9, 1998*)

QUESTION # _____

Standard #

Explanation of why you cannot answer "true" to this question:

Describe action plan implemented to correct this situation:

Date expected to be in compliance: _____



3.3 ISSUER/ DESIGNATED AGENT RESPONSE FORM (Amended January 9, 1998)

To: _____

Organization: _____

Date: _____

Re: _____

We have reviewed the exception form, the action expected to be implemented and the date expected to be in compliance, and:

Agree with the expected action and completion date.

Disagree with the expected action and have attached an alternative action to be completed by the expected completion date.

Disagree with the expected action and expected completion date and have attached an alternative action and date.

Disagree with the expected completion date and suggest the following:

At the expected completion date, we will be performing the following procedures:

Issuer/Designated Agent

Date



3.4 Obtaining ANSI Standards (Amended January 9, 1998)

If your organization does not have copies of the ANSI Standards, referenced in the Compliance Review, these may be obtained by contacting the appropriate Secretariat.

To obtain copies of X9.8 and X9.24, contact:

X9 Secretariat
American Bankers Association
1120 Connecticut Avenue, NW
Washington, D.C. 20036
Phone 202/663-5284

To obtain a copy of X3.92, contact:

X3 Secretariat
Computer & Business Equipment Manufacturers Association
1250 Eye Street, NW
Suite 200
Washington, D.C. 20005
Phone 202/737-8888



QUEST® OPERATING GUIDELINES

PREFACE (Amended December 16, 2008)

The *Quest Operating Guidelines (Guidelines)* were prepared to provide additional information and detail relative to the *Quest Operating Rules (Rules)*. The *Guidelines* are intended to be used as a reference with the *Rules*. In case of any inconsistency or conflict between the *Rules* and the *Guidelines*, the *Rules* shall govern.



***Guidelines for Including Programs
Under the Quest Operating Rules
Adopted January 25, 2000***

The purpose of this paper is to provide information to states and other EBT stakeholders on programs that are covered under the Quest® Operating Rules (Rules). Since the Rules clearly state that the QUEST Mark (Mark) may appear on a card with another mark, the paper is intended to provide guidance on which programs can be covered by the QUEST Mark and which should be covered by a separate mark. Based on various factors, including technology and business relationships, states can determine which benefits and which marks they wish to have on a card.

With regard to the QUEST Mark, government programs can fall into one of the following categories:

- Covered under the QUEST Mark with no Icon
- Covered under the QUEST Mark with an Icon
- Covered under a Separate Mark

Detail on each category is provided in the sections that follow.

The Fundamental Principle: Interoperability

The most basic principle governing use of the QUEST Mark is that the Mark can only be used for programs that are interoperable. That is, benefits can be accessed in an EBT project other than the project that issued the EBT card.

Beyond this principle, one must examine whether the benefit is restricted. If a benefit is provided as unrestricted cash, it may be covered by a QUEST Mark without an icon. If the program is governed by a universal restriction that applies in all jurisdictions, it may be covered by the QUEST Mark and an Icon that is adopted to signify the restriction.

A. Programs Covered under the QUEST Mark with No Icon

Criteria: Unrestricted Cash Benefits

Discussion: Unrestricted means there is no limitation on: a) interoperability or b) what can be purchased at a Quest retailer. Program benefits that could only be accessed in the state where they were issued could not be made available under the QUEST Mark, nor could a benefit that can only be used to buy a specific good or service. If a retailer/service provider is authorized to accept Quest Transactions, a cardholder should have access to the entire balance in his/her cash account to make purchases at that retailer/service provider, or to get cash back, if offered by the retailer. Placing restrictions on use of the benefit to buy fuel or pay rent, for instance, could confuse the merchant and cardholder as to the available balance on a card. For instance, a \$200 balance might only be \$100, if half of it were restricted to rent payments. A state may however, prohibit certain types of retailers within its jurisdiction - such as liquor stores or massage parlors - from participating in EBT and displaying the QUEST Mark.

This category is limited to cash benefits because any non-cash program is, by its very nature, restricted. Food stamps, for instance, can only be used to purchase approved items at FCS-authorized retailers. Food stamps cannot be used to buy napkins, nor can they be used at all merchants that display the QUEST Mark.

Table A lists programs that should be eligible for coverage under the QUEST Mark without an icon. This list, and all lists contained in this paper, may not include all programs that fall into each category. The lists are intended to be instructive rather than definitive.

B. Programs Covered under the QUEST Mark with an Icon

Criteria: Benefits with a Universal Restriction

Discussion: If a cash or non-cash program is interoperable and has a universal restriction that is adopted by all states offering the program, the program can be covered by Quest with an icon signifying the restriction. The icon would be



displayed at the terminal accepting the card, not on the card itself. The Food Stamp Program is the only current example. The grocery bag icon on the lower left corner of the QUEST Mark indicates that a merchant accepts food stamp transactions. Another possible example for the future would be a cash program that was limited to purchase transactions (cash could not be obtained from an ATM or a POS). To accommodate such new programs NACHA will have to conduct a careful review of the Rules and program requirements. (*Amended December 16, 2008*)

To be included under Quest with an icon, a program should be national or almost national in scope, otherwise icons signifying restrictions by individual states would confuse merchants. It would be impractical and costly for merchants to monitor icons approved for use by one state or by just a few states.

Table B lists programs that should be eligible for coverage under the QUEST Mark **with an icon**.

C. Covered under a Separate Mark

Criteria: Not interoperable

Discussion: If a program is not interoperable, it cannot be covered under the QUEST Mark. In general, a program is not interoperable if benefits cannot be accessed out of the state that issued the card. The inability to access benefits out of state could be due to the programmatic restrictions. If child care dollars can only be spent at a facility licensed by the issuing state, interoperability would not be possible across state lines and the QUEST Mark could not be used. If it were not for this restriction, childcare dollars could be deposited into a cardholder's pooled cash account and covered by a QUEST Mark. Table C lists programs that must be covered under a separate mark.



TABLE A
PROGRAMS THAT MAY INCLUDED UNDER QUEST
WITH NO ICON*

Child Care
Child Health Insurance Program
Child Support
Federal Direct Payment
Federal Emergency Assistance
Foster Care
In-Home and Family Support Services
Low-Income Energy Assistance
Petty Cash
Provider Payments (non-direct deposit)
Refugee Cash Assistance
State Payroll (non-direct deposit)
TANF
TANF One-Time
Unemployment Insurance

*Note: These programs may be included under the QUEST Mark with no icon if a state has not placed restrictions on the program that would limit interoperability or cash access. This list is provided to give the reader examples of programs that may be covered under the Quest Mark without an icon. It is intended to be instructive, but not definitive. Definitive categorization is not possible due to program differences between states and modifications that may be made to programs in the future.



TABLE B
PROGRAMS THAT MAY BE COVERED UNDER
THE QUEST MARK WITH AN ICON*

Employment Service Program
Food Stamp Program
Food Stamp Employment and Training Program
Housing
Primary Health Care

* Note: This list is provided to give the reader examples of programs that may be covered under the Quest Mark with an icon. The icon would be displayed at the terminal or provider site accepting the card, not on the card itself. This list is



intended to be instructive, but not definitive. Definitive categorization is not possible due to program differences between states and modifications that may be made to programs in the future.



TABLE C
PROGRAMS THAT MUST BE COVERED UNDER A SEPARATE MARK*

Child Care with Restrictions
Chronically Ill and Disabled Children's Program
Community Care for Aged and Disabled
Family Violence
Immunizations
Job Training Partnership Act (JTPA)
Medicaid
 Long Term Care
 Transportation
 Prescription Drugs
 Medicaid ID Form
 Primary Home Care
School Lunch Program
Special Nutrition Program
State Health Program
Women, Infants, and Children (WIC)

* Note: This list is provided to give the reader examples of programs that must be covered under a separate mark. The separate mark would be governed by separate operating rules and would likely be displayed on the card and at the terminal or provider site accepting the card. Display of the QUEST Mark at the terminal would be determined by whether the terminal also accepted Quest Transactions. This list is intended to be instructive, but not definitive.



Definitive categorization is not possible due to program differences between states and modifications that may be made to programs in the future.

[CONTACT US | NACHA HOME](#)

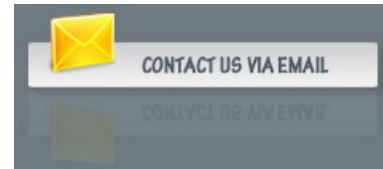
Amendments & Variances

Amendments and variances to the Quest® Operating Rules will be posted to this page, along with the status of each. Please continue to check back on a regular basis for updates.

Amendments of the Quest Operating Rules. The Quest Operating Rules may be amended from time to time by a vote of the Board of Directors of NACHA in accordance with the NACHA by-laws. NACHA shall distribute notice of any proposed amendment of the Rules to the Registered State Representatives. If at the time of such notice there are at least 20 Registered State Representatives and sixty percent (60%) or more of such Registered State Representatives object to the adoption of such amendment in a writing delivered to the designated NACHA contact within thirty (30) days of the date of such notice, the proposed amendment shall not become effective.

Variances of the Quest® Operating Rules. Any Participant may seek a variance from compliance with one or more provisions of the Rules by written application to NACHA. A variance should be requested only when special circumstances warrant exemption of the specific Participant that would not otherwise be applicable to other Participants. A variance of the Rules may be granted only by a vote of the Board of Directors of NACHA in accordance with the NACHA by-laws. NACHA shall distribute notice of any proposed variance from the Rules to the Registered State Representatives. If at the time of such notice there are at least 20 Registered State Representatives and sixty percent (60%) or more of such Registered State Representatives object to the adoption of such variance in a writing delivered to the designated NACHA contact within thirty (30) days of the date of such notice, the proposed variance shall not become effective.

Information

[Quest® Operating Rules](#)[Participating Quest Jurisdictions](#)[Amendments & Variances](#)[Quest State Agency Registration](#)[Quest Graphic Standards Manual](#)[White Papers](#)[Other Resources](#)[eGovernment Payments Council](#)

Copyright ©2003 by NACHA - The Electronic Payments Association
13450 Sunrise Valley Drive, Suite 100 Herndon, VA 20171

Appendix E: Nationwide Health Information Network

Attachment 1: DURSA Overview

Attachment 2: Data Use and Reciprocal Support Agreement (DURSA)

Attachment 3: NwHIN Onboarding Process



Page restrictions apply

● Added by [Linda Toscano](#), last edited by [Linda Toscano](#) on Jul 05, 2011 ([view change](#))

Comment:

[Go to start of metadata](#)

Introduction

In 2008, as part of the Nationwide Health Information Network Phase II Trial Implementations, a multi-disciplinary team was assembled to develop a comprehensive agreement that would create a legal framework using existing law for the electronic exchange of health data. The first version of this agreement, called the Data Use and Reciprocal Support Agreement, or DURSA, was executed by a number of Federal agencies and non-Federal organizations (the Participants) beginning in November 2009.

The executed DURSA created a Coordinating Committee and charged it with maintaining this Agreement. Pursuant to that charge, in 2010, the Coordinating Committee established a Task Group to suggest revisions to the Agreement based on the experience gained with the early implementations and to accommodate new opportunities for the promotion and expansion of health information exchange.

This Overview was prepared to facilitate the reader's understanding of the DURSA, and to place the DURSA into an appropriate context.

Why is a Data Use and Reciprocal Support Agreement (DURSA) Needed?

The DURSA is a legal agreement created to promote and establish trust among the Participants. It codifies a common set of trust expectations into an enforceable legal framework, and eliminates the need for point-to-point agreements. Because the DURSA must go through the Federal-approval process before Federal agencies can sign it, the parties have greater assurance that it has been thoroughly vetted.

What is the DURSA?

The DURSA is the legal, multi-party trust agreement that is entered into voluntarily by all entities, organizations and Federal agencies that desire to engage in electronic health information exchange with each other using an agreed upon set of national standards, services and policies developed by or under the auspices of the Office of the National Coordinator for Health IT (ONC) in the U.S. Department of Health and Human Services. (Those who sign the DURSA are known as Participants.)

The DURSA builds upon the various legal requirements that Participants are already subject to and describes the mutual responsibilities, obligations and expectations of all Participants under the Agreement. All of these responsibilities, obligations and expectations create a framework for safe and secure health information exchange, and are designed to promote trust among Participants and protect the privacy, confidentiality and security of the health data that is shared.

The DURSA is based upon the existing body of law (Federal, state, local) applicable to the privacy and

security of health information and is supportive of the current policy framework for health information exchange. The DURSA is not only a legally enforceable contract, it also represents a framework for broad-based information exchange among a set of trusted entities. The Agreement reflects consensus among the state-level, federal and private entities that were involved in the development of the DURSA regarding the following issues:

- Multi-Party Agreement
- Participants Actively Engaged in Health Information Exchange
- Privacy and Security Obligations
- Requests for Information Based on Permitted Purposes
- Duty to Respond
- Future Use of Data Received from Another Participant
- Respective Duties of Submitting and Receiving Participants
- Autonomy Principle for Access
- Use of Authorizations to Support Requests for Data
- Participant Breach Notification
- Mandatory Non-Binding Dispute Resolution
- Allocation of Liability Risk

Will the DURSA continue to evolve?

Yes. An initial group of Participants executed the DURSA in 2009 to support the first set of electronic health information exchange activities in production under the Agreement. Since then, other entities wishing to transact health information electronically using the agreed upon standards, services and policies have executed the DURSA. Additional entities are expected to execute the Agreement over time. (The November 2009 version of the DURSA is available at http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11673_910759_0_0_18/DURSA_2009_Version_for_Production_Pilots_20091123.pdf.) As a living document, the DURSA is being maintained using the process described in the Agreement. An amended and restated version of the DURSA will be available for execution in 2011.

When the Office of the National Coordinator issues final regulations addressing governance of the nationwide health information network, the Coordinating Committee will convene another Task Group to assess how the DURSA might need to be revised to accommodate the new regulations.

Can the DURSA be used for Other Purposes?

The DURSA was developed for a specific purpose – to establish the legal framework and to support the trust framework for health information exchange using an agreed upon set of standards, services and policies. Others may find this document helpful or informative for other types of information exchange models. The DURSA does not, however, contemplate other uses outside of the purpose for which it has been created. As a result, entities interested in using this Agreement for other information exchange purposes are encouraged to seek their own legal counsel regarding the applicability and appropriateness of the DURSA to other settings.

Labels parameters

Labels:

None

Top of Form

Enter labels to add to this page:





Exchange Trust Framework

[Skip to end of metadata](#)

- Page restrictions apply
- Added by [Linda Toscano](#), last edited by [Linda Toscano](#) on May 02, 2011 ([view change](#))
Comment:
[Go to start of metadata](#)

The following sections identify legal and accountability measures for the Exchange as well as broader ONC initiatives related to governance of the Nationwide Health Information Network. An overview of the Data Use and Reciprocal Support Agreement (DURSA) and a link to the DURSA follow.

Legal Measures

The [Data Use and Reciprocal Support Agreement \(DURSA\)](#) is a multi-party trust agreement that binds all parties to a common set of duties and accountability process for trust.

Accountability Measures

The Technical Committee and Coordinating Committee administer and support Exchange activities. ONC established these two committees to support the current set of Exchange Participants and functions. As new Participants and users emerge prior to completion of the governance rulemaking process, additional committees and processes are likely to evolve.

Technical Committee (TC)

Focuses on architectural and technical issues such as approval of new or modified technical requirements, specifications, and testing for the Exchange.

Members of the TC include:

- Nationwide Health Information Network and FHA Program Directors
- ONC Standards Lead
- Five representatives from the Cooperative, consisting of at least one representative from an entity in Production and at least one representative from an entity that is not in Production
- Director, Office of Policy and Planning
- Specifications and Connect Initiative Team Leads

Coordinating Committee (CC)

Provided authority by Exchange Participants to establish and maintain the set of policies, legal

agreements, and accountability measures for those entities exchanging data in production today using the Exchange.

In an operational role, the CC manages the following responsibilities:

- Committee membership and proceedings
- Admission, suspension and termination of Participants
- Receiving reports of breaches from Participants and acting upon such reports
- Resolving disputes between Participants
- Determining materiality of proposed new, or changes to technical specifications and testing plans
- Developing and amending operating policies and procedures
- Managing DURSA amendments

Members of the CC include:

- One representative from each signatory to the DURSA that is actively engaged in the exchange of data in a limited production pilot
- One representative from each entity or agency that is a party to a Definitive Plan that has been accepted by the Coordinating Committee
- Two representatives chosen by the Cooperative
- One representative from ONC

Roles and Responsibilities

Coordinating Committee Members

- Fulfill duties as specified in the DURSA and operating procedures
- Active engagement to help maintain operational Exchange and improve the Exchange to accommodate broader participation

NeHC

- Firewalled set of support functions to support Committee operations
- Separate set of activities (under ONC Cooperative Agreement) for education, stakeholder outreach, and engagement

ONC

- Ex-officio representation on Coordinating Committee
- Responsible for overall Nationwide Health Information Network Program - administered out of the Office of Interoperability and Standards (OIS)
- Nationwide Health Information Network Program governance rulemaking

ONC Initiatives related to governance of the Nationwide Health Information Network include the following:

- The HITECH Act (<http://whatishipaa.org/hitech-act.php>) instructs the National Coordinator to establish governance mechanisms for the Nationwide Health Information Network.
- ONC conducts rulemaking processes to gather input.
- The Health IT Policy Committee examines governance issues related to the broad spectrum of health information exchange scenarios. For more details, access the set of recommendations submitted to ONC on December 16, 2010 at http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_0_6011_1815_17825_43/http%3B/wci-pubcontent/publish/onc/public_communities/

[_content/files/hitpc_transmittal_letter_gov_wg_dec2010.pdf.](#)

- Leverage lessons learned from the early production exchange efforts, including the Committee processes to inform the rulemaking process.

Labels parameters

Labels:

None

Top of Form

Enter labels to add to this page:



Looking for a label? Just start typing.

Bottom of Form

1 Child Page

[Reorder Pages](#)

Page: [DURSA Overview](#)



Data Use and Reciprocal Support Agreement (DURSA)

Developed by:
NHIN Cooperative DURSA Team

November 18, 2009

Data Use and Reciprocal Support Agreement

This Data Use and Reciprocal Support Agreement is made and entered into by and between the undersigned (hereinafter referred to individually as "Participant" and collectively as "Participants") (the "DURSA" or the "Agreement") as of the Effective Date.

WITNESSETH:

WHEREAS, the Participants are either Health Information Exchanges that have each individually been accepted by the NHIN Coordinating Committee for participation in the Nationwide Health Information Network ("NHIN") ("HIE Participants"), Integrated Delivery Systems that have each individually been accepted by the NHIN Coordinating Committee for participation in the NHIN ("IDS Participants"), State agencies that have each individually been accepted by the NHIN Coordinating Committee ("State Participants"), or Federal agencies that have each individually been accepted by the NHIN Coordinating Committee for participation in the NHIN ("Federal Participants") (collectively State Participants and Federal Participants shall be referred to as "Governmental Participants");

WHEREAS, all Participants facilitate and govern the exchange of health data among groups of persons or organizations that wish to request and/or receive health data from other Participants in the NHIN;

WHEREAS, the relationship between the Participant and the individuals whose records are available within or through their respective Systems varies from Participant to Participant and, in some cases, there is no relationship at all;

WHEREAS, as a condition of participation in the NHIN, the Participants must enter into this Data Use and Reciprocal Support Agreement for purposes of electronic data exchange and have agreed to do so;

NOW, THEREFORE, for and in consideration of the mutual covenants herein contained, the Participants hereto mutually agree as follows:

1. **Definitions.** For the purposes of this Agreement, the following terms shall have the meaning ascribed to them below. All defined terms are capitalized throughout this Agreement.

- a. **Applicable Law** shall mean: (i) for the Participants that are not Federal Participants, all applicable statutes and regulations of the State(s) or jurisdiction(s) in which the Participant operates, as well as all applicable Federal statutes, regulations, standards and policy requirements; (ii) for the Federal Participants, all applicable Federal statutes, regulations, standards and policy requirements.
- b. **Authorization** shall meet the requirements and have the meaning set forth at 45 CFR § 164.508 of the HIPAA Regulations and include any similar but additional requirements under Applicable Law.

- c. **Breach** shall mean the unauthorized acquisition, access, disclosure, or use of Message Content through the NHIN. The term “Breach” does not include the following:
 - (i) any unintentional acquisition, access, disclosure, or use of Message Content through the NHIN by an employee or individual acting under the authority of a Participant or Participant User if—
 - (I) such acquisition, access, disclosure, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with the Participant or Participant User; and
 - (II) such Message Content is not further acquired, accessed, used, or disclosed by such employee or individual; or
 - (ii) any acquisition, access, use or disclosure of information contained in or available through the Participant’s System where such acquisition, access, use or disclosure was not directly related to transmission of Message Content through the NHIN.
- d. **Common NHIN Resource** shall mean software, utilities and automated tools made available for use in connection with the NHIN and which have been designated as a "Common NHIN Resource" by the NHIN Coordinating Committee and the NHIN Technical Committee.
- e. **Confidential Participant Information**, for the purposes of this Agreement, shall mean proprietary or confidential materials or information of a Discloser in any medium or format that a Discloser labels as such. Confidential Participant Information includes, but is not limited to: (i) the Discloser’s designs, drawings, procedures, trade secrets, processes, specifications, source code, System architecture, processes and security measures, research and development, including, but not limited to, research protocols and findings, passwords and identifiers, new products, and marketing plans; (ii) proprietary financial and business information of a Discloser; and (iii) information or reports provided by a Discloser to a Receiving Party pursuant to this Agreement. Notwithstanding any label to the contrary, Confidential Participant Information does not include Message Content; any information which is or becomes known publicly through no fault of a Receiving Party; is learned of by a Receiving Party from a third party entitled to disclose it; is already known to a Receiving Party before receipt from a Discloser as documented by Receiving Party’s written records; or, is independently developed by Receiving Party without reference to, reliance on, or use of, Discloser’s Confidential Participant Information. Message Content is excluded from the definition of Confidential Participant Information because other provisions of the DURSA address the appropriate protections for Message Content.
- f. **Definitive Plan** shall mean a written summary, signed by all entities or agencies that will participate in at least a limited production pilot and become signatories to the DURSA, which attests to the planned timeline, including substantive

milestones, that will allow the parties to the attestation to begin, no later than December 31, 2010, actively exchanging health information in compliance with the NHIN Specifications in at least a limited production pilot that is consistent with priorities set by the NHIN Technical Committee. The purpose of the Definitive Plan is to provide a mechanism for the NHIN Coordinating Committee to evaluate an entity's eligibility to serve on the Coordinating Committee, as described in Section 4.02 of the Agreement.

- g. **Digital Credentials** shall mean a digital certificate issued by the NHIN Coordinating Committee or its designee to Participants who meet NHIN Participant requirements as defined in the NHIN Operating Policies and Procedures. The Digital Credentials will be presented electronically to Participants to prove identity and the right to access Message Content through the NHIN and will include Server Certificates.
- h. **Discloser** shall mean a Participant that discloses Confidential Participant Information to a Receiving Party.
- i. **Dispute** shall mean any controversy, dispute, or disagreement arising out of or relating to this Agreement.
- j. **Effective Date** shall mean the date specified in Section 25.12 of this Agreement.
- k. **Health Care Operations** shall have the meaning set forth at 45 C.F.R. § 164.501 of the HIPAA Regulations.
- l. **Health Information Exchange or HIE** shall mean an organization that oversees and governs the exchange of health-related information among organizations.
- m. **Health Information Service Provider or HSP** shall mean a company or other organization that will support one or more Participants by providing them with operational, technical, or health information exchange services.
- n. **HIPAA Regulations** shall mean the Standards for Privacy of Individually Identifiable Health Information and the Security Standards for the Protection of Electronic Protected Health Information (45 C.F.R. Parts 160 and 164) promulgated by the U.S. Department of Health and Human Services under the Health Insurance Portability and Accountability Act (HIPAA) of 1996, as in effect on the date of this Agreement and as may be amended, modified, or renumbered.
- o. **Integrated Delivery System or IDS** shall mean a network of health care providers or organizations that provide a continuum of health care services to a defined population, or a health plan with care delivery components that represent a substantial proportion of its operations. An IDS may, but does not necessarily need to, include community and/ or tertiary hospitals, home health care and hospice services, primary and specialty outpatient care and surgery centers, social services, rehabilitation, preventive care, health education, and managed care financing.

- p. **Material** shall mean, for the purposes of Section 11.03 only, the implementation of, or change to, a NHIN Performance and Service Specification that will: (i) have a significant adverse operational or financial impact on at least 20% of Participants; (ii) require at least 20% of Participants to materially modify their existing agreements with or policies or procedures that govern Participant Users or third parties as required by Sections 17.04 and 17.05; or (iii) require an amendment to this Agreement.
- q. **Message** shall mean a mechanism for exchanging Message Content between Participants through the NHIN, which complies with the NHIN Performance and Service Specifications. Messages are intended to include all types of electronic transactions in the exchange, including, but not limited to, requests, assertions, responses, and notifications, including the data or records transmitted with those transactions.
- r. **Message Content** shall mean that information which is requested or sent by a Participant to another Participant through the NHIN. This includes, but is not limited to, Protected Health Information (PHI), individually identifiable information, de-identified data (as defined in the HIPAA Regulations), pseudonymized data, metadata, Digital Credentials, and schema.
- s. **Nationwide Health Information Network (NHIN)** shall mean a secure, nationwide, interoperable health information infrastructure that allows for the exchange of Message Content between and among Participants in support of the provision and improvement of health and healthcare services.
- t. **NHIN Operating Policies and Procedures** shall mean the policies and procedures adopted by the NHIN Coordinating Committee that describe management, operation, and participation in the NHIN, attached hereto as Attachment 3 and as amended from time to time in accordance with Section 12.03.
- u. **NHIN Performance and Service Specifications** shall mean the NHIN Test Approach and the NHIN Specifications.
- v. **NHIN Specifications** shall mean the specifications adopted by the NHIN Technical Committee to prescribe the data content, technical, and security requirements necessary to support information exchange among NHIN Participants. The NHIN Specifications are attached hereto as Attachment 1, and as amended from time to time in accordance with Sections 11.02 and 11.03.
- w. **NHIN Test Approach** shall mean the framework for Testing and demonstrations for parties seeking to participate in the NHIN. The NHIN Test Approach is attached hereto as Attachment 2, and as amended from time to time in accordance with Sections 11.02 and 11.03.
- x. **Notice or notify** shall mean a written communication, unless otherwise specified in this Agreement, sent to the appropriate Participant's representative at the address listed in Attachment 4 or the NHIN Coordinating Committee in accordance with Section 24.

- y. **ONC** shall mean the Office of the National Coordinator for Health Information Technology in the Office of the Secretary, U.S. Department of Health and Human Services.
- z. **Participant** shall mean any organization that (i) meets the requirements for participation in the NHIN as contained in the NHIN Operating Policies and Procedures; (ii) is provided with Digital Credentials; and (iii) is a signatory to this Agreement or a Joinder Agreement.
- aa. **Participant Users** shall mean those persons who have been authorized to access Message Content in connection with the NHIN through the respective Participant's System and in a manner defined by the respective Participant. "Participant Users" may include, but are not limited to, health care providers; individuals whose health information is contained within, or available through, a Participant's System; and employees, contractors, or agents of a Participant.
- bb. **Payment** shall have the meaning set forth at 45 C.F.R. § 164.501 of the HIPAA Regulations.
- cc. **Permitted Purposes** shall mean the following reasons for which Participant Users may legitimately exchange Message Content through the NHIN:
- Treatment of the individual who is the subject of the Message by the requesting Participant User or Recipient;
 - Payment, provided that: (i) the requesting Participant User is a Health Care Provider (as that term is defined at 45 C.F.R. § 160.103) of the individual who is the subject of the Message, and (ii) the requesting Participant User is requesting Message Content for its own use; and (iii) the Message Content is being transmitted to the requesting Participant User;
 - Health Care Operations, provided that (i) the requesting Participant User has an established Treatment relationship with the individual who is the subject of the Message; (ii) the purpose of the request is for those Health Care Operations listed in paragraphs (1) or (2) of the definition of Health Care Operations in 45 C.F.R. § 164.501 or health care fraud and abuse detection or compliance; and (iii) the requesting Participant User is requesting Message Content for its own use;
 - Public health activities and reporting as permitted by both the HIPAA Regulations at 45 C.F.R. § 164.512(b) and other Applicable Law;
 - Reporting on such clinical quality measures and such other measures to demonstrate "meaningful use," as specified in regulations promulgated by the Department of Health and Human Services under the American Recovery and Reinvestment Act, Sections 4101 and 4102 and as permitted by both the HIPAA Regulations and other Applicable Law; and
 - Uses and disclosures pursuant to an Authorization provided by the individual who is the subject of the Message or such individual's personal representative in accordance with 45 C.F.R. § 164.502(g) of the HIPAA Regulations.

- dd. **Protected Health Information or PHI** shall have the meaning set forth at 45 C.F.R. § 160.103 of the HIPAA Regulations.
 - ee. **Receiving Party** shall mean a Participant that receives Confidential Participant Information from a Discloser.
 - ff. **Recipient** shall mean the person(s) or organization(s) that receives Message Content from a Responding Participant for a Permitted Purpose. “Recipients” may include, but are not limited to, Participant Users and Requesting Participants.
 - gg. **Requesting Participant** shall mean the Participant that submits a Message, on behalf of a Participant User, which initiates an exchange of Message Content. A Requesting Participant is also a Recipient upon receipt of Message Content from a Responding Participant.
 - hh. **Responding Participant** shall mean the Participant that receives or responds to a Message from a Requesting Participant.
 - ii. **Server Certificates** shall mean a digital certificate that enables web servers to operate in a secure mode by unambiguously identifying and authenticating a server and encrypting any information passed between the server and a web browser.
 - jj. **System** shall mean software, portal, platform, or other electronic medium controlled by a Participant through which the Participant conducts its health information exchange related activities. For purposes of this definition, it shall not matter whether the Participant controls the software, portal, platform, or medium through ownership, lease, license, or otherwise.
 - kk. **Testing** shall mean the tests and demonstrations of a Participant’s System and processes used for interoperable health information exchange, to assess conformity with the NHIN Specifications and NHIN Test Approach.
 - ll. **Treatment** shall have the meaning set forth at 45 C.F.R. § 164.501 of the HIPAA Regulations.
2. **Incorporation of Recitals.** The Recitals set forth above are hereby incorporated into this Agreement in their entirety and shall be given full force and effect as if set forth in the body of this Agreement.
 3. **Purpose of the DURSA.** The purpose of this Agreement is to provide a legal framework that will enable Participants to exchange Message Content through the NHIN.
 4. **NHIN Coordinating Committee.**
 - 4.01. **Formation of the NHIN Coordinating Committee.** To accomplish the necessary planning, consensus building, and consistent approaches to developing, implementing, and operating the NHIN, there will be a NHIN Coordinating Committee.
 - 4.02. **Composition of the NHIN Coordinating Committee.** The NHIN Coordinating Committee shall be composed of (i) one representative from ONC; (ii) one representative from each signatory to the DURSA that is actively engaged in the

exchange of Message Content in at least a limited production pilot; (iii) one representative from each entity or agency that is a party to a Definitive Plan that has been accepted by the NHIN Coordinating Committee; and (iv) two representatives chosen by the Cooperative's Leadership Group. An entity or agency shall have only one representative on the NHIN Coordinating Committee even if it meets the requirements of multiple categories of membership as listed above. No entity or agency shall be party to a Definitive Plan unless it can demonstrate to the satisfaction of the NHIN Coordinating Committee that, at the time the Definitive Plan is submitted, it is conducting electronic transactions or exchanges of health information through production systems on a routine and on-going basis, with sufficient data to support priorities as defined by the NHIN Technical Committee.

- 4.03. **Grant of Authority.** The Participants hereby grant to the NHIN Coordinating Committee the right to provide oversight and facilitation for the continued development, implementation, and operation of the NHIN by conducting activities for the NHIN including, but not limited to, the following:

- a. Reviewing, evaluating, and acting upon Definitive Plans submitted by organizations that want to become members of the NHIN Coordinating Committee;
- b. Determining whether to admit new participants to the NHIN;
- c. Suspending or terminating Participants in accordance with Section 21 of this Agreement (Suspension and Termination);
- d. Receiving reports of Breaches and acting upon such reports in accordance with Section 16.03 of this Agreement (Breach Notification);
- e. Resolving Disputes between Participants in accordance with Section 23 of this Agreement (Dispute Resolution);
- f. Determining materiality of proposed new, or changes to existing, NHIN Performance and Service Specifications in accordance with Section 11.03 of this Agreement;
- g. Developing and amending NHIN Operating Policies and Procedures in accordance with Section 12 of this Agreement;
- h. Managing the amendment of this Agreement in accordance with Section 25.02 of this Agreement; and
- i. Fulfilling all other responsibilities delegated by the Participants to the NHIN Coordinating Committee as set forth in this Agreement.

To the extent permitted under Applicable Law, this grant of authority to the NHIN Coordinating Committee is unconditional and does not require any further consideration or action by any Participant.

- 4.04. In no case shall a Participant be required to disclose PHI to the Coordinating Committee in violation of Applicable Law. The Coordinating Committee shall not retaliate against a Participant that decides not to disclose PHI upon the request of the Coordinating Committee.

5. NHIN Technical Committee.

- 5.01. **Formation of the NHIN Technical Committee.** To accomplish the necessary priority-setting and oversight of changes to the NHIN Performance and Service Specifications, the parties to this Agreement acknowledge that ONC will arrange for the formation of a NHIN Technical Committee.
- 5.02. **Composition of the NHIN Technical Committee.** The NHIN Technical Committee shall be composed of no more than six ONC officials or personnel, including the individuals serving as the NHIN program lead and Federal Health Architecture (FHA) lead, and technical experts with appropriate expertise in the following areas: (i) standards and interoperability; (ii) policy and NHIN technical matters; and (iii) FHA technical matters. The NHIN Technical Committee shall also include five representatives chosen by the NHIN Cooperative Leadership Group. The NHIN Program Lead shall be the Chairperson of the NHIN Technical Committee.
- 5.03. **Grant of Authority.** The Participants hereby grant to the NHIN Technical Committee the right to prioritize NHIN functions and capabilities, including NHIN Performance and Service Specifications to be developed or modified; and, oversee and adopt changes to NHIN Performance and Service Specifications in accordance with Section 11.03 of this Agreement. To the extent permitted under Applicable Law, this grant of authority to the NHIN Technical Committee is unconditional and does not require any further consideration or action by any Participant.

6. Use of Message Content.

- 6.01. **Permitted Purposes.** The NHIN shall be used only for Permitted Purposes as defined in this Agreement. Each Participant shall require that its Participant Users only use the NHIN for the Permitted Purposes.
- 6.02. **Permitted Future Uses.** Subject to this Section 6.02 and Section 21.07, Recipients may retain, use and re-disclose Message Content received in response to a Message in accordance with Applicable Law and the Recipient's record retention policies and procedures. If the Recipient is a Participant that is a Business Associate of its Participant Users, such Participant may retain, use and re-disclose Message Content received in response to a Message in accordance with Applicable Law and the agreements between the Participant and its Participant Users.
- 6.03. **Management Uses.** The NHIN Coordinating Committee may request information from Participants, and Participants shall provide requested information, for the purposes listed in Section 4.03 of this Agreement. Notwithstanding the preceding sentence, in no case shall a Participant be required to disclose PHI to the Coordinating Committee in violation of Applicable Law. Any information, other than Message Content, provided by a Participant to the NHIN Coordinating Committee shall be labeled as Confidential Participant Information and shall be treated as such in accordance with Section 18.

7. **System Access Policies.** Each Participant shall have policies and procedures in place that govern its Participant Users' ability to access information on or through the Participant's System and through the NHIN ("Participant Access Policies"). Each Participant acknowledges that Participant Access Policies will differ among them as a result of differing

Applicable Law and business practices. Each Participant shall be responsible for determining whether and how to respond to a Message based on the application of its Participant Access Policies to the information contained in the assertions that accompany the Message as required by the NHIN Performance and Service Specifications. The Participants agree that each Participant shall comply with the Applicable Law, this Agreement, and the NHIN Performance and Service Specifications in responding to Messages.

8. **Enterprise Security.**

- 8.01. **General.** Each Participant shall be responsible for maintaining a secure environment that supports the operation and continued development of the NHIN. Participants shall use appropriate safeguards to prevent use or disclosure of Message Content other than as permitted by this Agreement, including appropriate administrative, physical, and technical safeguards that protect the confidentiality, integrity, and availability of that Message Content. Appropriate safeguards for non-Federal Participants shall be those identified in the HIPAA Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and C, as safeguards, standards, ‘required’ implementation specifications, and ‘addressable’ implementation specifications to the extent that the ‘addressable’ implementation specifications are reasonable and appropriate in the Participant’s environment. If an ‘addressable’ implementation specification is not reasonable and appropriate in the Participant’s environment, then the Participant must document why it would not be reasonable and appropriate to implement the implementation specification and implement an equivalent alternative measure if reasonable and appropriate. Appropriate safeguards for Federal Participants shall be those required by Applicable Law related to information security. Each Participant shall, as appropriate under either the HIPAA Regulations, or under Applicable Law, have written privacy and security policies in place by the earlier of the Participant’s respective Effective Date or the date on which its submits a Definitive Plan to the NHIN Coordinating Committee. Participants shall also be required to comply with any NHIN Performance and Service Specifications or NHIN Operating Policies and Procedures adopted by the NHIN Technical Committee or NHIN Coordinating Committee, respectively, that define expectations for Participants with respect to enterprise security.
- 8.02. **Malicious Software.** In participating in the NHIN, each Participant shall ensure that it employs security controls that meet applicable industry or Federal standards so that the information and Message Content being transmitted and any method of transmitting such information and Message Content will not introduce any viruses, worms, unauthorized cookies, trojans, malicious software, “malware,” or other program, routine, subroutine, or data designed to disrupt the proper operation of a System or any part thereof or any hardware or software used by a Participant in connection therewith, or which, upon the occurrence of a certain event, the passage of time, or the taking of or failure to take any action, will cause a System or any part thereof or any hardware, software or data used by a Participant in connection therewith, to be improperly accessed, destroyed, damaged, or otherwise made inoperable. In the absence of applicable industry standards, each Participant shall use all commercially reasonable efforts to comply with the requirements of this Section.

9. **Equipment and Software.** Each Participant shall be responsible for procuring, and assuring that its Participant Users have or have access to, all equipment and software necessary for it to participate in the NHIN. Each Participant shall ensure that all computers and electronic devices owned or leased by the Participant and its Participant Users to be used in connection with the NHIN are properly configured, including, but not limited to, the base workstation operating system, web browser, and Internet connectivity.
10. **Auditing.** Each Participant represents that, through its agents, employees, and independent contractors, it shall have the ability to monitor and audit all access to and use of its System related to this Agreement, for system administration, security, and other legitimate purposes. Each Participant shall perform those auditing activities required by the NHIN Performance and Service Specifications.

11. Performance and Service Specifications.

- 11.01. **General Compliance.** Each Participant shall comply with: (i) the NHIN Specifications; and (ii) the NHIN Test Approach. The NHIN Specifications and NHIN Test Approach are collectively referred to as the “NHIN Performance and Service Specifications.”
- 11.02. **Adoption of Performance and Service Specifications.** The Participants hereby grant the NHIN Technical Committee or its designee the power to adopt new NHIN Performance and Service Specifications, and to adopt amendments to, or repeal and replacement of, the NHIN Performance and Service Specifications at any time through the NHIN Performance and Service Specification Change Process described in Section 11.03.
- 11.03. **NHIN Performance and Service Specification Change Process.**
 - a. **Determination of Materiality.** The NHIN Technical Committee shall provide reasonable advance notification to the NHIN Coordinating Committee of any proposed new, or change to existing, NHIN Performance and Service Specifications. Upon receiving such notification, the NHIN Coordinating Committee shall determine, in its sole discretion, whether such proposal is Material. If the NHIN Coordinating Committee determines that the proposed NHIN Performance and Service Specification is not Material, then the NHIN Technical Committee shall follow the change process in Section 11.03(b). If the NHIN Coordinating Committee determines that the proposed NHIN Performance and Service Specification is Material, then the NHIN Technical Committee shall follow the change process in Section 11.03(c).
 - b. **Non-Material Changes to NHIN Performance and Service Specifications.** The NHIN Technical Committee may implement any new NHIN Performance and Service Specification, or amend, or repeal and replace any existing NHIN Performance and Service Specifications, at any time by providing the Participants notice of the change at least thirty (30) days prior to the effective date of the change so long as the new or amended NHIN Performance and Service Specification is not Material. Within fifteen (15) days of receiving notice of the non-Material change, a Participant may request that the NHIN Technical Committee delay implementation of the change based on unforeseen

complications or other good cause. The NHIN Technical Committee shall respond to a request to delay implementation within seven (7) days of receiving the request.

- c. **Material Changes to NHIN Performance and Service Specifications.** If the implementation of a new NHIN Performance and Service Specification, or change to any existing NHIN Performance and Service Specification, is Material, the NHIN Technical Committee shall notify Participants of the proposed Material change and allow Participants thirty (30) days to submit written comments to the NHIN Technical Committee regarding the proposed Material change. Within sixty (60) days of issuing notice of the proposed Material change, but not before either the end of the thirty (30) day written comment period or acknowledgement that all Participants have responded, the NHIN Technical Committee shall convene a meeting at which the Participants will be allowed to present information on the proposed Material change to the NHIN Technical Committee. Within ninety (90) days of issuing notice of the proposed Material change, the NHIN Technical Committee shall consider and evaluate both written comments received during the comment period and information presented at the meeting, make any revisions to the proposed Material change that are necessary, and provide the Participants final notice of the Material change. Participants shall be given at least one hundred and twenty (120) days after the NHIN Technical Committee provides the final notice to comply with the Material change.
- d. **Change Required to Comply with Federal Statutes or Regulations or the Stability of the NHIN.** If a new or changed NHIN Performance and Service Specification is required for the NHIN or Participants to comply with Federal statute or regulations or to maintain the stability of the NHIN (e.g. the performance and integrity of data exchanged among NHIN Participants), the NHIN Technical Committee shall seek input from the NHIN Coordinating Committee prior to implementing such change, but is not required to follow the processes required by Sections 11.03(b) and (c). The NHIN Technical Committee shall not require Participants to comply with such new or changed NHIN Performance and Service Specification prior to the legally required effective date of such Federal statutes or regulations. The NHIN Technical Committee shall notify Participants immediately in the event of a change that is required in order to comply with Federal statutes or regulations or to maintain the stability of the NHIN.
- e. **Participant Duty to Terminate Participation.** If, as a result of a change made by the NHIN Technical Committee in accordance with this Section 11.03, a Participant will not be able to comply with the NHIN Performance and Service Specifications or does not otherwise desire to continue participating in the NHIN after such change becomes effective, then such Participant shall terminate its participation in the NHIN in accordance with Section 21.02.

12. NHIN Operating Policies and Procedures.

- 12.01. **General Compliance.** Each Participant shall comply with the NHIN Operating Policies and Procedures.
- 12.02. **Development of the NHIN Operating Policies and Procedures.** The Participants hereby grant the NHIN Coordinating Committee the power to develop the NHIN Operating Policies and Procedures, and to amend, or repeal and replace, the NHIN Operating Policies and Procedures at any time through the NHIN Operating Policy and Procedure Change Process described in Section 12.03.
- 12.03. **NHIN Operating Policy and Procedures Change Process.** The NHIN Coordinating Committee may implement any new NHIN Operating Policy and Procedure, or amend, or repeal and replace any existing NHIN Operating Policy and Procedure, at any time by obtaining the approval of at least two-thirds of the non-governmental Participants and at least two-thirds of the Governmental Participants. The NHIN Coordinating Committee shall provide notice of the change at least thirty (30) days prior to the effective date of the change. Within fifteen (15) days of receiving notice of the change, a Participant may request that the NHIN Coordinating Committee delay implementation of the change based on unforeseen complications or other good cause. The NHIN Coordinating Committee shall respond to a request to delay implementation within seven (7) days of receiving the request.

13. Expectations of Participants.

13.01. Minimum Requirement for All Participants.

- a. All Participants that allow their respective Participant Users to submit Messages that seek Message Content for Treatment shall have a corresponding reciprocal duty to respond to Messages that seek Message Content for Treatment. A Participant shall fulfill its duty to respond by either (i) responding to the Message with the requested Message Content or, (ii) responding with a standardized response that indicates the Message Content is not available or cannot be exchanged. All responses to Messages shall comply with NHIN Performance and Service Specifications, this Agreement, any agreements between Participants and their Participant Users, and Applicable Law. Participants may, but are not required to, respond to Messages that seek Message Content for Permitted Purposes other than Treatment. Nothing in this Section 13.01(a) shall require a disclosure that is contrary to a restriction placed on the Message Content by a patient pursuant to Applicable Law.
- b. Each Participant that allows its respective Participant Users to submit Messages that seek Message Content for Treatment shall exchange Message Content with all other Participants for Treatment, in accordance with Sections 7, 13.01(a) and 15 of this Agreement. If a Participant desires to stop exchanging Message Content with another Participant based on the other Participant's acts or omissions in connection with the NHIN or this Agreement, the Participant may temporarily stop exchanging Message Content with such Participant, to the extent necessary to address the Participant's concerns, and shall notify the NHIN Coordinating Committee of such cessation and the reasons supporting the cessation. The Participants shall submit the Dispute leading to the cessation to the Dispute Resolution Process in Section 23. If the cessation is a result of a

Breach that was reported to, and deemed resolved by, the NHIN Coordinating Committee pursuant to Section 16.03, the Participants involved in the Breach and the cessation shall engage in the Dispute Resolution Process in Section 23 in an effort to attempt to reestablish trust and resolve any security concerns arising from the Breach.

13.02. **Participant Users and HSPs.** Each Participant shall require that all of its Participant Users and HSPs use the NHIN only in accordance with the terms and conditions of this Agreement, including without limitation those governing the use, confidentiality, privacy, and security of Message Content. Each Participant shall discipline appropriately any of its employee Participant Users, or take appropriate contractual action with respect to contractor Participant Users or HSPs, who fail to act in accordance with the terms and conditions of this Agreement relating to the privacy and security of Message Content, in accordance with Participant's employee disciplinary policies and procedures and its contractor and vendor policies and contracts, respectively.

13.03. **License to Common NHIN Resources.** Participant is hereby granted a nonexclusive, nontransferable, revocable and limited license to Common NHIN Resources solely for use as a Requesting Participant or a Responding Participant in performance of this Agreement. Participant shall not (a) sell, sublicense, transfer, exploit or, other than pursuant to this Agreement, use any Common NHIN Resources for Participant's own financial benefit or any commercial purpose, or (b) reverse engineer, decompile, disassemble, or otherwise attempt to discover the source code to any Common NHIN Resources. THE COMMON NHIN RESOURCES ARE PROVIDED "AS IS" AND "AS AVAILABLE" WITHOUT ANY WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT.

14. **Specific Duties of a Requesting Participant.** A Requesting Participant shall be responsible for:

- 14.01. Submitting each Message to the NHIN in compliance with the NHIN Performance and Service Specifications and NHIN Operational Policies and Procedures, including representing that the Message is: (i) for a Permitted Purpose; (ii) supported by appropriate legal authority for obtaining the Message Content; and (iii) submitted by a Participant User with the legal authority to make such a request;
- 14.02. Authenticating that Recipient is an authorized Participant User within the Participant's System and that Recipient has represented that it has requested the Message Content for a Permitted Purpose in accordance with the NHIN Performance and Service Specifications;
- 14.03. Sending any assertions required by the NHIN Performance and Service Specifications or NHIN Operational Policies and Procedures with the Message; and
- 14.04. Transmitting a copy of the Authorization, if such Authorization forms the sole legal basis for the Permitted Purpose. Nothing in this Section shall be interpreted as requiring a Requesting Participant to obtain or transmit an Authorization for Message

Content related to Treatment, Payment, or Health Care Operations, consistent with the Permitted Purposes, even though certain Responding Participants require such Authorization to comply with Applicable Law.

15. Specific Duties of a Responding Participant. A Responding Participant shall be responsible for:

- 15.01. Authenticating requests for Message Content, meaning that the Responding Participant shall confirm and verify that the request was submitted by a Requesting Participant, in accordance with the NHIN Performance and Service Specifications and NHIN Operating Policies and Procedures;
- 15.02. In accordance with Section 7, determining whether and how to respond to a Message based on the application of its Participant Access Policies to the information contained in the assertions that accompany a Message;
- 15.03. Responding to all authenticated Messages that seek Message Content for Treatment, in accordance with this Agreement, the NHIN Performance and Service Specifications, and the NHIN Operating Polices and Procedures. The Participant may respond to Messages that seek Message Content for a Permitted Purpose other than Treatment, in accordance with this Agreement, the NHIN Performance and Service Specifications, and the NHIN Operating Polices and Procedures;
- 15.04. Authenticating its response to a Message by confirming and verifying that it is transmitting the requested Message Content to the Requesting Participant, in accordance with NHIN Performance and Service Specifications;
- 15.05. Ensuring that any requirements under the Responding Participant's Applicable Law, the NHIN Performance and Services Specifications, or the NHIN Operating Policies and Procedures including, but not limited to, obtaining consent and Authorization, if required, have been met before making Message Content available for exchange through the NHIN; and
- 15.06. For Federal Participants only, in addition to complying with Sections 15.01 through 15.05, ensuring that Message Content transmitted adhere to interoperability standards adopted by the Secretary of Health and Human Services, and the National Institute of Standards and Technology (NIST) and the Federal Information Processing Standards (FIPS), as applicable.

16. Privacy and Security.

- 16.01. **Applicability of HIPAA Regulations.** The Message Content exchanged through the NHIN and in accordance with this Agreement may contain PHI. Furthermore, some, but not all, Participants are either Covered Entities or Business Associates of Covered Entities, as those terms are defined in the HIPAA Regulations. Because the Participants are limited to exchanging Message Content through the NHIN for only Permitted Purposes, the Participants do not intend to become Business Associates of each other by virtue of signing this Agreement or exchanging Message Content. As a result, the DURSA is not intended to serve as a Business Associate Agreement among the Participants. To support the privacy, confidentiality, and security of the Message Content and the NHIN, each Participant agrees as follows:

- a. If the Participant is a Covered Entity, the Participant does, and at all times shall, comply with the HIPAA Regulations to the extent applicable.
 - b. If the Participant is a Business Associate of a Covered Entity, the Participant does, and shall at all times, comply with the provisions of its Business Associate Agreements and Applicable Law.
 - c. If the Participant is a Governmental Participant, the Participant does, and at all times shall, comply with the applicable privacy and security laws and regulations to which it is subject.
 - d. If the Participant is neither a Covered Entity, a Business Associate nor a Governmental Participant, the Participant shall, as a contractual standard, at all times, at a minimum, comply with the provisions of the HIPAA Regulations set forth in Attachment 5 as if it were acting in the capacity of a Covered Entity or such other standards as decided by the NHIN Coordinating Committee.
- 16.02. **Safeguards.** In accordance with Sections 8, 9 and 10, Participant agrees to use reasonable and appropriate administrative, physical, and technical safeguards and any NHIN Performance and Service Specifications and NHIN Operating Policies and Procedures to protect Message Content and to prevent use or disclosure of Message Content other than as permitted by Section 6 of this Agreement.

16.03. **Breach Notification.**

- a. Each Participant agrees that within one (1) hour of discovering information that leads the Participant to reasonably believe that a Breach may have occurred, it will alert other Participants whose Message Content may have been Breached and the NHIN Coordinating Committee to such information. As soon as reasonably practicable, but no later than twenty-four (24) hours after determining that a Breach occurred, the Participant will notify all Participants likely impacted by the Breach and the NHIN Coordinating Committee or its designee of such Breach. The notification should include sufficient information for the NHIN Coordinating Committee to understand the nature of the Breach. For instance, such notification could include, to the extent available at the time of the notification, the following information:
 - One or two sentence description of the Breach
 - Description of the roles of the people involved in the Breach (e.g. employees, Participant Users, service providers, unauthorized persons, etc.)
 - The type of Message Content Breached
 - Participants likely impacted by Breach
 - Number of individuals or records impacted/estimated to be impacted by the Breach
 - Actions taken by the Participant to mitigate the Breach
 - Current Status of the Breach (under investigation or resolved)
 - Corrective action taken and steps planned to be taken to prevent a similar Breach.

The Participant shall have a duty to supplement the information contained in the notification as it becomes available and cooperate with other Participants and the

NHIN Coordinating Committee or its designee in accordance with Section 22(e) of this Agreement. The notification required by this Section 16.03 shall not include any PHI. If, on the basis of the notification, a Participant desires to stop exchanging Message Content with the Participant that reported a Breach, it shall stop exchanging Message Content in accordance with Section 13.01(b) of this Agreement. If, on the basis of the notification, the NHIN Coordinating Committee or its designee determines that (i) the other Participants that have not been notified of the Breach would benefit from a summary of the notification or (ii) a summary of the notification to the other Participants would enhance the security of the NHIN, it may provide, in a timely manner, a summary to such Participants that does not identify any of the Participants or individuals involved in the Breach.

- b. Information provided by a Participant in accordance with this Section 16.03, except Message Content, may be “Confidential Participant Information.” Such “Confidential Participant Information” shall be treated in accordance with Section 18.
- c. This Section 16.03 shall not be deemed to supersede a Participant’s obligations (if any) under relevant security incident, breach notification or confidentiality provisions of Applicable Law.
- d. Compliance with this Section 16.03 shall not relieve Participants of any other security incident or breach reporting requirements under Applicable Law including, but not limited to, those related to consumers.

17. **Representations and Warranties.** Each Participant hereby represents and warrants the following:

17.01. **Accurate Participant Information.** Except to the extent prohibited by Applicable Law, each Participant has provided, and will continue to provide, the NHIN Coordinating Committee with all information reasonably requested by the NHIN Coordinating Committee and needed by the NHIN Coordinating Committee to discharge its duties under this Agreement or Applicable Law, including during the Dispute Resolution Process. Any information provided by a Participant to the NHIN Coordinating Committee shall be responsive and accurate. Each Participant shall provide notice to the NHIN Coordinating Committee if any information provided by the Participant to the NHIN Coordinating Committee materially changes. Each Participant acknowledges that the NHIN Coordinating Committee reserves the right to confirm or otherwise verify or check, in its sole discretion, the completeness and accuracy of any information provided by a Participant at any time and each Participant will reasonably cooperate with the NHIN Coordinating Committee in such actions, given reasonable prior notice.

17.02. **Execution of the DURSA.** Prior to participating in the NHIN, each Participant shall have executed this Agreement and returned an executed copy of this Agreement to the NHIN Coordinating Committee. In doing so, the Participant affirms that it has full power and authority to enter into and perform this Agreement and has taken whatever measures necessary to obtain all required approvals or consents in order for it to execute this Agreement. The representatives signing this Agreement on behalf of

the Participants affirm that they have been properly authorized and empowered to enter into this Agreement on behalf of the Participant.

- 17.03. **Compliance with this Agreement.** Except to the extent prohibited by Applicable Law, each Participant shall comply fully with all provisions of this Agreement. To the extent that a Participant delegates its duties under this Agreement to a third party (by contract or otherwise) and such third party will have access to Message Content, that delegation shall be in writing and require the third party to agree to the same restrictions and conditions that apply through this Agreement to a Participant.
- 17.04. **Agreements with Participant Users.** Each Participant has valid and enforceable agreements with each of its Participant Users that require the Participant User to, at a minimum: (i) comply with all Applicable Law; (ii) reasonably cooperate with the Participant on issues related to this Agreement; (iii) submit a Message through the NHIN only for Permitted Purposes; (iv) use Message Content received through the NHIN in accordance with the terms and conditions of this Agreement; (v) as soon as reasonably practicable after determining that a Breach occurred, report such Breach to the Participant; and (vi) refrain from disclosing to any other person any passwords or other security measures issued to the Participant User by the Participant. Notwithstanding the foregoing, for Participant Users who are employed by a Participant or who have agreements with the Participant which became effective prior to the Effective Date, compliance with this Section 17.04 may be satisfied through written policies and procedures that address items (i) through (vi) of this Section 17.04 so long as the Participant can document that there is a written requirement that the Participant User must comply with the policies and procedures.
- 17.05. **Agreements with Technology Partners.** To the extent that a Participant uses technology partners in connection with the NHIN, each Participant affirms that it has valid and enforceable agreements with each of its technology partners, including HSPs, that require the technology partner to, at a minimum: (i) comply with Applicable Law; (ii) protect the privacy and security of any Message Content to which it has access; (iii) as soon as reasonably practicable after determining that a Breach occurred, report such Breach to the Participant; and (iv) reasonably cooperate with the other Participants to this Agreement on issues related to the NHIN, under the direction of the Participant.
- 17.06. **Compliance with Specifications, Policies and Procedures.** Each Participant affirms that it fully complies with the NHIN Performance and Service Specifications and the NHIN Operating Policies and Procedures as more fully discussed in Sections 11.01 and 12.01 of this Agreement.
- 17.07. **Creation of Test Data.** Certain Participants have agreed to anonymize PHI to create Test Data to be used by other Participants for Testing. Each Participant that has so agreed represents that the Test Data do not contain PHI and further represents that it has created the Test Data in accordance with the Test Approach.
- 17.08. **Accuracy of Message Content.** When acting as a Responding Participant, each Participant, in accordance with Section 19.02, hereby represents that at the time of transmission, the Message Content it provides is (a) an accurate representation of the data contained in, or available through, its System, (b) sent from a System that

employs security controls that meet industry standards so that the information and Message Content being transmitted are intended to be free from malicious software in accordance with Section 8.02, and (c) provided in a timely manner and in accordance with the NHIN Performance and Service Specifications and NHIN Operating Policies and Procedures. Other than those representations in Sections 17.07, 17.08 and 17.09, the Responding Participant makes no other representation, express or implied, about the Message Content.

- 17.09. **Express Warranty of Authority to Transmit** Message Content. To the extent each Participant is a Responding Participant and is providing Message Content to a Recipient, each Participant represents and warrants that it has sufficient authority to provide or make such Message Content available to Recipient.
- 17.10. **Use of Message Content.** Each Participant hereby represents and warrants that it shall use the Message Content only in accordance with the provisions of this Agreement.
- 17.11. **Compliance with Laws.** Each Participant will, at all times, fully comply with all Applicable Law relating to this Agreement, the exchange of Message Content for Permitted Purposes and the use of Message Content.
- 17.12. **Absence of Final Orders.** Each Participant hereby represents and warrants that, as of the Effective Date, it is not subject to a final order issued by any Federal, State, local or international court of competent jurisdiction or regulatory or law enforcement organization, which will materially impact the Participant's ability to fulfill its obligations under this Agreement. Each Participant shall inform the NHIN Coordinating Committee if at any point during its participation in the NHIN it becomes subject to such an order.
- 17.13. **Federal Program Participation.** Each non-Federal Participant hereby represents and warrants that it is not excluded, debarred, or otherwise ineligible from participating in Federal contracts, subcontracts, grants, and nonprocurement transactions ("Federal Programs"). Each non-Federal Participant will immediately provide written notice to the NHIN Coordinating Committee if it is suspended, proposed for debarment or other exclusion, or otherwise disqualified or declared ineligible from participating in a Federal Program for any reason, or is a party to a legal proceeding that may result in any such action.

18. Confidential Participant Information.

- 18.01. Each Receiving Party shall hold all Confidential Participant Information in confidence and agrees that it shall not, during the term or after the termination of this Agreement, redisclose to any person or entity, nor use for its own business or benefit, any information obtained by it in connection with this Agreement, unless such use or redisclosure is permitted by the terms of this Agreement.
- 18.02. Confidential Participant Information may be redisclosed under operation of law, provided that the Receiving Party immediately notifies the Discloser of the existence, terms and circumstances surrounding such operation of law to allow the Discloser its rights to object to such disclosure. If after Discloser's objection, the Receiving Party

is still required by law to redisclose Discloser's Confidential Participant Information, it shall do so only to the minimum extent necessary to comply with the operation of the law and shall request that the Confidential Participant Information be treated as such.

19. Disclaimers.

- 19.01. **Reliance on a System.** Each Participant acknowledges and agrees that: (i) the Message Content provided by, or through, its System is drawn from numerous sources, and (ii) it can only confirm that, at the time Message Content is transmitted by the Responding Participant, the information and Message Content transmitted are an accurate representation of data contained in, or available through, its System. Nothing in this Agreement shall be deemed to impose responsibility or liability on a Participant related to the clinical accuracy, content or completeness of any Message Content provided pursuant to this Agreement. The Participants acknowledge that other Participants' Digital Credentials may be activated, suspended or revoked at any time or the Participant may suspend its participation; therefore, Participants may not rely upon the availability of a particular Participant's Message Content.
- 19.02. **Incomplete Medical Record.** Each Participant acknowledges that Message Content received in response to a Message may not include the individual's full and complete medical record or history. Such Message Content will only include that data which is the subject of the Message and available for exchange among Participants in the NHIN.
- 19.03. **Patient Care.** Message Content obtained through a Message is not a substitute for any Participant or Participant User, if that person/entity is a health care provider, obtaining whatever information he/she/it deems necessary, in his/her professional judgment, for the proper treatment of a patient. The Participant or Participant User, if he/she/it is a health care provider, shall be responsible for all decisions and actions taken or not taken involving patient care, utilization management, and quality management for their respective patients and clients resulting from, or in any way related to, the use of the NHIN or the Message Content made available thereby. None of the Participants, by virtue of executing this Agreement, assume any role in the care of any patient.
- 19.04. **Carrier lines.** All Participants acknowledge that the exchange of Message Content between Participants is to be provided over various facilities and communications lines, and information shall be transmitted over local exchange and Internet backbone carrier lines and through routers, switches, and other devices (collectively, "carrier lines") owned, maintained, and serviced by third-party carriers, utilities, and Internet service providers, all of which may be beyond the Participants' control. Provided a Participant uses reasonable security measures, no less stringent than those directives, instructions, and specifications contained in this Agreement, the NHIN Performance and Service Specifications, and the NHIN Operating Policies and Procedures, the Participants assume no liability for or relating to the integrity, privacy, security, confidentiality, or use of any information while it is transmitted over those carrier lines, which are beyond the Participants' control, or any delay, failure, interruption, interception, loss, transmission, or corruption of any Message Content or other

information attributable to transmission over those carrier lines which are beyond the Participants' control. Use of the carrier lines is solely at the Participants' risk and is subject to all Applicable Law.

- 19.05. **No Warranties.** EXCEPT AS REPRESENTED IN SECTION 17.08, THE MESSAGE CONTENT OBTAINED BY A RECIPIENT ARE PROVIDED "AS IS" AND "AS AVAILABLE" WITHOUT ANY WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT. IT IS EXPRESSLY AGREED THAT IN NO EVENT SHALL THE PARTICIPANT BE LIABLE FOR ANY SPECIAL, INDIRECT, CONSEQUENTIAL, OR EXEMPLARY DAMAGES, INCLUDING BUT NOT LIMITED TO, LOSS OF PROFITS OR REVENUES, LOSS OF USE, OR LOSS OF INFORMATION OR DATA, WHETHER A CLAIM FOR ANY SUCH LIABILITY OR DAMAGES IS PREMISED UPON BREACH OF CONTRACT, BREACH OF WARRANTY, NEGLIGENCE, STRICT LIABILITY, OR ANY OTHER THEORIES OF LIABILITY, EVEN IF THE PARTICIPANT HAS BEEN APPRISED OF THE POSSIBILITY OR LIKELIHOOD OF SUCH DAMAGES OCCURRING. THE PARTICIPANT DISCLAIMS ANY AND ALL LIABILITY FOR ERRONEOUS TRANSMISSIONS AND LOSS OF SERVICE RESULTING FROM COMMUNICATION FAILURES BY TELECOMMUNICATION SERVICE PROVIDERS OR OTHER THIRD PARTIES.
- 19.06. **Performance of the NHIN.** The Participant makes no representation, express or implied, as to the performance of the NHIN. This disclaimer is not intended to diminish or limit in any way the other representations and warranties that the Participant is making in this Agreement. It is intended to recognize that the overall performance of the NHIN is beyond the power of any individual Participant to control.

20. **Liability.**

- 20.01. **Participant Liability.** As between Participants to this Agreement: Each Participant shall be responsible for its acts and omissions and not for the acts or omissions of any other Participant. In circumstances involving harm to other Participants caused by the acts or omissions of individuals who access the NHIN, Message Content or Confidential Participant Information through the Participant or by use of any password, identifier, or log-on received or obtained directly or indirectly, lawfully or unlawfully, from the Participant or any of the Participant Users, each Participant shall be responsible for such harm to the extent that the individual's access was caused by the Participant's breach of the Agreement or its negligent conduct for which there is a civil remedy under Applicable Law. Notwithstanding any provision in this Agreement to the contrary, Participant shall not be liable for any act or omission if a cause of action for such act or omission is otherwise prohibited by Applicable Law, [or for which a defense exists for the United States under the Federal Tort Claims Act.](#) This section shall not be construed as a hold harmless or indemnification provision.

- 20.02. **Effect of Agreement.** Except as provided in Section 19.05 ("No Warranties") and Article 23 ("Dispute Resolution"), nothing in this Agreement shall be construed to

restrict a Participant's right to pursue all remedies available under law for damages or other relief arising from acts or omissions of other Participants related to the NHIN or this Agreement, or to limit any rights, immunities or defenses to which a Participant or Participant User may be entitled under Applicable Law.

- 20.03. **Coordinating Committee and Technical Committee Liability.** Each Participant has agreed to comply with this Agreement. Accordingly, the Participants shall not hold the NHIN Coordinating Committee or NHIN Technical Committee liable for or relating to any impairment of the privacy, security, confidentiality, integrity, availability, or restricted use of any information on a Participant's System resulting from any Participant's actions or failures to act, except to the extent such action or failure to act was directed by the NHIN Coordinating Committee or the NHIN Technical Committee.

21. Term, Suspension and Termination.

- 21.01. **Term.** The initial term of this Agreement shall be for a period of one year commencing on the Effective Date. Upon the expiration of the initial term, this Agreement shall automatically renew for successive one-year terms unless terminated pursuant to this Section 21.

21.02. Suspension or Termination by Participant.

- a. A Participant may voluntarily suspend its own participation in the NHIN for a valid purpose, as determined by the NHIN Coordinating Committee, by giving the NHIN Coordinating Committee at least twenty-four (24) hours prior written notice. Once proper notice is given, the NHIN Coordinating Committee shall be empowered to suspend the Participant's Digital Credentials as of the date of suspension specified in the notice. Once the NHIN Coordinating Committee suspends the Participant's Digital Credentials, the NHIN Coordinating Committee shall provide notice of such voluntary suspension to all other Participants. During the suspension, neither the Participant, nor its Participant Users, shall access the NHIN or be responsible for complying with the terms of this Agreement except those terms that survive termination of this Agreement in accordance with Section 25.05. Any voluntary suspension shall be for no longer than five (5) consecutive calendar days or for more than twenty (20) calendar days during any twelve (12) month period, unless a longer period is agreed to by the NHIN Coordinating Committee.
- b. A Participant may terminate its participation in the NHIN by terminating this Agreement, with or without cause, by giving the NHIN Coordinating Committee at least five (5) business days prior written notice. Once proper notice is given, the NHIN Coordinating Committee shall be empowered to revoke the Participant's Digital Credentials as of the date of termination specified in the notice. Once the NHIN Coordinating Committee revokes the Participant's Digital Credentials, the NHIN Coordinating Committee shall provide notice of such revocation to the remaining Participants.

- 21.03. **Suspension by Coordinating Committee.** Upon the Coordinating Committee completing a preliminary investigation and determining that there is a substantial

likelihood that a Participant's acts or omissions create an immediate threat or will cause irreparable harm to another party including, but not limited to, a Participant, a Participant User, the NHIN, or an individual whose Message Content is exchanged through the NHIN, the Participants hereby grant to the Coordinating Committee the power to summarily suspend, to the extent necessary to address the threat posed by the Participant, a Participant's Digital Credentials, pending the submission and approval of a corrective action plan, as provided in this Section. Upon suspension, the Coordinating Committee shall immediately suspend the Participant's Digital Credentials and within twelve (12) hours of suspending a Participant's right to participate in the NHIN (i) provide notice of such suspension to all Participants; and (ii) provide to the suspended Participant a written summary of the reasons for the suspension. The Participant shall use reasonable efforts to respond to the suspension notice with a detailed plan of correction or an objection to the suspension within three (3) business days or, if such submission is not reasonably feasible within three (3) business days, then at the earliest practicable time. If the Participant submits a plan of correction, the Coordinating Committee will within five (5) business days review and either accept or reject the plan of correction. If the plan of correction is accepted, the Coordinating Committee will, upon completion of the plan of correction, reinstate the Participant's Digital Credentials and provide notice to all Participants of such reinstatement. If the plan of correction is rejected, the Participant's suspension will continue, during which time the NHIN Coordinating Committee and the Participant shall work in good faith to develop a plan of correction that is acceptable to both the Participant and the NHIN Coordinating Committee. At any time after the NHIN Coordinating Committee rejects a Participant's plan of correction, either the Participant or the NHIN Coordinating Committee may submit a Dispute to the Dispute Resolution Process described in Section 23. If the Coordinating Committee and the Participant cannot reach agreement on a plan of correction through the Dispute Resolution Process, the Coordinating Committee may terminate the Participant in accordance with Section 21.04.

21.04. Termination by Coordinating Committee. The Participants hereby grant to the Coordinating Committee the power to terminate a Participant's participation in the NHIN as follows:

- a. After taking a suspension action in accordance with Section 21.03 when there is a substantial likelihood that the Participant's acts or omissions create an immediate threat or will cause irreparable harm to another party including, but not limited to, a Participant, a Participant User, the NHIN, or an individual whose Message Content is exchanged through the NHIN; or
- b. In the event a Participant is in material default of the performance of a duty or obligation imposed upon it by this Agreement and such default has not been substantially cured within thirty (30) days following receipt by the defaulting Participant of written notice thereof from the Coordinating Committee.

A Participant whose Digital Credentials are revoked by virtue of termination may appeal such revocation through the Dispute Resolution Process. However, during the pendency of any such appeal, the Participant's Digital Credentials may continue to be revoked at the discretion of the NHIN Coordinating Committee.

- 21.05. **Effect of Termination.** Upon any termination of this Agreement for any reason, the terminated party shall cease to be a Participant and thereupon and thereafter neither that party nor its Participant Users shall have any rights to use the NHIN (unless such Participant Users have an independent right to access the NHIN through another Participant). The Coordinating Committee shall revoke a terminated Participant's Digital Credentials, which will terminate Participant's ability to access the NHIN. Once the Coordinating Committee revokes the Participant's Digital Credentials, the Coordinating Committee shall provide notice of such revocation to the remaining Participants. In the event that any Participant(s) are terminated, this Agreement will remain in full force and effect with respect to all other Participants. Certain provisions of this Agreement survive termination, as more fully described in Section 25.05 (Survival Provisions).
- 21.06. **Confidential Participant Information.** All information used, provided, or created in accordance with this Section 21, except for Message Content, shall be labeled as "Confidential Participant Information" and shall be treated as such in accordance with Section 18.
- 21.07. **Disposition of Message Content on Termination.** At the time of termination, Recipient may, at its election, retain Message Content on Recipient's System in accordance with the Recipient's document and data retention policies and procedures, Applicable Law, and the terms and conditions of this Agreement, including Section 6.02.
22. **Cooperation.** Each Participant understands and acknowledges that numerous activities with respect to the NHIN shall likely involve another Participant's employees, agents, and third party contractors, vendors, or consultants. To the extent not legally prohibited, each Participant shall: (a) cooperate fully with the NHIN Coordinating Committee, each other Participant, and any such third parties with respect to such activities as they relate to this Agreement; (b) provide such information to the NHIN Coordinating Committee, each other Participant, or such third parties as they may reasonably request for purposes of performing activities related to this Agreement; (c) devote such time as may reasonably be requested by the NHIN Coordinating Committee to review information, meet with, respond to, and advise the NHIN Coordinating Committee or other Participants with respect to activities as they relate to this Agreement; (d) provide such reasonable assistance as may be requested by the NHIN Coordinating Committee when performing activities as they relate to this Agreement; and (e) subject to a Participant's right to restrict or condition its cooperation or disclosure of information in the interest of preserving privileges in any foreseeable dispute or litigation or protecting a Participant's Confidential Participant Information, provide information and assistance to the NHIN Coordinating Committee or other Participants in the investigation of Breaches and Disputes. In no case shall a Participant be required to disclose PHI in violation of Applicable Law. In seeking another Participant's cooperation, each Participant shall make all reasonable efforts to accommodate the other Participant's schedules and operational concerns. A Participant shall promptly report, in writing, to any other Participant and the NHIN Coordinating Committee, any problems or issues that arise in working with the other Participant's employees, agents, or subcontractors that threaten to delay or otherwise adversely impact a Participant's ability to fulfill its responsibilities under this Agreement.

This writing shall set forth in detail and with clarity the problems that the Participant has identified.

23. Dispute Resolution.

23.01. **General.** The Participants acknowledge that it may be in their best interest to resolve Disputes through an alternative dispute resolution process rather than through civil litigation. The Participants have reached this conclusion based upon the fact that the legal and factual issues involved in this Agreement are unique, novel, and complex and limited case law exists which addresses the legal issues that could arise from this Agreement. Therefore, the Participants shall submit Disputes related to this Agreement to the non-binding Dispute Resolution Process attached hereto as Attachment 6 and incorporated herein. Except in accordance with Section 23.02(a), if a Participant refuses to participate in the Dispute Resolution Process, such refusal shall constitute a material breach of this Agreement and may be grounds for termination in accordance with Section 21.04(b).

23.02. Immediate Injunctive Relief.

- a. Notwithstanding Section 23.01, a Participant may be relieved of its obligation to participate in the Dispute Resolution Process if such Participant (i) believes that another Participant's acts or omissions create an immediate threat to the confidentiality, privacy or security of Message Content exchanged through the NHIN or will cause irreparable harm to another party (Participant, Participant User, NHIN or consumer) and (ii) pursues immediate injunctive relief against such other Participant in a court of competent jurisdiction. The Participant pursuing immediate injunctive relief must notify the NHIN Coordinating Committee of such action within 24 hours of filing for the injunctive relief and of the result of the action within 24 hours of learning of same.
- b. If the injunctive relief sought in Section 23.02(a) is not granted and the Participant seeking such relief chooses to pursue the Dispute, the Participants must then submit to the Dispute Resolution Process in accordance with Section 23.01.

23.03. **Activities during Dispute Resolution Process.** Pending resolution of any Dispute under this Agreement, the Participants agree to fulfill their responsibilities in accordance with this Agreement, unless the Participant voluntarily suspends its participation in the NHIN in accordance with Section 21.02(a), is suspended in accordance with Section 21.03, or exercises its right to cease exchanging Message Content in accordance with Section 13.01(b).

23.04. **Implementation of Agreed Upon Resolution.** If, at any point during the Dispute Resolution Process, all of the Participants to the Dispute accept a proposed resolution of the Dispute, the Participants agree to implement the terms of the resolution in the agreed upon timeframe.

23.05. **Reservation of Rights.** If, following the Dispute Resolution Process, in the opinion of any involved Participant, the mandatory Dispute Resolution Process failed to adequately resolve the Dispute, the Participant(s) may pursue any remedies available to it in a court of competent jurisdiction.

24. **Notices.** All notices to be made under this Agreement shall be given in writing to the appropriate Participant's representative at the address listed in Attachment 4 or the NHIN Coordinating Committee, and shall be deemed given: (i) upon delivery, if personally delivered; (ii) upon the date indicated on the return receipt, when sent by the United States Postal Service Certified Mail, return receipt requested; and (iii) if by facsimile telecommunication or other form of electronic transmission, upon receipt when the notice is directed to a facsimile telecommunication number or electronic mail address listed on Attachment 4 and the sending facsimile machine or electronic mail address receives confirmation of receipt by the receiving facsimile machine or electronic mail address.

25. **Miscellaneous/General.**

- 25.01. **Governing Law.** In the event of a Dispute between or among the Participants arising out of this Agreement, the applicable Federal and State conflicts of law provisions that govern the operations of the Participants involved in the Dispute shall determine governing law.
- 25.02. **Amendment.** This Agreement may be amended in accordance with the Change Process described in Section 12.03. However, if the change is required for the NHIN, the NHIN Coordinating Committee, or Participants to comply with Applicable Law, the NHIN Coordinating Committee may implement the change with approval of at least a majority of non-governmental Participants and at least a majority of Governmental Participants and within a time period the NHIN Coordinating Committee determines is appropriate under the circumstances. All Participants shall be required to sign an amendment adopted in accordance with the provisions of this Section or terminate participation in the NHIN in accordance with Section 21.02.
- 25.03. **Additional Participants.** Upon the NHIN Coordinating Committee's acceptance of new participant in the NHIN, the NHIN Coordinating Committee shall have the new participant execute and become bound by this Agreement. To accomplish this, the new participant will enter into a Joinder Agreement, the form of which is attached hereto as Attachment 7, pursuant to which the new participant agrees to be bound by this Agreement. The Participants agree that upon execution of the Joinder Agreement by a duly authorized representative of the NHIN Coordinating Committee, all then-current Participants shall be deemed to be signatories to the Joinder Agreement with the result being that current Participants and the new participant are all bound by this Agreement. The new participant shall not be granted the right to participate in the NHIN until both it and the NHIN Coordinating Committee execute the Joinder Agreement.
- 25.04. **Assignment.** No Party shall assign or transfer this Agreement, or any part thereof, without the express written consent of the NHIN Coordinating Committee. Any assignment that does not comply with the requirements of this Section 25.04 shall be void and have no binding effect.
- 25.05. **Survival.** The provisions of Sections 6.02, 6.03, 16, 17.10, 18, 20, 21.06, 21.07, 22 and 23 shall survive the termination of this Agreement for any reason.

- 25.06. **Waiver.** No failure or delay by any Participant in exercising its rights under this Agreement shall operate as a waiver of such rights, and no waiver of any right shall constitute a waiver of any prior, concurrent, or subsequent right.
- 25.07. **Entire Agreement.** This Agreement, together with all Attachments, sets forth the entire and only Agreement among the Participants relative to the subject matter hereof. Any representation, promise, or condition, whether oral or written, not incorporated herein, shall not be binding upon any Participant.
- 25.08. **Validity of Provisions.** In the event that a court of competent jurisdiction shall hold any Section, or any part or portion of any Section of this Agreement, invalid, void or otherwise unenforceable, each and every remaining Section or part or portion thereof shall remain in full force and effect.
- 25.09. **Priority.** In the event of any conflict or inconsistency between a provision in the body of this Agreement and any attachment hereto, the terms contained in the body of this Agreement shall prevail.
- 25.10. **Headings.** The headings throughout this Agreement are for reference purposes only, and the words contained therein may in no way be held to explain, modify, amplify, or aid in the interpretation or construction of meaning of the provisions of this Agreement. All references in this instrument to designated "Sections" and other subdivisions are to the designated Sections and other subdivisions of this Agreement. The words "herein," "hereof," "hereunder," and other words of similar import refer to this Agreement as a whole and not to any particular Section or other subdivision.
- 25.11. **Relationship of the Participants.** The Participants are independent contracting entities. Nothing in this Agreement shall be construed to create a partnership, agency relationship, or joint venture among the Parties. Neither the NHIN Coordinating Committee nor any Participant shall have any authority to bind or make commitments on behalf of another Participant for any purpose, nor shall any such Party hold itself out as having such authority. No Participant shall be held liable for the acts or omissions of another Participant.
- 25.12. **Counterparts.** With respect to the first two Participants to this Agreement, the Effective Date shall be the date on which the second Participant executes this Agreement. For all Participants thereafter, the Effective Date shall be the date that the Participant executes this Agreement or the Joinder Agreement, in accordance with Section 25.03. This Agreement or the Joinder Agreement may be executed in any number of counterparts, each of which shall be deemed an original as against the Participant whose signature appears thereon, but all of which taken together shall constitute but one and the same instrument.
- 25.13. **Third-Party Beneficiaries.** With the exception of the Participants to this Agreement, there shall exist no right of any person to claim a beneficial interest in this Agreement or any rights occurring by virtue of this Agreement.
- 25.14. **Force Majeure.** A Participant shall not be deemed in violation of any provision of this Agreement if it is prevented from performing any of its obligations by reason of: (a) severe weather and storms; (b) earthquakes or other disruptive natural occurrences; (c) strikes or other labor unrest; (d) power failures; (e) nuclear or other

civil or military emergencies; (f) terrorist attacks; (g) acts of legislative, judicial, executive, or administrative authorities; or (h) any other circumstances that are not within its reasonable control. This Section 25.14 shall not apply to obligations imposed under Applicable Law.

- 25.15. **Time Periods.** Any of the time periods specified in this Agreement may be changed pursuant to the mutual written consent of the NHIN Coordinating Committee and the affected Participant(s).

This Agreement has been entered into and executed by officials duly authorized to bind their respective parties.

[REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK]

This Agreement has been entered into and executed by officials duly authorized to bind their respective parties.

Michael Matthews	Date:
Chief Executive Officer	MedVirginia

	Date:
	Social Security Administration

W. Scott Gould	Date:
Deputy Secretary	US Department of Veterans Affairs

Robert A. Petzel, M.D.	Date:
Under Secretary for Health	Veterans Health Administration

Stephen B. Thacker, M.D., M.Sc. RADM (Ret.), USPHS	Date:
Acting Deputy Director Office of Surveillance, Epidemiology and Laboratory Services	Centers for Disease Control and Prevention

Richard D. Daniels	Date:
Senior Vice President and Business Information Officer	Kaiser Permanente

Attachment 1 - NHIN Specifications

Accessible on the NHIN Resources Page:

http://healthit.hhs.gov/portal/server.pt?open=512&objID=1194&parentname=CommunityPage&parentid=18&mode=2&in_hi_userid=10882&cached=true

Attachment 2 - NHIN Test Approach and Test Materials

Accessible on the NHIN Resources Page:

http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10731_848165_0_0_18/NHIN%20Trial%20Implementation%20Test%20Approach%20and%20Test%20Materials%20V2.0%2012.12.08%20FINAL-3.pdf

Attachment 3 - NHIN Operating Policies and Procedures

Accessible on the NHIN Resources Page:

http://healthit.hhs.gov/portal/server.pt?open=512&objID=1407&parentname=CommunityPage&parentid=5&mode=2&in_hi_userid=10741&cached=true

Attachment 4 - Participant Addresses for Notice

Primary Contact	Alternate Contact
<p>Centers for Disease Control and Prevention</p> <p>Charles Magruder Senior Advisor CENT Bldg 2500 Rm 2319 - MS E68 Atlanta, GA 30333 Phone: 404-498-2443 E-mail: zgu4@cdc.gov Fax: 404-498-6565</p>	<p>Centers for Disease Control and Prevention</p> <p>Sudevi Ghosh Attorney Advisor CLFT Bldg 21 Rm 10119 - MS D53 Atlanta, GA 30333 Phone: 404-639-7016 E-mail: gqg4@cdc.gov Fax: 404-639-7351</p>
<p>MedVirginia</p> <p>Attn: Michael Matthews Chief Executive Officer 2201 West Broad Street, #202 Richmond VA 23220 Phone: 804-359-4500 x 225 E-mail: mmatthews@cvhn.com Fax: 804-359-1021</p>	<p>MedVirginia</p> <p>Attn: Jean McGraw Chief Operations Officer 2201 West Broad Street, #202 Richmond VA 23220 Phone: 804.359.4500 x229 E-mail: jmcgraw@cvhn.com Fax: 804-359-1021</p>
<p>Kaiser Permanente</p> <p>Attn: Richard D. Daniels Senior Vice President and Business Information Officer 1800 Harrison St., 24th floor Oakland, CA 94612 Phone (510) 267 - 5317 E-mail: richard.d.daniels@kp.org Fax: (510) 267- 2155</p>	<p>Kaiser Permanente</p> <p>Attn: Allen Samelson Senior Counsel One Kaiser Plaza, 21Lakeside Oakland, CA 94612 Phone (510) 271- 6927 E-mail: allen.samelson@kp.org Fax: (510) 267- 2128</p>
<p>Social Security Administration</p> <p>Name: Title: 416 Altmeyer 6401 Security Blvd. Baltimore, MD 21235 Phone E-mail: Fax:</p>	<p>Social Security Administration</p> <p>Name: Title: 416 Altmeyer 6401 Security Blvd. Baltimore, MD 21235 Phone E-mail: Fax:</p>

Department of Veterans Affairs	Department of Veterans Affairs
Gerald M. Cross, MD, SAAFP	Will A. Gunn
Acting Under Secretary for Health	General Counsel
Veterans Health Administration	Office of General Counsel
810 Vermont Avenue, NW	810 Vermont Avenue, NW
Washington, DC 20420	Washington, DC 20420
Phone: (202) 461-7008	Phone: (202) 461-4995
Email: Gerald.m.cross@va.gov	Email: will.gunn@va.gov
Fax: (202) 273-5787	Fax: (202) 273-6671

Attachment 5 – Applicable HIPAA provisions for Participants that are neither Covered Entities, Business Associates nor Governmental Participants

Pursuant to Section 16.01(d), the following HIPAA provisions are applicable to Participants that are neither Covered Entities, Business Associates nor Governmental Participants as if they were acting in the capacity of a Covered Entity. Definitions contained in the various provisions of 45 C.F.R. Parts 160 through 164 apply to the provisions listed in this Attachment 1 to the extent they are used in said sections.

- 45 C.F.R. § 164.306 (Security Rule – General rules) *[This is not required of BAs by the HITECH Act, but it nevertheless appears to be appropriate to include here, e.g., “Covered entities must ... Ensure the confidentiality, integrity, and availability of all electronic [PHI] the covered entity creates, receives, maintains, or transmits.”]*
- 45 C.F.R. § 164.308 (Security Rule – Administrative Safeguards)
- 45 C.F.R. § 164.310 (Security Rule – Physical Safeguards)
- 45 C.F.R. § 164.312 (Security Rule – Technical Safeguards)
- 45 C.F.R. § 164.314 (Security Rule – Organizational requirements)
- 45 C.F.R. § 164.316 (Security Rule – Policies and procedures and documentation requirements)
- 45 C.F.R. § 164.502, other than paragraphs (h), and (i) (Privacy Rule – Uses and disclosures of PHI: general rules) *[see notes below for descriptions of excluded subsections]*
- 45 C.F.R. § 164.504 (Privacy Rule – Uses and disclosures: Organizational requirements)
- 45 C.F.R. § 164.506 (Privacy Rule – Uses and disclosures to carry out treatment, payment, or health care operations)
- 45 C.F.R. § 164.508 (Privacy Rule – Uses and disclosures for which an authorization is required)
- 45 C.F.R. § 164.510 (Privacy Rule – Uses and disclosures requiring an opportunity to agree or to object)
- 45 C.F.R. § 164.512 (Privacy Rule – Uses and disclosures for which an authorization or opportunity to agree or object is not required)
- 45 C.F.R. § 164.514 (Privacy Rule – Other requirements relating to uses and disclosures of PHI)
- 45 C.F.R. § 164.520 (Privacy Rule – Notice of privacy practices for PHI)
- 45 C.F.R. § 164.522 (Privacy Rule – Rights to request privacy protection for PHI)
- 45 C.F.R. § 164.524 (Privacy Rule – Access of individuals to PHI)
- 45 C.F.R. § 164.528 (Privacy Rule – Accounting of disclosures of PHI)
- The following provisions of 45 C.F.R. § 160.530, but only to the extent that they relate to the above provisions. For example, with respect to 45 C.F.R. § 164.530(b), the Participant must

provide training with respect to the above provisions, such as § 164.506, but not with respect to other provisions of the HIPAA Regulations, such as § 164.522.

- 45 C.F.R. § 164.530(b) (Privacy Rule – Administrative Requirements, Training)
- 45 C.F.R. § 164.530(c) (Privacy Rule – Administrative Requirements, Safeguards)
- 45 C.F.R. § 164.530(d) (Privacy Rule – Administrative Requirements, Complaints to the Covered Entity)
- 45 C.F.R. § 164.530(e) (Privacy Rule – Administrative Requirements, Sanctions)
- 45 C.F.R. § 164.530(f) (Privacy Rule – Administrative Requirements, Mitigation)
- 45 C.F.R. § 164.530(g) (Privacy Rule – Administrative Requirements, Refraining from intimidating or retaliatory acts)
- 45 C.F.R. § 164.530(h) (Privacy Rule – Administrative Requirements, Waiver of rights)
- 45 C.F.R. § 164.530(i) (Privacy Rule – Administrative Requirements, Policies and procedures)
- 45 C.F.R. § 164.530(j) (Privacy Rule – Administrative Requirements, Documentation)

Notes:

The following requirements have not been included:

- 45 C.F.R. § 164.302 (Security Rule – Applicability)
- 45 C.F.R. § 164.304 (Security Rule – Definitions)
- 45 C.F.R. § 164.500 (Privacy Rule – Applicability)
- 45 C.F.R. § 164.501 (Privacy Rule – Definitions)
- 45 C.F.R. § 164.502(h) (Confidential communications), and (i) (Uses and disclosures consistent with notice)
- 45 C.F.R. § 164.526 (Privacy Rule – Amendment of PHI)
- 45 C.F.R. § 164.530(a) (Privacy Rule – Administrative Requirements, Personnel designations)
- 45 C.F.R. § 164.530(k) (Privacy Rule – Administrative Requirements, Group health plans)
- 45 C.F.R. § 164.532 (Privacy Rule – Transition provisions)

Attachment 6 - Dispute Resolution Process

- When a Dispute arises, a Participant will send written notice, in accordance with the notice provision in the DURSA, to the other Participant(s) involved in the Dispute. The notice must contain a summary of the issue as well as a recommendation for resolution. The Participant must send a copy of the notice to the Dispute Resolution Subcommittee (see below) for informational purposes.
- Within thirty (30) calendar days of receiving the notice, the Participants are obligated to meet and confer with each other, at least once in good faith and at a mutually agreeable location (or by telephone), to try to reach resolution (the "Informal Conference"). If the Participants reach a resolution at the Informal Conference, they will provide notification to that effect to the Dispute Resolution Committee.
- If the Participants are unable to participate in an Informal Conference during the thirty (30) day period or to reach resolution at the Informal Conference, they have ten (10) business days following the end of the thirty (30) day period or the Informal Conference, respectively, in which to escalate the Dispute to the Dispute Resolution Committee in writing.
 - The Dispute Resolution Subcommittee (the "Subcommittee") will be a five (5) member standing subcommittee of the NHIN Coordinating Committee. The NHIN Coordinating Committee will appoint each member of the Subcommittee for a definite term. The members must be representative of the Participants, have diverse skill sets, and be able to help facilitate and reach resolution on conflicts between the Participants. The Subcommittee must have access to legal counsel to advise it on the law relevant to matters before it.
 - In addition to appointing the five (5) members of the Subcommittee, the NHIN Coordinating Committee must also appoint three (3) to five (5) alternates for the Subcommittee. Alternates will serve on the Subcommittee should any of the members have a conflict on a particular Dispute or in the event that member(s) are unavailable. Subcommittee members are required to declare any conflicts in accordance with the NHIN Coordinating Committee's conflict of interest policy. Once a Subcommittee member declares a conflict, the remaining Subcommittee members will decide amongst themselves whether such member must withdraw from the Subcommittee for the dispute in question.
 - The Subcommittee must also have access to panels of subject matter experts, as identified by the NHIN Coordinating Committee, for a variety of topics that may be implicated by a Dispute. Each subject matter expert panel must have at least three (3) experts on it who will rotate as advisors to the Subcommittee.
- Once a Participant escalates a Dispute to the Subcommittee, the Subcommittee will have thirty (30) calendar days in which to convene a meeting of the involved Participants ("Committee Meeting"). During this meeting, each Participant will be able to present its version of the Dispute and any information that it believes is pertinent to the Subcommittee's decision.

- The Subcommittee will have the ability to request additional information from the Participants to help it make its determination. The Subcommittee, however, will not have the authority to compel a response or the production of testimony or documents by the Participants. To the extent that the Participants do respond to requests of the Subcommittee by producing documents, Participants will have the ability to mark the documents produced as “Confidential Participant Information” and the Subcommittee will treat those documents in accordance with Section 18 of the DURSA.
- The Subcommittee is encouraged to develop an appropriate and equitable resolution of each submitted Dispute, considering all available evidence, the goals of the NHIN and other relevant considerations. The Subcommittee must also have the authority to recommend sanctions for the breaching Participant. These sanctions include developing corrective action plans, suspension of participation rights, and termination of participation rights. The type of sanction will depend on the nature and severity of the breach.
- Within fifteen (15) calendar days of the Subcommittee Meeting, the Subcommittee will issue a written recommendation for resolution, including an explanation of the basis and rationale of its recommendation. If either Participant is dissatisfied with the Subcommittee’s recommendation for resolution, it will have five (5) business days in which to escalate the Dispute to the NHIN Coordinating Committee.
- Within twenty (20) calendar days of receiving notice of escalation from a Participant, the NHIN Coordinating Committee will review the Subcommittee’s recommendation along with the information on which such recommendation was based and issue a final resolution. The NHIN Coordinating Committee may seek additional information from the Participants to aid its resolution of the Dispute.
- Within seven (7) calendar days of receiving the final resolution from the NHIN Coordinating Committee, the Participants will determine whether to accept or reject the resolution and so notify the NHIN Coordinating Committee.
- The NHIN Coordinating Committee will send a written summary of the resolution of the Dispute to all NHIN Participants. The summary will not identify the Participants involved, but will contain sufficient detail about the resolution to serve as an instructive resource for other Participants.
- In no case shall a Participant be required to disclose PHI in violation of Applicable Law as part of its participation in the Dispute Resolution Process. The decision to not disclose PHI shall not be held against a Participant in the Dispute Resolution Process.

Attachment 7 – Joinder Agreement

THIS JOINDER AGREEMENT (this "Joinder"), made as of January 29, 2010, by and between NHIN CC (the "NHIN Coordinating Committee") and DoD (the "New Participant") makes New Participant a party to that certain Data Use and Reciprocal Support Agreement dated 11/18/09 among the participants in the Nationwide Health Information Network ("NHIN"), as amended through the date hereof (the "DURSA").

RECITALS:

- A. The New Participant desires to become a participant in the NHIN.
- B. The NHIN Coordinating Committee has accepted and approved the New Participant's application to participate in the NHIN, with the condition precedent that the New Participant executes this Joinder.

AGREEMENT:

NOW, THEREFORE, in consideration of good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the undersigned hereby agree as follows:

1. **JOINDER.** The New Participant is hereby made a party to the DURSA, and agrees to be bound by, and shall comply with, the terms thereof. From the date hereof, the New Participant shall be a "Participant" as that term is defined in the DURSA and shall be subject to all of the duties and obligations and entitled to the rights and benefits of a "Participant" as provided therein.

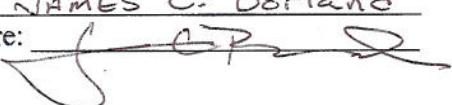
2. **ACKNOWLEDGEMENT.** The New Participant hereby acknowledges that it has received and reviewed a copy of the DURSA.

4. **REAFFIRMATION.** The terms and provisions of the DURSA remain in full force and effect in all respects.

5. **COUNTERPARTS.** This Joinder may be executed in any number of counterparts, each of which will be an original, but all of which taken together will constitute one and the same instrument.

IN WITNESS WHEREOF, the undersigned have caused this Joinder to be executed, all as of the day and year first written above.

NHIN COORDINATING COMMITTEE

By: Chair
Name: JAMES C. Borland
Signature: 

NEW PARTICIPANT

By: Deputy Secretary of Defense
Name: William J. Lynn
Signature: 

JAN 28 2010



General Information

- Added by [Linda Toscano](#), last edited by [Linda Toscano](#) on Jul 09, 2011 ([view change](#))
[Go to start of metadata](#)

view	7407241
----------------------	---------

To gain knowledge about the Nationwide Health Information Network, the Exchange, and general Onboarding requirements, refer to the sections below.

- [**What is the Nationwide Health Information Network?**](#)
- [**What is the Nationwide Health Information Network Exchange?**](#)
- [**What are the benefits to joining the Exchange?**](#)
- [**Who currently participates in the Exchange?**](#)
- [**Who can join the Exchange?**](#)
- [**What are the gateway requirements?**](#)

What is the Nationwide Health Information Network?

The Nationwide Health Information Network is a set of policies, standards, and services that enable Participants to use the Internet for secure and meaningful exchange of health information to improve health and health care. For more information, go to

http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov_nationwide_health_information_network/1142.

[Back to Top](#)

What is the Nationwide Health Information Network Exchange?

The Nationwide Health Information Network Exchange is a confederation of trusted entities, bound by a mission and a common framework of trust, to securely exchange health information using Nationwide Health Information Network standards and specifications. It is a diverse set of entities facilitating information exchange with a broad set of users, systems, geography, or community:

- Internet-based, using common implementation of standards and specifications with secure transport
- Tested for conformance and interoperability
- Enables valid, trusted entities to participate
- Signed trust agreement that allocates responsibilities and accountability to protect information exchanged
- Digital credentials issued to permit only approved Participants to exchange data with other members
- Committee structures to oversee and support activities

For more information about the Exchange, go to

http://healthit.hhs.gov/portal/server.pt?open=512&objID=1407&parentname=CommunityPage&parentid=8&mode=2&in_hi_userid=11113&cached=true.

[Back to Top](#)

What are the benefits to joining the Exchange?

- Locate and verify consumers of health care services within organizations and accurately link to their records.
- Find and retrieve health care information within and between health information exchanges and other organizations.
- Deliver a summarized patient record to support patient care and to support the patient's health.
- Support consumer preferences regarding the exchange of his or her information, including the ability to choose not to participate in the Exchange.
- Link to a secure information exchange.
- Join a common trust agreement that establishes the obligations and assurances to which all Exchange Participants agree.
- Match patients to their data without a national patient identifier.
- Use harmonized standards for the exchange of health information across entities and networks.

[Back to Top](#)

Who currently participates in the Exchange?

- Centers for Disease Control and Prevention (CDC)
- Department of Defense (DoD)
- Department of Veterans Affairs (VA)
- Douglas County Independent Physicians Association (DCIPA)
- E H R Doctors, Inc.
- HealthBridge
- Inland Northwest Health Services (INHS)
- Kaiser Permanente
- MedVirginia
- North Carolina Healthcare Information and Communication Alliance (NCHICA)
- Oregon Community Health Information Network (OCHIN)
- Regenstrief Institute
- Social Security Administration (SSA)

[Back to Top](#)

Who can join the Exchange?

- A federal agency, state agency, Health Information Exchange, or Integrated Delivery System
- A valid legal entity, either public or private, that is a contractor, grantee or party to a cooperative agreement with a federal government agency that addresses participation in the transaction of Message Content among Participants
- An organization or agency that oversees and conducts, on its own behalf and/or on behalf of its Participant Users, electronic transactions or exchanges of health information among groups of persons or organizations
- The agency, entity, or organization must meet the following:
 - Technical ability to meet the Performance and Service Specifications to electronically transact health information on its own behalf or on behalf of its Participant Users
 - Organizational infrastructure and legal authority (through statutes, regulations, organizational agreements, contracts or binding policies) to comply with the obligations in the Data Use and Reciprocal Support Agreement (DURSA)

(http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11673_910759_0_0_18/DURSA_2009_Version_for_Production_Pilots_20091118.pdf) and to require its Participant Users to comply with applicable requirements of the DURSA Intent to transact information with other Participants for a permitted purpose Sufficient financial, technical, and operational resources to support the testing and operation of transactions among Participants Ability to submit a completed Application for Participation (for specific information, refer to http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11113_911030_0_0_18/NHINCC_1_ReviewandDispositionofAppsforParticipationandDefinitivePlans_Approved_20100218.pdf) Federal Contract requirement:

- Organization must be performing activities that come under a federal contract, grant, or cooperative agreement that includes Nationwide Health Information Network Exchange as part of its scope, either as a direct contractor or indirectly as a Participant in the contracted activities, or
- Organization must indicate it is performing health information exchange under the scope of the State Health Information Exchange's (HIE's) activities.

[Back to Top](#)

What are the gateway requirements?

Applicants can use any compliant instantiation of specifications and services as their gateway for the Exchange. Applicants have the option to either implement their own gateway or implement the CONNECT gateway, an open-source software solution for health information exchange using nationally-recognized interoperability standards.

Applicants may select either Option 1 or Option 2:

Option 1: If Applicants have an existing gateway or choose to implement their own gateway, they need to ensure that it meets the Nationwide Health Information Network final production specifications. Applicants can access the Nationwide Health Information Network specifications and use cases from [Specifications and Use Cases](#).

Option 2: If Applicants choose to implement CONNECT, they can access the CONNECT Web site and download the document, *Using the CONNECT Gateway to Support HIE*. Go to www.connectopensource.org > Product > select the latest CONNECT release > download the latest version of this document.

[Back to Top](#)

Labels parameters	<input type="text" value="http://jira.siframe"/>	<input type="text" value="12386454"/>	<input type="text" value="OBTI"/>
Labels:			
None			



Specifications and Use Cases

- Added by [Linda Toscano](#), last edited by [Linda Toscano](#) on Jul 07, 2011 ([view change](#))
[Go to start of metadata](#)

view	7407241
----------------------	---------

Nationwide Health Information Network Specifications and Use Cases

The Nationwide Health Information Network Web Service Interface specifications define the core set of standard services to be implemented by each node on the network in order to exchange interoperable health information over the Internet. These functional services provide discovery and information exchange capabilities and rest upon a foundational set of messaging, security, and privacy services.

For up-to-date specification information, refer to the Exchange Specification Web site at <http://exchange-specifications.wikispaces.com/>.

The following sections provide listings and links to the Final Production Specifications, the Emergence Pilot Specifications, and the Use Case Requirements and Specifications.

Final Production Specifications

Specification Title and Version
Access Consent Policies Production Specification
Authorization Framework Production Specification
Query for Documents Production Specification
Retrieve Documents Production Specification
Health Information Event Messaging Production Specification
Messaging Platform Production Specification
Patient Discovery Production Specification
Web Services Registry Production Specification

Emergency Pilot Specifications

Specification Title and Version
Continuity Assessment Record and Evaluation (CARE) Emergency Pilot Profile Specification
Document Submission Emergency Pilot Specification
Geocoded Interoperable Population Summary Exchange (GIPSE) Profile Definition
Administrative Distribution Emergency Pilot Specification
Physician Quality Reporting Initiative (PQRI) Emergency Pilot Profile Definition
NHIN Medicaid Eligibility Verification Emergency Pilot Specification

Use Case Requirements and Specifications

Use Case Requirements and Specifications
Authorized Release of Information to a trusted entity Use Case Narrative
Biosurveillance Use Case
Consumer Preference Registration Med History Requirements
EHR Lab Scenarios Use Case Requirements
Emergency Responder Use Case Requirements
Quality Use Case Requirements
Quality Use Case Requirements 2
Quality Use Case Requirements 3
Quality Use Case Requirements 4
Authorized Case Follow Up
Medication Management

Labels parameters

<http://jira.siframe.com>

6685087

OBTI

Labels:

None

Are you sure you

Click to toggle the

Cancel



Onboarding Overview

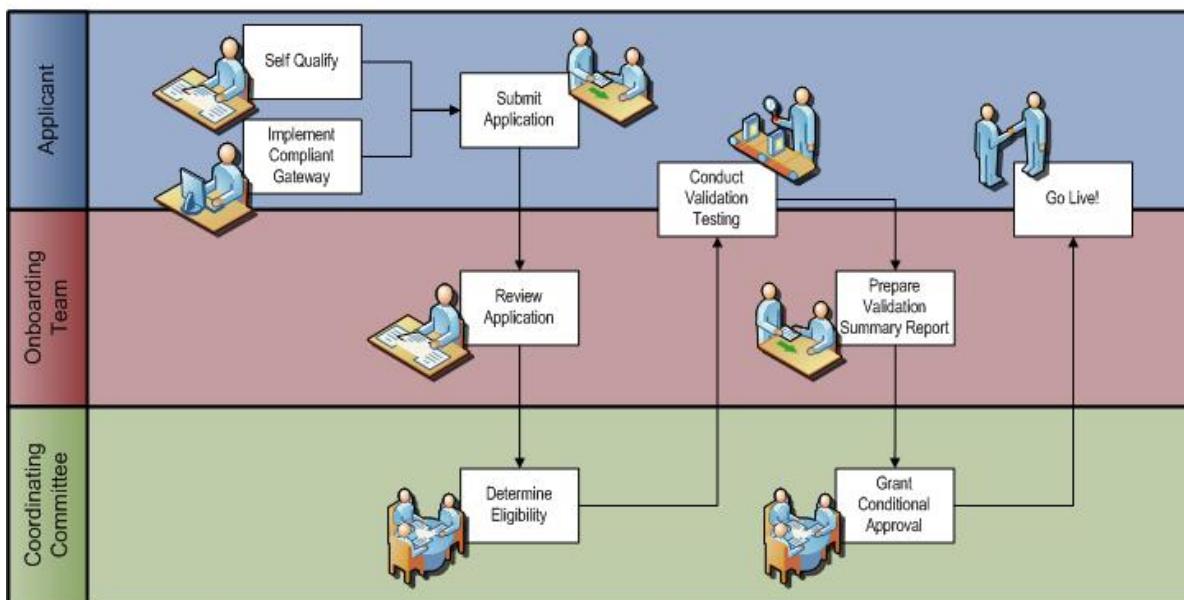
- Attachments:1
- Added by Linda Toscano, last edited by Linda Toscano on May 11, 2011 (view change)
[Go to start of metadata](#)

[view](#)

7407241

Onboarding is a self-guided process for Applicants to join the Exchange. The Exchange is designed for Applicants wishing to exchange health information with federal agencies and large nationwide entities requiring a high level of trust and the ability to engage in multi-point health information exchanges.

Onboarding Process Overview



Onboarding Stages

The following table provides an overview of the Onboarding Stages.

Qualification	<ul style="list-style-type: none">Applicant requests an Application Packet from the Onboarding TeamApplicant submits completed Application Packet to the Onboarding TeamOnboarding Team reviews Application Packet for completenessOnboarding Team forwards Application Packet to the Nationwide Health Information Network Coordinating Committee (CC)CC reviews Application Packet and makes eligibility determination
Validation	<ul style="list-style-type: none">Onboarding Team sends test certificate and validation framework information to ApplicantApplicant configures its test environment and conducts Conformance and Interoperability testingOnboarding Team collects testing logs and conducts analysis for Conformance and

	<p>Interoperability testing</p> <ul style="list-style-type: none"> Onboarding Team prepares Validation Summary Report and submits to CC If required, Applicant submits remediation plan to Onboarding Team for CC review
Activation	<ul style="list-style-type: none"> CC evaluates Validation Summary Report and remediation plan, if applicable, and determines whether to grant conditional approval for the Applicant to attain Participant status on the production Exchange CC notifies the Onboarding Team and the Applicant of Participant status Onboarding Team sends Activation Packet to Applicant Applicant returns Activation Packet to Onboarding Team Onboarding Team configures the Nationwide Health Information Network registry with Applicant's information and issues a production cert to the Applicant CC executes the DURSA Joinder Applicant is now a Participant and ready to exchange data over the Nationwide Health Information Network Exchange

Next Step

To guide the Applicant through the complete Onboarding process, the Onboarding Team has established a Road Map which provides an outline of the processes and decisions occurring during the Onboarding journey. To continue learning about Onboarding, access the [Onboarding Process - Applicant Steps](#).

Labels parameters	http://jira.siframe	5604064	OBTI
Labels:	None		
<input type="button" value="Are you sure you"/> <input type="button" value="Click to toggle the"/> <input type="button" value="Cancel"/>			



Onboarding Process - Applicant Steps

- Added by [Linda Toscano](#), last edited by [Linda Toscano](#) on May 11, 2011 ([view change](#))

[Go to start of metadata](#)

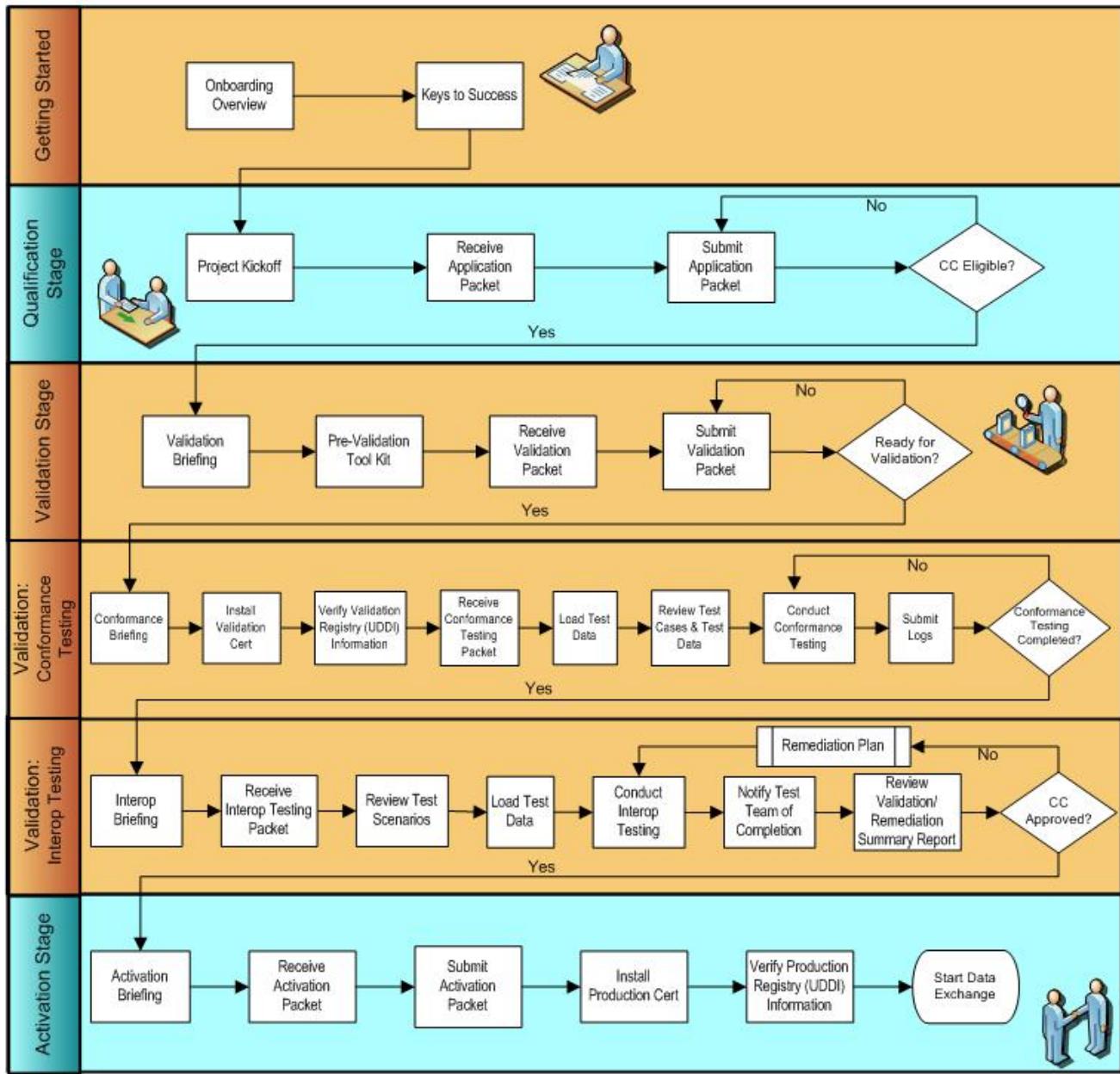
[view](#)

7407241

Onboarding Process - Applicant Steps

To guide the Applicant through the Onboarding process, the Exchange Onboarding Team has established an Onboarding Process Flow. The diagram below provides an outline of the processes and decisions occurring during the Applicant's Onboarding journey. The Team strongly advises the Applicant to move through the steps in the suggested order, completing each process before continuing with the next one.

Onboarding Process Flow – Applicant



Next Step

When the Applicant is ready to continue, go to the **Qualification Stage**.

Labels parameters

Labels:

None



Qualification Stage

Added by Judith Hutman, last edited by Linda Toscano on May 11, 2011 ([view change](#))

[Go to start of metadata](#)

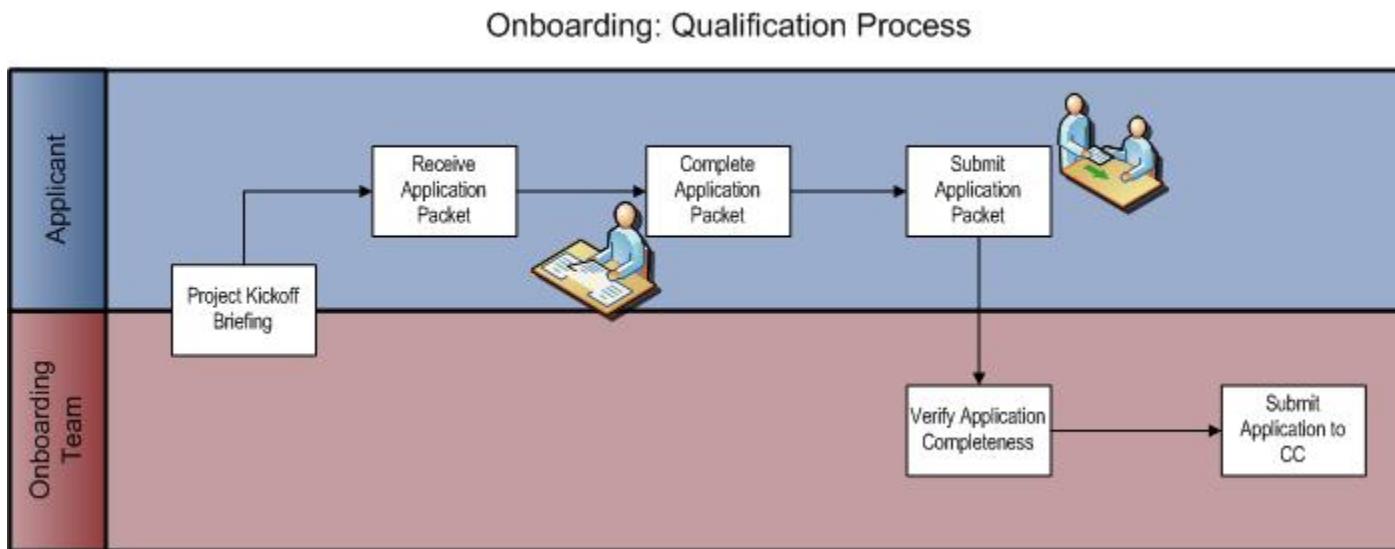
[view](#)

7407241

Qualification Stage

Early in the Qualification Stage, the Applicant conducts a pre-qualification assessment. During the assessment, the Applicant reviews eligibility criteria to ensure it can meet standards, services, and policies to securely exchange health information over the Internet with its Exchange-compliant gateway. Then, the Applicant requests an Application Packet from the Exchange Onboarding Team. Following completion and submission of the Application Packet, the Coordinating Committee (CC) makes an eligibility determination and notifies the Applicant and the Onboarding Team of same.

Qualification Stage Workflow



Qualification Stage Process

1. Onboarding Team conducts the Project Kickoff Briefing with the Applicant.
2. Applicant receives the Application Packet. The packet includes:
 - a. Application Packet Checklist (guides the Applicant through the review and completion of necessary documentation)
 - b. Application for Participation
 - c. Links to Data Use and Reciprocal Service Agreement (DURSA) files
3. Using the Application Checklist as a guide, the Applicant completes the Application forms:

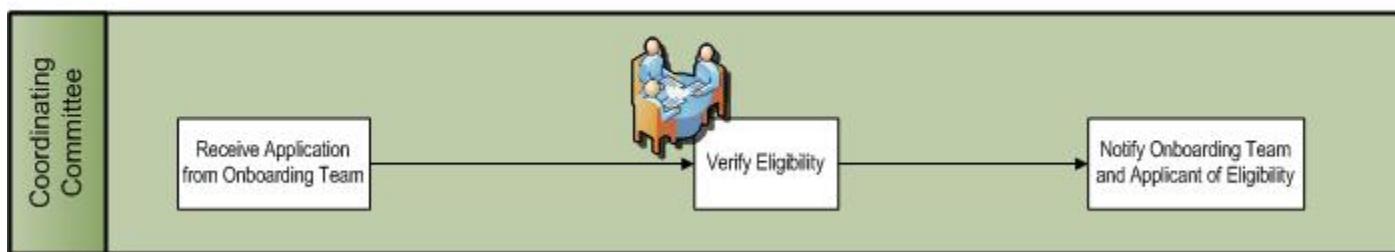
- a. Signed Application
 - b. Signed DURSA
4. Applicant submits the Application Packet with the completed forms.
 5. Onboarding Team receives the Application Packet and reviews for completeness.
 6. Onboarding Team submits the Application Packet to the CC for an eligibility determination. The CC meets once a month and agenda items must be submitted at least two weeks prior to the meeting.

Coordinating Committee Review

The CC reviews all the components of the Applicant's Application Packet. The CC verifies the Applicant's eligibility to join the Exchange and gives the go-ahead for the Applicant to proceed with the Validation Stage.

CC Workflow

Onboarding: Exchange Trust Framework Process - Eligibility



CC Process

1. Following receipt of the Application Packet from the Onboarding Team, the CC makes a determination of the Applicant's eligibility for Exchange participation at its next meeting. The CC meets once a month, requiring any agenda and review items two weeks in advance of each meeting.
2. CC reviews all components of the Applicant's Application Packet.
3. CC notifies the Onboarding Team and the Applicant of the Applicant's eligibility for participation and gives the go-ahead to proceed with Validation testing.

Next Step

After the Applicant completes the Qualification Stage process and receives eligibility notification from the CC, the Applicant proceeds to the [Validation Stage](#).

Labels parameters	<input type="text" value="http://jira.sifframe"/>	<input type="text" value="4194738"/>	<input type="text" value="OBTI"/>
Labels:			
None			
<input type="button" value="Are you sure you"/> <input type="button" value="Click to toggle the"/> <input type="button" value="Cancel"/>			



Validation Stage

Added by [Judith Hutman](#), last edited by [Linda Toscano](#) on Jul 06, 2011 ([view change](#))

[Go to start of metadata](#)

[view](#)

7407241

Validation Stage

The Validation Stage demonstrates that an Applicant's gateway complies with Nationwide Health Information Network Exchange specifications and verifies that each Applicant's gateway can interact with other Nationwide Health Information Network Participants. This page opens with an overview of the Validation process. Then, it identifies how Applicants move through Conformance Testing and Interoperability Testing.

To ensure an Applicant's gateway conforms to specifications and is capable of exchanging information with other Participants, the Test Team conducts validation testing with the Applicant. Validation testing focuses on two areas:

1. Conformance Testing – Ensures that a Gateway conforms to Nationwide Health Information Network specifications.
2. Interoperability Testing – Validates interoperability with other Exchange Participants across business scenarios.

Since conformance does not guarantee interoperability, Exchange functionality requires both elements.

Conformance Testing focuses on validating a particular version of a single gateway to a specific set of standards and specifications. Primarily, this testing confirms that a system correctly encodes the syntax and structure of a given data standard in the physical files or transactions that a system produces and receives.

Interoperability Testing seeks to validate that multiple gateways implementing a particular standard or set of standards can communicate with one another across a business scenario.

What Is Tested?

All Applicants must support a minimum set of services. In the Application Packet, the Applicant identifies which services it intends to support, including this minimum set of services. The Onboarding Team guides the Applicant through the testing process for the specifications relevant to the services identified, and coordinates testing with the Applicant and the Test Team.

Re-validating

If an Exchange Participant makes a material change to their gateway or services, they must pass through the Validation process again.

The following occurrences trigger the re-validation process:

- When the Participant upgrades or modifies the gateway software
- When the Participant upgrades the specification version it supports
- When the Participant elects to support a new specification

System Readiness

The gateway to be tested should be production ready, having undergone thorough integration testing before coming to Validation. The tested system is not solely a Nationwide Health Information Network gateway; the Applicant must test the system that generates, transmits, and/or receives the Nationwide Health Information Network transmitted messages.

Preparing for Testing

To prepare for testing, the Onboarding Team provides Applicants with the following materials:

- One or more test guides for the specification(s) the Applicant elects to support
- Test cases and data
- A digital certificate which the Applicant installs in its system's local keystore
- Community ID
- Entry into the test Universal Description Discovery Interface (UDDI) services registry

Prior to conducting testing, the Applicant reviews the Test Guide and other documents to ensure its system can perform the tests.

A testing preparation checklist for the Applicant follows.

- Load test data into the system. (Depending on the system and the tests, this process can take from several hours to several days).
- As needed for the setup requirements, configure certain access permissions for individual tests.
- Load the digital certificate into the system's local keystore.
- Register its Community ID for use by its gateway.
- Ensure the system has an IP address and is accessible through the Internet.
- Ensure the system's Web service is operational.

Conducting Testing

Following the Test Guide, the document defining the particular process and artifacts required for evidence, the Applicant conducts Conformance and Interoperability Testing. When testing is complete, the Test Team collects the testing logs and conducts an analysis of the log data.

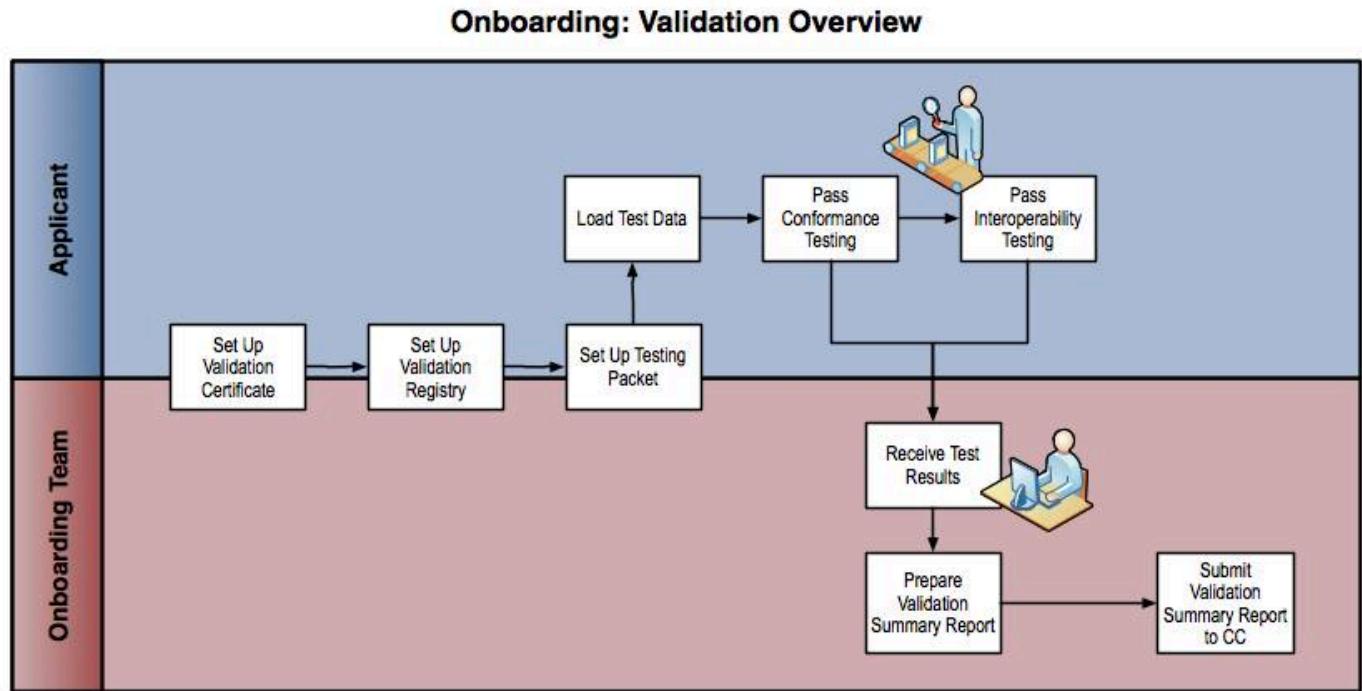
Validating Test Results

The Test Team reviews the Test Logs from both Conformance and Interoperability testing. The Team forwards Conformance Testing logs to National Institute of Standards and Technology (NIST) for analysis. The Test Team analyzes the Interoperability Test Logs. The Team captures the analyses in the

Validation Summary Report for Nationwide Health Information Network Coordinating Committee (CC) review.

Refer to the following Validation process workflow for a high-level overview of the Validation processes. The sections following the workflow provide the specific process details.

Validation Overview Workflow



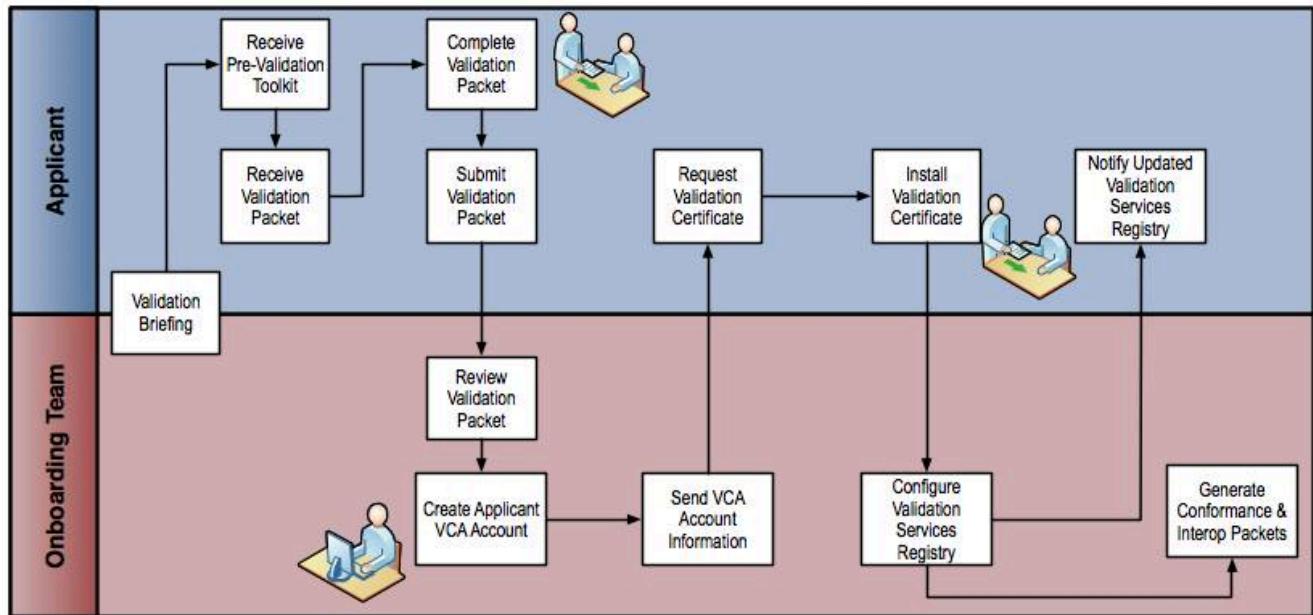
Validation Process

Validation Prep

The Onboarding Team works closely with the Applicant to complete the Validation set-up steps. This process starts with CC notifying the Applicant they are eligible for Participation and ends with the Applicant loading the Validation test data. Applicants load test data sets for both Conformance and Interoperability Testing.

Workflow

Onboarding: Validation Process - Setup



Process

1. Onboarding Team conducts the Validation Briefing with the Applicant.
2. Applicant reviews the **Pre-Validation Testing Tool Kit**. The kit includes:
 - a. Conducting Gateway-to-Gateway Exchanges before Entering Validation
 - b. Ensuring Correct Configuration of Certificates
 - c. Confirming Correct CONNECT Configuration
 - d. Ensuring Services Registry Entry is Correct
 - e. Ensuring Correct Formatting of Message Codes
 - f. Using the NIST Tools to Review Messages for Conformance
 - g. Avoiding Common Authorization Framework Conformance Errors
3. Applicant receives the Validation Packet. The packet includes:
 - a. Validation Packet Checklist
 - b. Onboarding Validation Overview
 - c. Certificates Guide for Organizations
 - d. Validation Certificate Authority Form (VCAF)
 - e. Validation Services Registry Form (VSRF)
 - f. Patient Discovery (PD) Query for Documents (QD) Parameter Questionnaire
 - g. Installation Conformance Questionnaire
 - h. Pre-validation Test Patient Information
4. Using the Validation Packet Checklist as a guide, the Applicant completes the validation forms and questionnaires:
 - a. VCAF
 - b. VSRF
 - c. PD QD Parameter Questionnaire
 - d. Installation Conformance Questionnaire

5. Applicant submits the Validation Packet with the completed forms.
6. Onboarding Team receives the Validation Packet and reviews for completeness.
7. Onboarding Team logs into the Validation Certificate Authority (VCA) NFI Test Administration and creates an account for the Applicant.
8. Onboarding Team sends two emails to the Applicant:
 - a. First email provides the VCA URL log on information, instructions, and Reference Number.
 - b. Second email provides the VCA Authorization Code.
9. Applicant receives the emails, logs into the VCA account, and requests a digital certificate.
10. Applicant receives the digital certificate from VCA.
11. Applicant installs the validation certificate on the validation host server.
12. Onboarding Team configures the Validation Services Registry (Validation Universal Description Discovery Interface (UDDI)) with the Applicant's VSRF information.
13. Onboarding Team notifies the Applicant it has updated the Validation Services Registry.
14. Onboarding Team forwards the questionnaires to the Test Team.
15. Test Team uses the questionnaire responses to generate the Applicant's Conformance and Interop Packets.

Conformance Testing

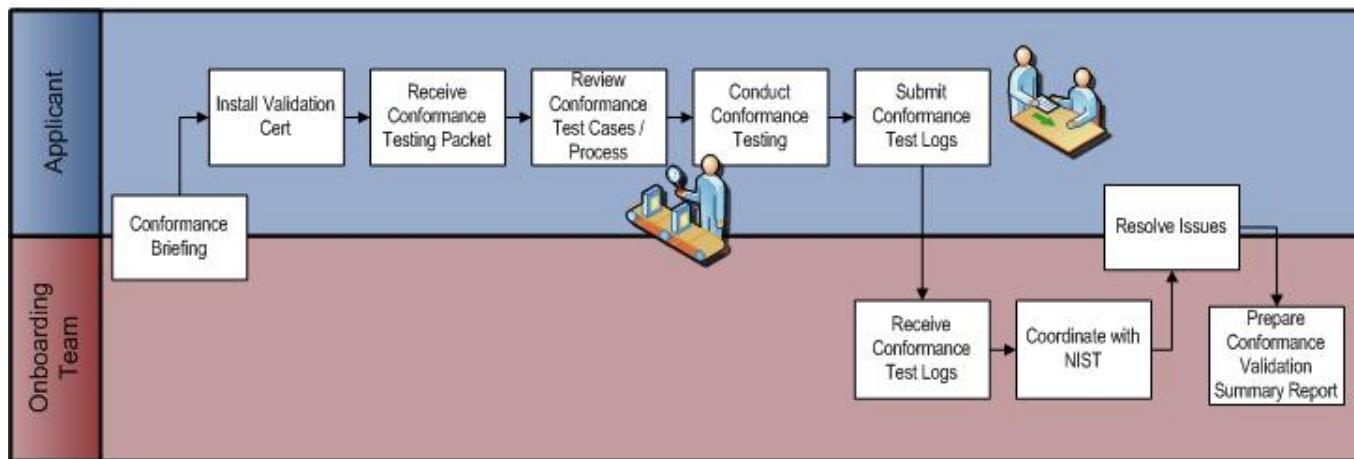
Following validation setup, the Applicant is ready to start Conformance Testing. There are two types of Conformance Testing:

1. Full, or Product, Conformance Testing
2. Installation Conformance Testing

The Nationwide Health Information Network has a full suite of conformance tests for each specification. If an Applicant is using a gateway that has already been validated for conformance, the Onboarding Team permits the Applicant to conduct a smaller subset of conformance test cases (Installation Conformance Testing). If an Applicant has a gateway that has not gone through conformance validation, the Applicant needs to run through all of the tests (Full, or Product Conformance Testing).

After the Applicant completes Conformance Testing, it sends the test artifacts (logs) to the Test Team for analysis.

Onboarding: Validation Process - Conformance Testing



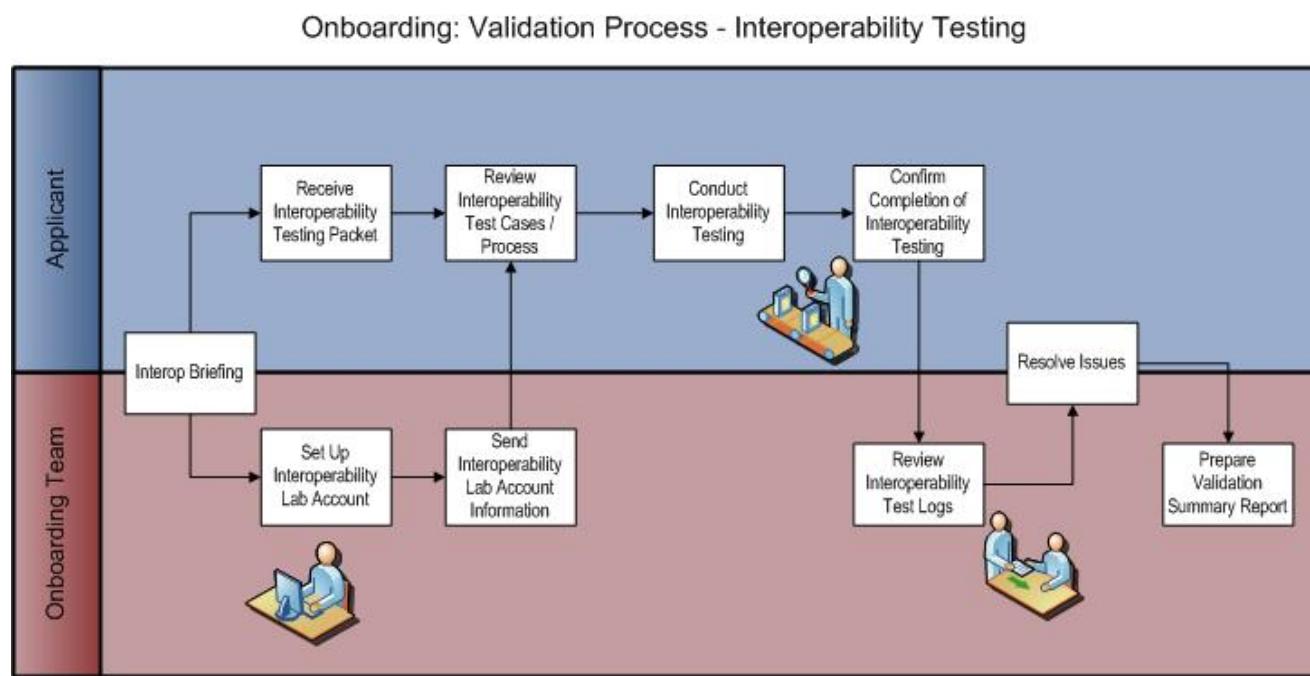
Process

1. Onboarding Team conducts the Conformance Briefing with the Applicant to kickoff Conformance Testing.
2. Applicant installs the Validation Certificate.
3. Applicant verifies the Validation Registry (UDDI) information.
4. Applicant receives the Conformance Testing Packet. The packet includes:
 - a. Conformance Checklist
 - b. Test Guide
 - c. Test Report
 - d. Initial Connectivity Test Quick Guide
 - e. Test Cases
 - f. Test Patient Inventory
 - g. Test Patient Data
5. Applicant reviews the Conformance Testing process and test cases, and loads the test data.
6. Test Team schedules and conducts Connectivity Testing (to confirm both gateways are talking to each other) with the Applicant.
7. Test Team analyzes the results of connectivity testing for conformance to give the Applicant a preview of any issues it may expect to uncover in Conformance Testing.
8. Test Team schedules and conducts Conformance Testing with the Applicant.
9. Applicant submits the conformance test artifacts (logs and test report) to the Test Team.
10. Test Team receives the Test Logs.
11. Test Team coordinates with NIST to complete the analysis.
12. Test Team schedules and holds a review with the Applicant to notify the Applicant of any issues noted during the analysis.
13. As needed, the Applicant fixes any issues raised during Conformance Testing or analysis and submits evidence of the fix (may require redoing some test cases).
14. Test Team prepares the Conformance Testing section of the Validation Summary Report for Coordinating Committee review.

Interoperability Testing

After the Applicant submits the Conformance Testing logs and while the Applicant is waiting for the NIST analysis, the Onboarding Team sends the Interoperability Packet to the Applicant, sets up an Interoperability lab account and then, sends the lab account information to the Applicant. When the Applicant completes Interoperability Testing, it simply clicks a button to indicate completion so the Onboarding Team can access the Interoperability Testing logs.

Workflow



Process

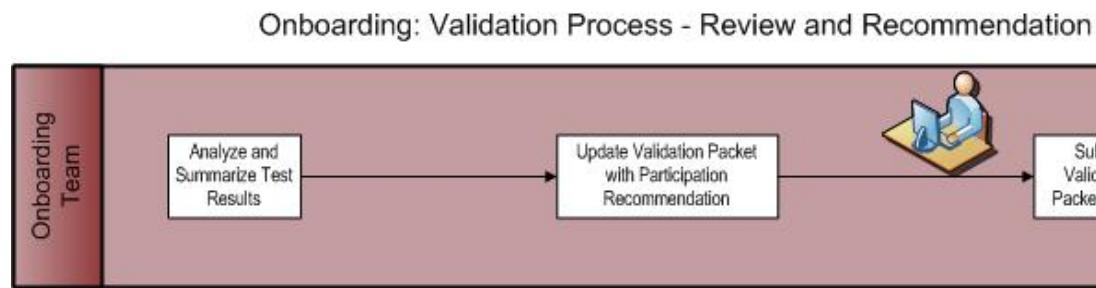
1. Onboarding Team conducts the Interop Briefing with the Applicant to kickoff Interoperability Testing.
2. Applicant receives Interoperability Testing Packet. The packet includes:
 - a. Interoperability Checklist
 - b. Interoperability Lab Registration Form
 - c. PD QD RD Interop Scenarios
 - d. Test Patient Data
3. Applicant returns Interoperability Lab Registration Form to the Onboarding Team.
4. Onboarding Team sets up the Applicant's account in the Interoperability Lab.
5. Onboarding Team sends URL, account information, and instructions to the Applicant.
6. Applicant reviews the Interoperability Testing packet and test cases, loads the test data, and configures its account in the Interoperability Lab.
7. Applicant conducts Interoperability Testing and submits its results in the Lab.
8. Applicant notifies the Onboarding Team when it has completed Interoperability Testing.

9. Test Team reviews the Applicant's interoperability test logs with the Applicant and notifies the Applicant of any issues observed in the log review.
10. As needed, the Applicant fixes any issues observed in the log review and submits evidence of the fix (may require redoing some test scenarios).
11. Test Team prepares the Interoperability Testing section of the Validation Summary Report for CC review and approval.

CC Review and Recommendation

This final segment of the validation phase consists of an analysis, summary, and participation recommendation on the Applicant's behalf from the Onboarding Team.

Workflow



Process

Onboarding Team submits the Validation Summary Report, consisting of Conformance and Interoperability Testing analysis, to the CC.

Note: When an Applicant completes the validation stage, Onboarding Team does not permit any further changes to the designated system or software code until after the Applicant receives notification of their Participant status from the CC. Material changes to the system require re-validation.

Next Step

After the Applicant completes the Validation Stage process, the Applicant proceeds to the [Activation Stage](#).

Labels parameters	http://jira.siframe	4194746	OBTI
Labels:			

None

1 Child Page

Page: [Pre-Validation Testing Tool Kit](#)



Pre-Validation Testing Tool Kit

- Added by [Azreen Rahman](#), last edited by [Linda Toscano](#) on May 11, 2011 ([view change](#))
[Go to start of metadata](#)

[view](#)

4194746

Keys to Success for Nationwide Health Information Network Validation Testing

The *Nationwide Health Information Network Pre-Validation Tool Kit* provides Applicants with the approach, processes, and requirements for readiness prior to entering Validation Testing.

In an effort to optimize and reduce the current length of time to successfully complete Validation Testing, the Nationwide Health Information Network Testing Team has identified the following items as "Keys to Success" in the Nationwide Health Information Network Validation Testing.

This Tool Kit assists the Applicant to better understand the specifications and prepares the Applicant to conduct Validation Testing more efficiently and effectively in advance.

Conducting these activities typically results in a smoother and faster path through Validation Testing.

For each "Keys to Success," click on "This section" to follow the link to the associated pages which describes the steps in further detail.

1. Conducting Gateway-to-Gateway Exchanges Before Entering Validation

- Gateway-to-Gateway Testing is an integral element in your gateway's Integration/System Testing. It is part of your internal development milestone prior to entering Nationwide Health Information Network Validation.
- This section** provides guidance and recommendations to ensure your gateway's implementation has the ability to connect and exchange messages with other Nationwide Health Information Network gateways.

2. Ensuring Correct Configuration of Certificates

- Correct installation of the Nationwide Health Information Network Validation and Production Certificates are the first steps to enabling information exchange.
- This section** provides a step-by-step guide on how to correctly install and verify installation of the Certificates.

3. Confirming Correct CONNECT Configuration

- CONNECT is an open source software solution that supports health information exchange, and uses the Nationwide Health Information Network standards and governance to ensure health information exchanges are compatible with other operating exchanges throughout the country.
- **This section** guides you through CONNECT's Test Tools to ensure correct installation and configuration of your system.

4. Ensuring Services Registry Entry is Correct

- ONC requires all Exchange participants to enter their connection information in the Exchange's Service Registry (UDDI). The testing tools use the UDDI to communicate with candidate systems. Before testing begins, ensure your UDDI entry is valid. If it is not, be sure to correct and confirm the entry before testing.
- **This section** guides you through the details of UDDI confirmation.

5. Ensuring Correct Formatting of Message Codes

- In Document Query messages, the specification defines how coded values are to be formatted. Ensure your system formats the codes correctly if it uses them when querying for documents, and that your system can handle the specified code formats when it receives document queries.
- **This section** guides you through the codes.

6. Using the NIST Tools to Review Messages for Conformance

- The National Institute of Standards and Technology (NIST) provides a public tool for validating that messages conform to the specifications for Query for Documents (QD) and Retrieve Document (RD) exchanges on the Nationwide Health Information Network.
- **This section** provides a guide on using NIST's Tools and how to interpret the results.

7. Avoiding Common Authorization Framework Conformance Errors

- During Validation testing, we find numerous message conformance errors related to the Authorization Framework specification, which form the access control backbone of the Exchange.
- **This section** helps you capture your SOAP messages and avoid the most common Authorization Framework (SAML) errors.

Labels parameters

<input type="text" value="http://jira.siframes"/>	<input type="text" value="4195427"/>	<input type="text" value="OBTI"/>
---	--------------------------------------	-----------------------------------

Labels:

None

[7 Child Pages](#)

[Reorder Pages](#)



Conducting Gateway-to-Gateway Testing Before

Entering Validation

view

4195427

Prior to Entering the Nationwide Health Information Network Validation Process

Many Nationwide Health Information Network candidates attempt to begin the Validation process without ever having tested their candidate gateway's ability to establish Certificate-Based communication with any other gateway, i.e. without conducting "Gateway-to-Gateway" Testing.

To date, the universally common experience of such Nationwide Health Information Network candidates is that they have a very challenging, lengthy, and at times frustrating path through the first handful of Conformance test cases.

- During the Validation process, a sizable percentage of these Nationwide Health Information Network candidates then discover significant defects in their gateway implementation which have impacted their own deployment and production schedules.
- In some cases, the resulting lengthy delays have risked Nationwide Health Information Network candidates in losing their place in the Validation "queue", having to restart Validation over again.

The Key to Success is to include Gateway-to-Gateway Testing as an integral element of a candidate gateway's Integration/System Testing, and as an internal development milestone well in advance of entering Nationwide Health Information Network Validation.

Gateway-to-Gateway testing is defined as standing up two distinct instances of a candidate gateway, and having them exchange Nationwide Health Information Network Specification-Based messages, such as Patient Discovery (PD) or Query for Documents (QD) across a secure network. This may involve implementing Self-Signed Certificates within an Organization's internal network, or configuring local Universal Description Discovery Interface (UDDI) entries for the candidate gateway, etc. It is in manipulating such elements of the testing environment that a Development Team gains valuable experience and insight into ensuring their gateway implementation actually has the ability to connect with and exchange messages with other Nationwide Health Information Network gateways.

Gateway-to-Gateway Testing is the best, most productive method for identifying and then troubleshooting and resolving the following types of defects which typically pose challenges to Nationwide Health Information Network gateway Development Teams:

- Incorrect/misconfigured Certificates
- Incorrect gateway configuration, such as
 - Errors with Assigning Authority ID
 - Errors with Home Community ID
 - Other problems introduced during gateway installation and initial gateway configuration

Incorrect UDDI configuration
SAML problems

While SOAPUI Testing or other standalone, single-gateway methods of testing do exercise certain functional elements of a candidate Nationwide Health Information Network gateway, these single-gateway methods of testing often do not uncover communications and integration related gateway issues. And those types of issues are often most costly, in terms of time and resources, to identify and resolve.

Planning on How to Address Issues Identified During the Nationwide Health Information Network Validation Process

A Key to Nationwide Health Information Network Validation Success

One important pitfall to avoid in managing a Nationwide Health Information Network gateway development effort, is viewing the start of the Validation process as the “finish line” of the development effort. While it is one of the final milestones on the Nationwide Health Information Network Onboarding path, to date, the experience of many seasoned Development Teams indicates that Conformance and Interoperability Testing typically uncover defects in Nationwide Health Information Network Candidate's gateway implementation which must be addressed prior to Onboarding.

From a proactive Project Management perspective, projects should recognize that Nationwide Health Information Network Validation's Conformance and Interoperability Testing is:

- An instance of Testing not too dissimilar from their own System and Integration Testing
- Likely to identify defects which must be resolved prior to Onboarding
- A phase in their development schedule which will likely be followed by an additional development or bug-fix release

...and plan accordingly.

From a Risk Management perspective, projects should consider adding the following risk to their risk register:

Risk: There is a risk that defects will be encountered during the Nationwide Health Information Network Validation process (in either Conformance or Interoperability Testing) which will require development resources to resolve prior to Nationwide Health Information Network Onboarding.

Suggested initial values for Risk Assessment:

- **Risk Probability:** High
- **Risk Impact:** Moderate-to-High

The fact that this risk presents itself very late in the development cycle tends to make its impact greater.

Risk Response & Planning:

- A successful mitigation strategy is to implement Gateway-to-Gateway testing throughout the development cycle.

- A successful acceptance strategy is to ensure that sufficient resources (both development budget and time) are provided in the development project plan and that project sponsors and stakeholders are well-informed of the risk.

Labels parameters

<http://jira.siframe>

7405887

OBTI

Labels:

None



Ensuring Correct Configuration of Certificates

- Added by [Leslie Power](#), last edited by [Azreen Rahman](#) on Jan 28, 2011 ([view change](#))
[Go to start of metadata](#)

view	4195427
----------------------	---------

One of the key features of the Nationwide Health Information Network Exchange is the Digital Security Certificates that underlie each exchange. Before an organization enters validation, it should ensure that the certificates are installed correctly. This page explains how to perform the certificate installation.

Obtain and Install Certificates

To obtain and install Validation Certificates, follow the directions indicated on the Onboarding **Validation Stage** page. This will also reference the Certificate Guide, Validation Certificate Authority Form, and Validation Services Registry Form.

In general, the key steps are:

- Generate the Certificate Signing Request (CSR)
- Submit the CSR
- Import the Web Server Certificate
- Install the Certificate Authority (CA) Certificate into the web server
- Install the CA Certificate into the web browser

You should have performed ***all*** of these steps prior to confirming successful installation and beginning Validation.

Confirm Successful Installation

A simple method to confirm that your Certificate is installed correctly is to call a (secured) web service through a web browser and view the Certificate through the web browser interface.

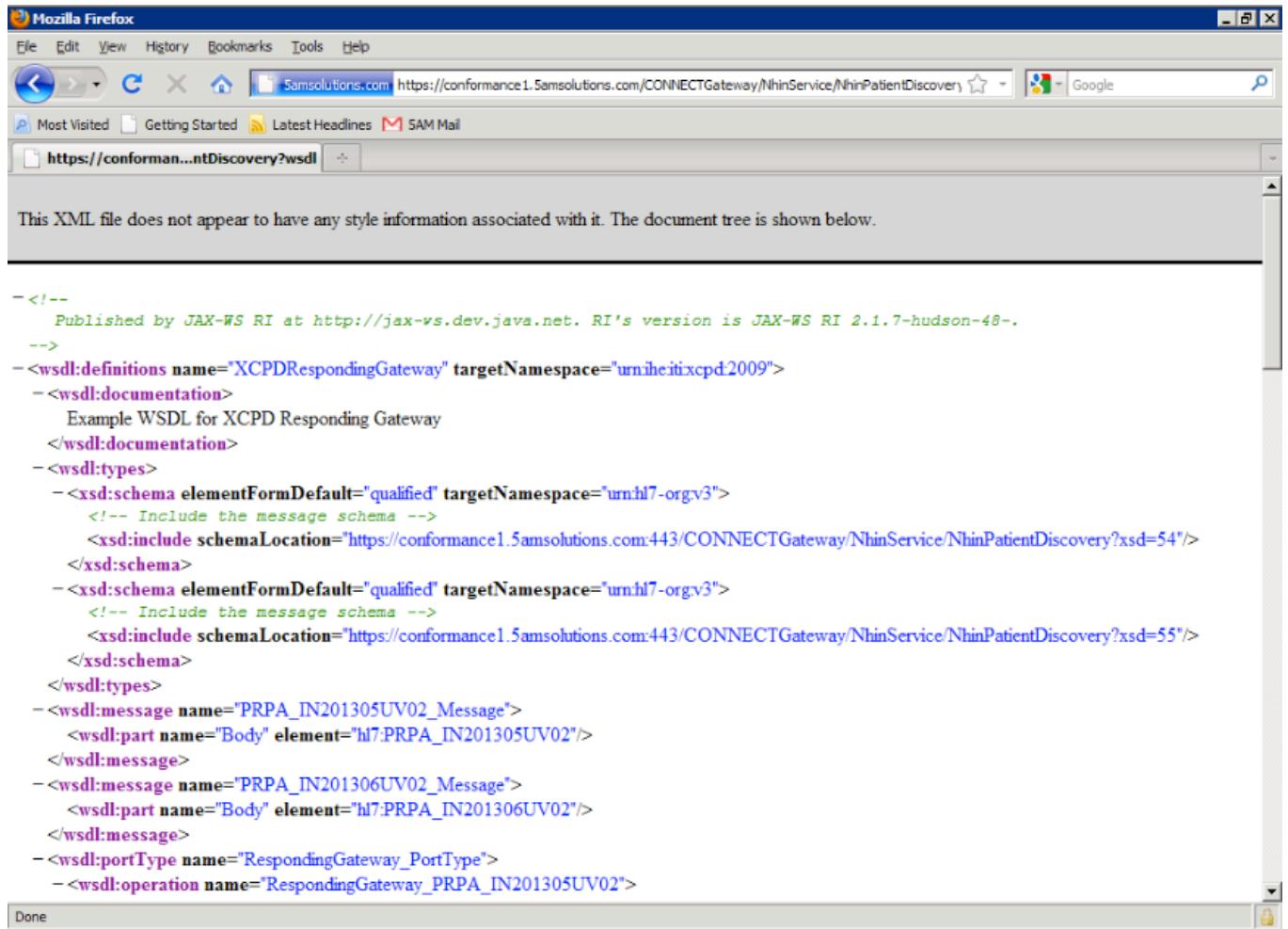
Follow the steps below to perform this task:

Enter a **secured** web service end point in the web browser address field. (You will need to call the WSDL by appending WSDL to the end point uri).

For example:

<https://conformance1.5amsolutions.com:443/CONNECTGateway/NhinService/NhinPatientDiscovery?wsdl>. This will show the end point WSDL, as shown in Figure 1 below.

Figure 1: Example of the WSDL End Point



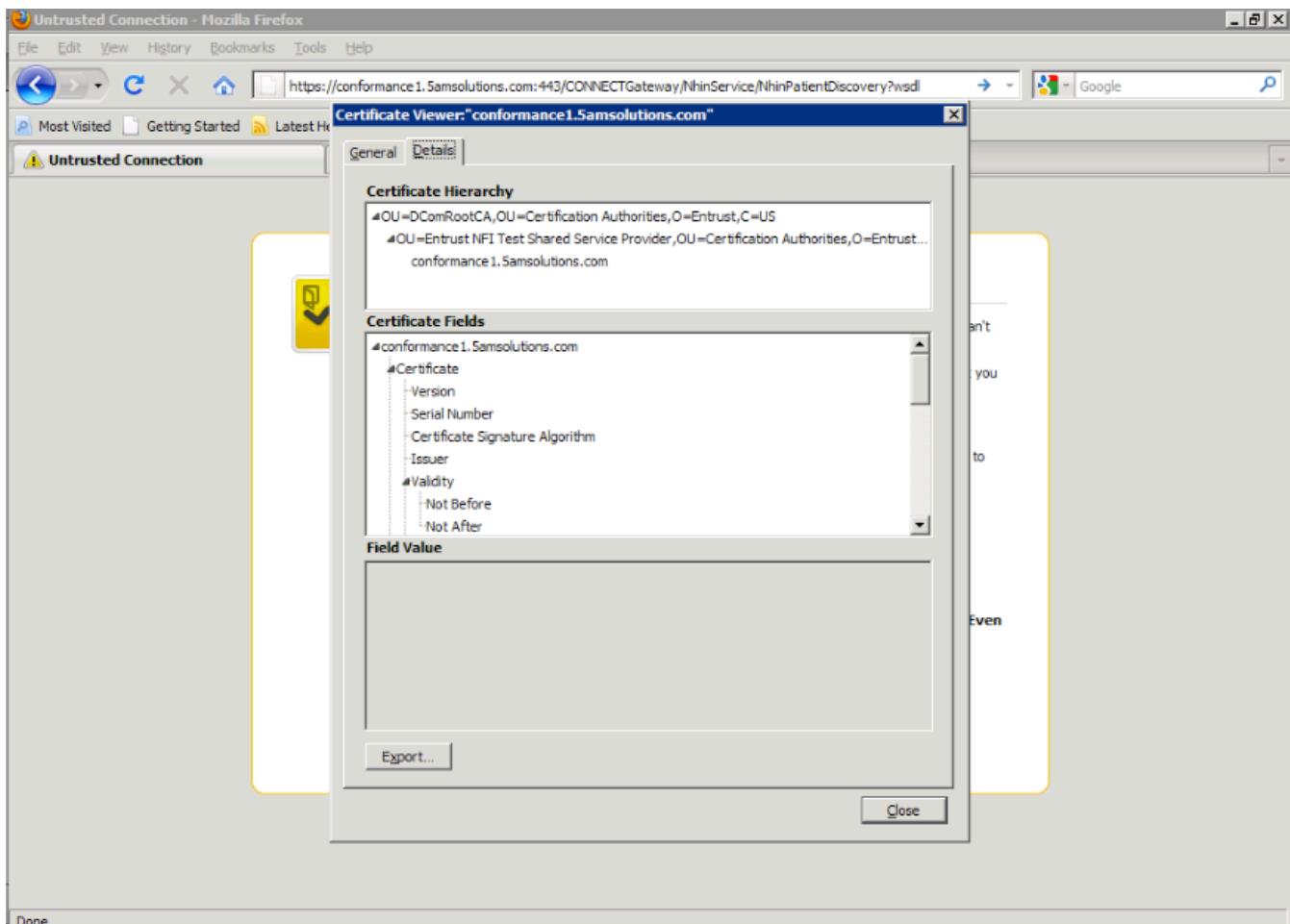
This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
--<!-- Published by JAX-WS RI at http://jax-ws.dev.java.net. RI's version is JAX-WS RI 2.1.7-hudson-48-. -->
-<wsdl:definitions name="XCPDRespondingGateway" targetNamespace="urn:hl7:org:v3">
--<wsdl:documentation>
    Example WSDL for XCPD Responding Gateway
</wsdl:documentation>
--<wsdl:types>
--<xsd:schema elementFormDefault="qualified" targetNamespace="urn:hl7:org:v3">
    <!-- Include the message schema -->
    <xsd:include schemaLocation="https://conformance1.5amsolutions.com:443/CONNECTGateway/NhinService/NhinPatientDiscovery?xsd=54"/>
</xsd:schema>
--<xsd:schema elementFormDefault="qualified" targetNamespace="urn:hl7:org:v3">
    <!-- Include the message schema -->
    <xsd:include schemaLocation="https://conformance1.5amsolutions.com:443/CONNECTGateway/NhinService/NhinPatientDiscovery?xsd=55"/>
</xsd:schema>
</wsdl:types>
--<wsdl:message name="PRPA_IN201305UV02_Message">
    <wsdl:part name="Body" element="hl7:PRPA_IN201305UV02"/>
</wsdl:message>
--<wsdl:message name="PRPA_IN201306UV02_Message">
    <wsdl:part name="Body" element="hl7:PRPA_IN201306UV02"/>
</wsdl:message>
--<wsdl:portType name="RespondingGateway_PortType">
--<wsdl:operation name="RespondingGateway_PRPA_IN201305UV02">
```

From the browser, view the Certificate (which should have been installed in the general steps above), by going to advanced, view certificates or advanced, encryption in most browsers.

You should see the trust chain flow from the root CA to your server, as shown in Figure 2 below.

Figure 2: Trust Chain Flow from the Root CA



Viewing the chain provides you with the assurance that the Certificate has been installed correctly.

Labels parameters

Labels:

None



Confirming Correct CONNECT Configuration

- Added by [Leslie Power](#), last edited by [Azreen Rahman](#) on Jan 28, 2011 ([view change](#))
[Go to start of metadata](#)

view	4195427
------	---------

Organizations employing CONNECT solutions have numerous resources available to guide the decision-making, development, installation, and configuration process.

Please refer to the [CONNECT](#) website for more details.

Listed below are some ***common configuration misunderstandings*** that impact Validation Testing.

Understand the Difference Between a Home Community ID (HCID) and Assigning Authority (AA)

According to the Nationwide Health Information Network specifications, available on the [ONC NHIN Overview](#) webpage, the Home Community ID is an Object Identified (OID) ID assigned to an organization. The Home Community ID applies to the organization that is participating in an exchange; for example, it will be used to identify the organization making a request.

For more information on the formatting of OIDs, please visit the [OID FAQ](#) webpage. One way to obtain an OID is via the [OID Registry](#) webpage.

An Assigning Authority is also represented by an Object Identifier, and represents an entity that has information on a patient. In the health information exchange model, a Home Community may represent several other organizations, entities, or storage locations, while Assigning Authorities holds patient data.

An organization could receive a Patient Discover (PD) request, and respond with information from several "different" Assigning Authorities. Every organization must have a Home Community ID and will have at least one Assigning Authority. A Home Community ID and Assigning Authority ID are not required to be the same.

Properly Configure adapter.properties File with your Home Community ID (HCID) and Assigning Authority (AA)

In CONNECT, the adapter.properties file (located in <root>/config/nhin) is where the organization's HCID and AA are set. Please note, the default CONNECT configuration assumes a single HCID-to-AA relationship, that a single HCID has one and only one AA. Please refer to the [CONNECT](#) website for more information.

These values should be set before Validation Testing begins, and the HCID should match the HCID that the organization uses for its registration in the Services Registry.

?

```
assigningAuthorityId=<your assigning authority, often same as your HCID:  
example: 2.16.840.1.113883.3.900000000>  
XDSBHomeCommunityId=<typically your HCID: example:  
2.16.840.1.113883.3.900000000>
```

Properly Configure gateway.properties File with your Home Community ID (HCID) and Assigning Authority (AA)

In CONNECT, the gateway.properties file (located in <root>/config/nhin) also contains HCID and AA properties which should be set before Validation Testing begins, and the HCID should match the HCID that the organization uses for its registration in the Services Registry.

?

```
localHomeCommunityId=<your HCID: example: 2.16.840.1.113883.3.900000000>  
localDeviceId=<typically your HCID: example: 2.16.840.1.113883.3.900000000>
```

Properly use UDDI or internalConnectionInfo.xml to Access Other Exchange Gateways.

CONNECT can be configured to pull Exchange participant endpoints from the Services Registry (UDDI), and can also accommodate hard-coded endpoints in its internalConnectionInfo.xml file.

To set CONNECT to pull from the validation UDDI, edit gateway.properties (located in <root>/config/nhin) to set the UDDI refresh to true (at whatever frequency, apparently in seconds, you desire) and point to the validation UDDI.

?

```
UDDIRefreshActive=true  
UDDIRefreshDuration=3600  
UDDIInquiryEndpointURL=https://registry-vs.nhinonline.net/uddi/inquiry
```

After the initial connection is made CONNECT will update its uddiConnectionInfo.xml (located in <root>/config/nhin) with the endpoints registered in the UDDI. Please send the contents of this file to your validation representative, to validate on the Services Registry specification.

To manually set an endpoint, edit the internalConnectionInfo.xml file (located in <root>/config/nhin). Create a new <internalConnectionInfo> node, and enter the endpoint information of the system you seek to communicate with. If you do not plan to access the conformance and interoperability endpoints using the UDDI, your validation representative will provide you with the test lab endpoints, which you can then enter in internalConnectionInfo.xml.

Please note, that when CONNECT gathers information for its endpoint registry, it loads uddiConnectionInfo first, then loads internalConnectionInfo, which will overwrite any duplicate information loaded from uddiConnectionInfo.

Labels parameters	http://jira.siframe	5604140	OBTI
Labels:			



Ensuring Services Registry Entry is Correct

- Added by [Azreen Rahman](#), last edited by [Azreen Rahman](#) on Jan 28, 2011 ([view change](#))
[Go to start of metadata](#)

[view](#) 4195427

All Exchange participants are required to enter their service end points in the Exchange's Services Registry (UDDI). The Exchange validation program uses UDDI entries to communicate with candidate systems, so it is essential that each organization confirms its UDDI entry before beginning testing.

"Check your entry" is the content of this Key to Success. When the UDDI entry is correct, the validation labs know how to reach the proper end points, and an initial connectivity hurdle is overcome.

Tips on Proper Completion of the Validation Services Registry Form

When you enter Validation, your system should be Production-Ready and on a Staging-Type tier within your infrastructure. You will have installed your Validation Certificate prior to completing your Validation Services Registry form. You should be on a system with a stable IP address or domain name, with appropriate Ports open.

The form asks for the end points for the services your system will provide across the Exchange. Double-check your entries, and when your Onboarding Manager provides you with a confirmation form, take the time to review it and make any corrections. Last minute Path or Port changes can impact your test schedule.

You can also query the Validation Services Registry to find your own entry and confirm correction. This is also good practice if you will be seeking validation on the Services Registry specification.

Tips for CONNECT Users

For Patient Discovery (PD), Query for Documents (QD), and Retrieve Documents (RD) services, the external end points for CONNECT are typically those outlined below:

?

Patient Discovery:
<server domain>:<port, usually 443 secure>/<path, often
CONNECTGateway>/NhinService/NhinPatientDiscovery

?

Query for Documents:
<server domain>:<port, usually 443 secure>/<path, often
CONNECTGateway>/NhinService/RespondingGateway_Query_Service/DocQuery

?

Retrieve Documents:
<server domain>:<port, usually 443 secure>/<path, often
CONNECTGateway>/NhinService/RespondingGateway_Retrieve_Service/DocRetrieve

Labels parameters

Labels:

None



Ensuring Correct Formatting of Message Codes

- Attachments:1
- Added by [Azreen Rahman](#), last edited by [Azreen Rahman](#) on Jan 28, 2011 ([view change](#))
[Go to start of metadata](#)

[view](#)

4195427

Formatting Requirements

While most Query for Documents (QD) code values are optional, candidate systems need to understand the formatting requirements so that they can send and respond to properly formatted codes.

The basic requirement for codes in the Query for Documents (QD) message is listed below:

?

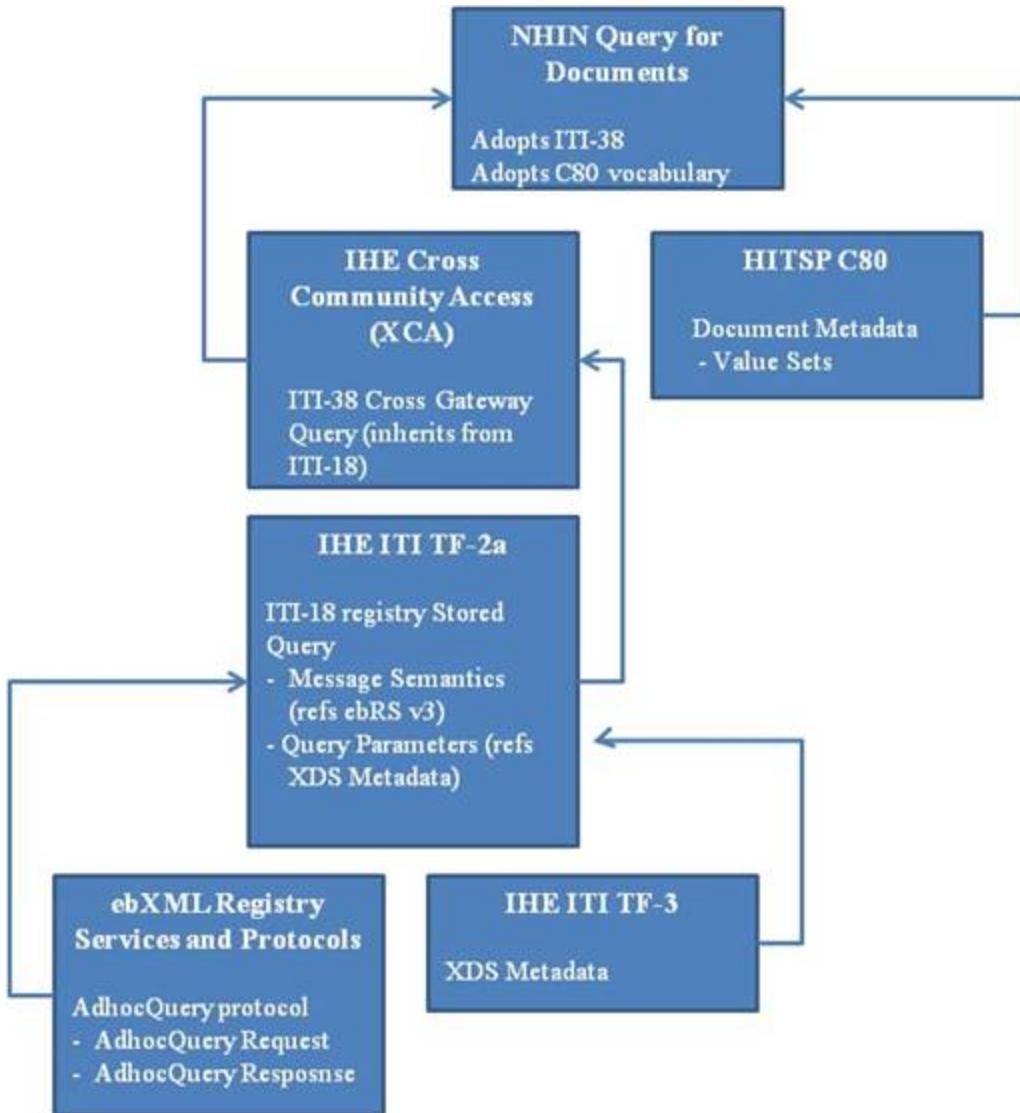
`"code^^coding-scheme"`

This formatting applies to the following message codes:

- Class Code
- Confidentiality Code
- Format Code
- Practice Setting Code
- Language Code
- Type Code

The Query for Documents (QD) specification depends on other specs and standards, as described in the Figure 1 below.

Figure 1: Specs and Standards



The following text walks through those dependencies to point out how the specification is referenced.

1. The specific format requirement can be found in:

- [IHE ITI TF vol2a|http://www.google.com/url?sa=t&source=web&cd=4&ved=0CCcQFjAD&url=http%3A%2F%2Fwww.ihe.net%2FTechnical_Framework%2Fupload%2FIHE_ITI_TF_6-0_Vol2x_FT_2009-08-10.pdf&rct=j&q=IHE%20ITI%20TF-6&ei=CEk-TdybloL-8AahkpzZCg&usg=AFQjCNExzeV1YHM69JLs9aINOh8la1yt0g&sig2=6RniiEdF3k6YXrJX0vByvw&cad=rja], 3.18.4.1.2.3.7, and the first subsection under that is 3.18.4.1.2.3.7.1 FindDocuments, which is the primary query used by the Exchange.
- That section lists all the parameters for the FindDocuments query, including \$XDSDocumentEntryClassCode, which has a footnote.
- The footnote says "Shall be coded according to specification in ITI TF-2a: 3.18.4.1.2.3.4 Coding of Code/Code-Scheme", which says: 3.18.4.1.2.3.4 Coding of Code/Code-Scheme.
- When specifying a coded value parameter, an abbreviated form of the HL7 V2.5 CE format shall be used.

- Only the first (identifier) and third (coding scheme) elements shall be specified. Both are required. The second element shall be empty. The HL7 V2.5 length limits shall not apply. The ebRIM limit on Slot Value size does apply.
 - An example of this format is: code^{coding-scheme}. This style parameter always accepts multiple values so example codings in context look like: <Value>(code1^{coding-scheme1})</Value>.
2. Unfortunately,a proper example is not available in the specs. The v2.0 of the Exchange Query for Documents (QD) spec does not provide an example of any coded value. In IHE ITI TF vol2a, if you go down to section 3.18.4.1.2.7.1.1 Sample Registry Stored Query SOAP Request, you will see another coded value:
3. ?

```
<rim:Slot name="$XDSDocumentEntryHealthcareFacilityTypeCode">
  <rim:ValueList>
    <rim:Value>('Emergency Department')</rim:Value>
  </rim:ValueList>
</rim:Slot>
```

4. ...please note that the example is incorrect as it does not follow the spec. Therefore, putting it all together (and ignoring the incorrect example), the slot should look like this:
5. ?

```
<Slot name="$XDSDocumentEntryClassCode">
  <ValueList>
    <Value>('codecoding-scheme')</Value>
  </ValueList>
</Slot>
```

6. ...that applies to all code parameters on a Query for Document (QD) message.

Labels parameters

<http://jira.sifframe>

7405941

OBTI

Labels:

None

Are you sure you Click to toggle the Cancel



Using the NIST Tools to Review Messages for Conformance

- Added by [Mike Hunter](#), last edited by [Azreen Rahman](#) on Feb 02, 2011 ([view change](#))
[Go to start of metadata](#)

view	4195427
------	---------

Validating Messages Using XDS Tools

Introduction

The National Institute of Standards and Technology (NIST) provides a public tool for validating that messages conform to the specifications for Query for Documents (QD) and Retrieve Document (RD) exchanges on the Nationwide Health Information Network. The tool is known as "XDS Tools" and resides at the following URL: <http://ihexds.nist.gov/xdstools2/>

This document describes how to use the Message Validator functionality of the tool to validate message conformance.

The tool only validates the complete message in XML format with the full SOAP envelope. You can extract these messages from your gateway logs by searching for the strings in Table 1, then extracting the XML message containing the string.

Table 1: Search Strings by Message Type

Message Type	Search String	Grep String
Query for Documents Request	<Action>urn:ihe:iti:2007:CrossGatewayQuery</Action>	urn\:\ihe\:\iti\:\2007\:\CrossGatewayQuery
Query for Documents Response	<Action>urn:ihe:iti:2007:CrossGatewayQueryResponse</Action>	urn\:\ihe\:\iti\:\2007\:\CrossGatewayQuery Response

Retrieve Document Request	<Action>urn:ihe:iti:2007:CrossGatewayRetrieve</Action>	urn\ihe\iti\2007\CrossGatewayRetrieve
Retrieve Document Response	<Action>urn:ihe:iti:2007:CrossGatewayRetrieveResponse</Action>	urn\ihe\iti\2007\CrossGatewayRetrieveResponse

Accessing XDS Tools

Using your browser, navigate to this link: <http://ihexds.nist.gov/xdstools2/>.

You should see the Home Page for the tool, as shown in Figure 1.

Figure 1: XDS Tools Home Page

Queries & Retrieves	Tools	Simulators
FindDocuments	Site/Actor Configuration	Simulator Control
MPQ-FindDocuments	Repository Listing	Simulator Message View
GetDocuments	Pre-Connectathon Tests	
GetRelated	Test Log Listing	
GetFolders	Connectathon Tools	
GetSubmissionSetAndContents	Message Validator	
RetrieveDocument	Registry Test Data	
	Repository Test Data	

Accessing the Message Validator

From the XDS Tools Home Page, click on the "Message Validator" link. This will load the Message Validator tab, as shown in Figure 2.

Figure 2: Message Validator Tab

[Home](#) [Message Validator](#)

[\[close\]](#) [\[help\]](#)

Message Validator

Choose message type

ProvideAndRegister.b
 Register.b
 XDR
 XDM
 Stored Query
 Retrieve
 Guess based on content

Request Message
 Response Message

Cross-Community
 with SOAP Wrapper
 with HTTP Wrapper
 Show less detail

Validating the Message

To validate a Query for Documents (QD) or Retrieve Document (RD) message:

1. Click on the “Browse” button
2. Navigate to the XML message
3. Ensure that the radio button “Guess based on content” is selected
4. Click the “Validate” button

You will see a report similar to what is presented in Figure 3.

Figure 3: Sample Report

[\[close\]](#) [\[help\]](#)

Message Validator

Choose message type

- ProvideAndRegister.b
 - Register.b
 - XDR
 - XDM
 - Stored Query
 - Retrieve
 - Guess based on content
-
- Request Message
 - Response Message
-
- Cross-Community
 - with SOAP Wrapper
 - with HTTP Wrapper
 - Show less detail

/Users/mhunter/Document

[Browse...](#)[Validate](#)[Inspect Metadata](#)**Summary:** Errors were found

Time of validation: Fri Jan 28 10:37:12 EST 2011

Client IP Address: 71.163.115.118

File validated: qdi.xml

Detail**Status Reference****Requested Validation Context**

???;Updateable

ok

Parse Decision - Explicit validation not requested - looking at content**SOAP Wrapper**

Envelope	ok	
Header	ok	
WS-Addressing	ok	
A WS-Addressing SOAP header element must have attribute soapenv:mustUnderstand="1" error		ITI TF-2x: V.3.2.2
WS-Addressing Action Header	ok	
Found WS-Action: urn:ihe:iti:2007:CrossGatewayQuery	ok	
Body	ok	
Scheduling validation of body based on WS-Action	ok	
Validation Context is Request;SQ;XC;Updateable	ok	

Interpreting the Results

All errors will be flagged in red on the report. To interpret the error, go to the referenced specification, also shown in red on the right, and navigate to the referenced section or table.

The specification will explain the expected behavior, often illustrated with examples.

If you have questions after reviewing the specification, or believe the error may be an issue with CONNECT, please contact the Conformance Testing Team for support.

Validating the Message Payload Using the CDA Validation Tool

Introduction

NIST provides a public tool for validating message payloads conformance to the specifications for the following payloads used in exchanges on the Nationwide Health Information Network:

- C37: Lab Report Document
- C32: HITSP Summary Documents Using HL7 CCD (formerly known as Registration and Medication History)
- C28: Emergency Encounter Summary Document Component

Please see <http://xreg2.nist.gov/cda-validation/index.html> for more details.

The tool is known as the CDA Validation Tool and resides at the following URL: <http://xreg2.nist.gov/cda-validation/validation.html>

This document describes how to use the tool to validate message payloads. The tool only validates the CDA document in XML format. You can extract these documents from your gateway logs by searching for the string "ClinicalDocument," then extracting the corresponding XML document. For C32s, the XML document will also include the string, "urn:hl7-org:v3 C32_CDA.xsd".

Accessing the CDA Validation Tool

Using your browser, navigate to: <http://xreg2.nist.gov/cda-validation/validation.html>

You will be directed to the Home Page for the tool, as shown in Figure 4.

Figure 4: CDA Validation Tool Home Page

CDA Guideline Validation

NIST CDA Guideline Validation DRAFT – How to Use the NIST T... +

[FAQs](#) [Contact](#)

CDA Guideline Validation

Home Validation Tool Downloads Web Service Meaningful Use

1. Upload the file for validation:
2. Please select the level of detail:
 - Everything (Errors, Warnings, Notes)
 - Errors and Warnings only
 - Errors Only
3. What would you like this file to validate to?

Name	Description	Dependencies (if applicable)
<input checked="" type="radio"/> CDA R2	HL7 CDA R2 (with no extensions)	
<input type="radio"/> CCD	Continuity of Care Document	• CDA R2
<input type="radio"/> CRS Level 1 & 2	HL7 Care Record Summary	• CDA R2
<input type="radio"/> CDA4CDT (header only)	HL7 CDA For Common Document Types (CDA4CDT) -- header only	• CDA R2
<input type="radio"/> HITSP/C32 v2.5 – HITSP/C83 v2.0	HITSP/C32 v2.5 Summary Documents Using HL7 CCD	• CDA R2 (With HITSP Extensions) • CDA4CDT (header only and with IHE modifications) • CCD
<input type="radio"/> HITSP/C32 v2.5 – HITSP/C83 v1.1	HITSP/C32 v2.5 Summary Documents Using HL7 CCD (using HITSP/C83 v1.1)	• CDA R2 (With HITSP Extensions) • CDA4CDT (header only and with IHE modifications) • CCD
<input type="radio"/> HITSP/C32 v2.4	HITSP/C32 v2.4 Summary Documents Using HL7 CCD (using HITSP/C83 v1.0)	• CDA R2 (With HITSP Extensions) • CCD
<input type="radio"/> HITSP/C32 v2.1	HITSP/C32 v2.1 Summary Documents Using HL7 CCD	• CDA R2 (With HITSP Extensions) • CCD
<input type="radio"/> NHIN Summary Patient Record	NHIN Summary Patient Record (based on HITSP/C32)	• CDA R2 (With HITSP Extensions) • CCD • HITSP/C32 v2.1
<input type="radio"/> IHF Lab 2008	IHF Laboratory Report -- 2008	• CDA R2 (With IHF IAR)

Find: Next Previous Highlight all Match case

Done

Validating the Message Payload

To validate a CDA document from the message:

1. Click on the “Browse” button
2. Navigate to the XML message
3. Select the desired level of validation. "Errors only" is recommended.
4. Select the payload specification to use in the validation. For example, for C32s, you could select "HITSP/C32 v2.5 – HITSP/C83 v1.1" to validate to version 2.5 of the HITSP specification.
5. Click the “Validate” button

You will see a report similar to what is presented on Figure 5.

Figure 5: Sample Report

The screenshot shows a web browser window titled "CDA Guideline Validation". The URL is <http://xreg2.nist.gov/cda-validation/validation.html>. The page content is as follows:

CDA Guideline Validation

Home Validation Tool Downloads Web Service Meaningful Use

CDA R2 (With HITSP Extensions) Errors:

- cvc-pattern-valid: Value '02/07/2008' is not facet-valid with respect to pattern '[0-9]{1,8}([0-9]{9,14}|[0-9]{14,14}\.[0-9]+)([+\-\][0-9]{1,4})?' for type 'ts'.
- cvc-attribute.3: The value '02/07/2008' of attribute 'value' on element 'time' is not valid with respect to its type, 'ts'.
- cvc-pattern-valid: Value 'N0000005824 (Prochlorperazine)' is not facet-valid with respect to pattern '[^\s]+' for type 'cs'.
- cvc-attribute.3: The value 'N0000005824 (Prochlorperazine)' of attribute 'code' on element 'code' is not valid with respect to its type, 'cs'.
- cvc-datatype-valid.1.2.2: " is not a valid value of list type 'real'.
- cvc-attribute.3: The value " of attribute 'value' on element 'period' is not valid with respect to its type, 'real'.

CDA R2 (With HITSP Extensions) Warnings: *No warnings!*

CDA4CDT (header only and with IHE modifications):

Schematron Report

Schematron schema for validating conformance to History and Physical documents

CCD:

Schematron Report

Schematron schema for validating conformance to CCD documents

HITSP/C32 v2.5 -- HITSP/C83 v1.1:

Schematron Report

HITSP_C32 V2.5

Find: Next Previous Highlight all Match case Done

Interpreting the Results

Because the payload specifications are composed of other specifications, errors are listed in the report under the appropriate referenced specification composing the specification selected for validation. An explanation of the expected result is provided with the flagged error.

If you have questions after reviewing the specification, or believe the error may an issue with CONNECT, please contact the Conformance Testing Team for support.



Avoiding Common Authorization Framework

Conformance Errors

- Added by [Joe Lamy](#), last edited by [Azreen Rahman](#) on Jan 28, 2011 ([view change](#))
[Go to start of metadata](#)

[view](#) 4195427

During testing, we find numerous message conformance errors related to the Authorization Framework specification, which forms the access control backbone of the Exchange.

This section will provide you with the guidance to avoid the most common errors. You'll notice most of the examples provided are of problems rather than solutions. The specifications themselves (linked below) provide positive examples of what gateways should do.

Authorization Framework Overview

You can find the most recent Exchange specifications from the [Nationwide Health Information Network Inventory of Tools](#) webpage.

From the Authorization Framework specification:

- The Authorization Framework defines the exchange of metadata used to characterize the initiator of an NHIN request so that it may be evaluated by responding NHIOs in local authorization decisions.
- Along with the Messaging Platform, this specification forms the NHIN's messaging, security, and privacy foundation. It employs SAML 2.0 assertions.
- The purpose of this exchange is to provide the responder with the information needed to make an authorization decision for the requested function. Each initiating message must convey information regarding end user attributes and authentication using SAML 2.0 assertions.

Simply put,

- The Messaging Platform provides base messaging, security, and privacy for all participants.
- The Authorization Framework allows responders an extra layer of control over each response based on information about the initiator passed in a Security Assertion Markup Language (SAML) assertion.

The SAML assertion is included in the security header in request messages only, as follows:

- Simple Object Access Protocol (SOAP) envelope
 - SOAP Header - contains timestamp, addressing and security header (which includes the SAML assertion).
 - SOAP Body - contains the actual request message.

Note that the requirements burden falls squarely on the initiator to provide all the necessary information, formatted correctly, in the SAML header. The responder MAY choose to use this information or ignore it entirely. **This is probably the main reason why we see many errors in this area: you can send**

messages perfectly well with much of the authorization information missing or formatted incorrectly.

Reviewing Cross-Gateway Messages

Since most of our testing revolves around the Patient and Document Service Set (Patient Discovery, Query for Documents, and Retrieve Documents), we will focus on addressing that here. These basic concepts should carry no matter what Exchange services you are exercising.

A **key step** in avoiding Authorization Framework errors is the inspection of your actual Cross-Gateway Request messages. If you are integrating with a gateway product rather than building your own gateway, you may not be aware of what actually goes across the wire until you look.

Check a Representative Sample of Requests

First, a good rule of thumb is to check one of each of the Service Request messages you make, for example, one each of Patient Discovery (PD), Query for Documents (QD), and Retrieve Documents (RD) requests. We often find errors in calls to one service but not another.

Use Server Logs from the Receiving Side (if possible)

When we are inspecting messages for validation, we prefer the Web Server logs from the receiving side, even though both sides' logs may contain Cross-Gateway messages. This ensures that we are seeing the actual message that crossed the wire. Therefore, we would look at the Responder's logs for request messages.

Make Sure to Look at the Cross-Gateway Messages

CONNECT and other gateways often have a lot of SOAP message traffic that shows up in logs apart from the actual cross-gateway (i.e. Exchange) messages. These additional messages can represent logging or intermediate stages in building the final message, and as such, may look confusingly similar to the Cross-Gateway messages.

We look for the WS-Addressing Action element to separate out the Cross-Gateway messages. In the example snippet below, from the **Messaging Platform specification**, you see part of the example SOAP request showing the Action as the last line:

?

```
<soapenv:Envelope
  xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope"
  xmlns:wsa="http://www.w3.org/2005/08/addressing"
  xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
  wssecurity-secext-1.0.xsd"
  xmlns:wsu="http://docs.oasis-open.org//wss/2004/01/oasis-200401-
  wsswssecurity-utility-1.0.xsd"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <soapenv:Header>
```

```

<!-- MessageID, To and Action are required elements -->
<!-- Unique identifier of this message -->
<wsa:MessageID>urn:uuid:0fbfdced-6c01-4d09-a110-
2201afedaa02</wsa:MessageID>
<!-- URI of the service -->
<wsa:To
soapenv:mustUnderstand="1">http://stlsewhere.com/XdsService/IHEXDSRepository
.svc</wsa:To>
<!-- URI indicates specific action that is requested to be performed by
the service -->
<!-- Same as To URI in HTTP requests -->
<!-- In a non-HTTP request, To and Action may be different, with Action
pointing to the WSDL PortType -->
<wsa:Action
soapenv:mustUnderstand="1">urn:ihe:iti:2007:RetrieveDocumentSet</wsa:Action>
.....

```

The Actions used in the Patient and Document Service Set are as follows (for SAML we will only be looking for the requests, which have been highlighted):

urn:hl7-org:v3:PRPA_IN201305UV02:CrossGatewayPatientDiscovery (PD request)
urn:hl7-org:v3:PRPA_IN201306UV02:CrossGatewayPatientDiscovery (PD response)
urn:ihe:iti:2007:CrossGatewayQuery
urn:ihe:iti:2007:CrossGatewayQueryResponse
urn:ihe:iti:2007:CrossGatewayRetrieve
urn:ihe:iti:2007:CrossGatewayRetrieveResponse

Given all this, an easy way to find cross-gateway messages is to search the logs using the string ":CrossGateway".

Inspect the Messages in an XML-Aware Tool if Possible

Now that you have the messages, it is much easier to inspect them by saving each one as an .xml file and opening it in an XML-aware tool like a web browser or XMLSpy.

Frequent SAML Errors

Issuer Element Not Referring to an Identifiable Person or System

In the header of request messages, the Issuer element is often sent using default values (e.g. CN=SAML User).

- Specification reference: Authorization Framework Section 3.3
- XPath (2 places):
 - Envelope/Header/Security/Assertion/Issuer
 - Envelope/Header/Security/Assertion/AuthzDecisionStatement/Evidence/Assertion/Issuer

As described in the specification, the Issuer element is required to identify the individual responsible for issuing the Assertions carried in the message. This is normally the system security officer for the sending

NHIO. The Spec Factory recently clarified that this can represent a system: "This is the identity of the identity-provider, not necessarily a human. At best, this might be an organization or arm-of-an-organization.".

See the discussion in this [forum](#).

Example of the Issuer not being set ("SAML User" is the name used in the Authorization Framework specification example and not a real identity provider name):

?

```
<saml2:Issuer Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName">
    CN=SAML User,OU=Harris,O=HITS,L=Melbourne,ST=FL,C=US
</saml2:Issuer>
```

Subject Element or Subject ID Attribute (both should represent the same identity) is Missing or Not Referring to an Identifiable Person or System

There are two locations (differently formatted) in the SAML that represent the same identity - the subject of the request, meaning the individual making the request. The Spec Factory recently clarified that this could represent a system in some cases. Please see the discussion in this [forum](#).

We often see one of these missing or containing a value that is not a person or system.

Subject

- Specification reference: Authorization Framework Section 3.3
- XPath: Envelope/Header/Security/Assertion/Subject

Subject ID attribute

- Specification reference: Authorization Framework Section 3.3.2.1
- XPath: Envelope/Header/Security/Assertion/AttributeStatement/Attribute, where Attribute/@Name = "urn:oasis:names:tc:xspa:1.0:subject:subject-id"

Example, where the sender is only using default values:

?

```
<saml2:Issuer Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName">
    CN=defaultIssuerCommonName,OU=defaultIssuerOrganizationalUnit,O=defaultIssu
erOrganization,
    L=defaultIssuerLocality,ST=defaultIssuerStateOrProvince,C=USA
</saml2:Issuer>
```

Incorrect/Missing Subject Organization ID or Home Community ID Attributes

Two required attributes in the Attribute Statement refer to OIDs, and are often missing or incorrect.

Subject Organization ID attribute

- Specification reference: Authorization Framework Section 3.3.2.3
- XPath: Envelope/Header/Security/Assertion/AttributeStatement/Attribute, where Attribute/@Name = "urn:oasis:names:tc:xspa:1.0:subject:organization-id"

Home Community ID attribute

- Specification reference: Authorization Framework Section 3.3.2.4
- XPath: Envelope/Header/Security/Assertion/AttributeStatement/Attribute, where Attribute/@Name = "urn:nhin:names:saml:homeCommunityId"

The most common error with both is leaving off the "urn:oid:" at the beginning of the OID, for example:

?

```
<saml2:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:organization-id">
  <saml2:AttributeValue>
    ns6:type="ns7:string">2.16.840.1.113883.3.333</saml2:AttributeValue>
</saml2:Attribute>
```

Another error often seen is when a clearly invalid OID is used, for example "1.1", which meets the syntactic definition, but has not been assigned to an organization.

Purpose of Use Attribute Contains Element Called "Attribute/AttributeValue/PurposeForUse" Instead of "Attribute/AttributeValue/PurposeOfUse"

This is a known issue that exists in all testing candidates and participants to date. It is described here on the [Spec Factory Wiki](#).

The specification in this area used an incorrect example, and this was followed by all existing exchange participants. Because of this, the incorrect value has become a defacto standard, and will remain so until the Spec Factory employs the change management process to change it. For now, the Test Team flags the error but does not force any change.

- Specification reference: Authorization Framework Section 3.3.2.6
- XPath: Envelope/Header/Security/Assertion/AttributeStatement/Attribute, where: Attribute/@Name = "urn:oasis:names:tc:xspa:1.0:subject:purposeofuse"

Incorrect Patient Identifier Attribute

Note: the Spec Factory has recently clarified that this attribute is optional even for patient-specific service calls such as Patient Discovery, Query for Documents, and Retrieve Documents, unless it is needed for an ACP retrieval.

The optional Patient Identifier attribute in the Attribute Statement is often incorrectly formatted.

- Specification reference: Authorization Framework Section 3.3.2.7
- XPath: Envelope/Header/Security/Assertion/AttributeStatement/Attribute, where Attribute/@Name = "urn:oasis:names:tc:xacml:2.0:resource:resource-id"

This value contains the patient identifier of the requesting organization, formatted as:

?

```
|IDNumber^^^&OIDofAA&ISO|
```

Where "OIDofAA" is the OID of the assigning authority.

In XML, encode ampersands, for example:

?

```
|543797436^^^&1.2.840.113619.6.197&ISO|
```

The most common errors are:

- Passing the IDNumber only:

?

```
|543797436|
```

- Failing to encode the ampersands:

?

```
|543797436^^^&1.2.840.113619.6.197&ISO|
```

- Doubly encoding the ampersands:

?

```
|543797436^^^&amp;1.2.840.113619.6.197&amp;ISO|
```

Authorization Decision Statement Present but With No ACPs Referenced Within

This optional element should only be present if at least one Access Consent Policy (ACP) or Instance Access Consent Policy (IACP) is referenced within it. If any IACPs are referenced, they must refer to documents that can be queried and retrieved using TP30 mechanisms. We see these basic requirements violated in a few ways.

- Specification reference: Authorization Framework Section 3.3.3
- XPath: Envelope/Header/Security/Assertion/AuthzDecisionStatement

ACP reference and retrieval is a complex mechanism not very clearly described in the specifications. See the [Spec Factory wiki](#) page for a detailed explanation.

The following example is the most typical error. The AuthzDecisionStatement element contains the ACP and IACP attributes, but they contain no ACP references, which are required:

?

```
<AuthzDecisionStatement Decision="Permit"  
Resource="https://exttestgw3.fedsconnect.org:443/CONNECTGateway/NhinService/N  
hinPatientDiscovery">  
  <Action  
    Namespace="urn:oasis:names:tc:SAML:1.0:action:rwedc">Execute</Action>
```

```

<Evidence>
    <Assertion ID="c8ac7d09-cbde-4f10-891e-57a9c336b62f" IssueInstant="2010-07-13T18:10:12.351Z" Version="2.0">
        <Issuer Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
            CN=SAML User,OU=SU,O=SAML User,L=Los Angeles,ST=CA,C=US
        </Issuer>
        <Conditions NotBefore="2010-07-13T18:10:12.351Z" NotOnOrAfter="2010-07-13T18:10:12.351Z"/>
        <AttributeStatement>
            <Attribute Name="AccessConsentPolicy"
NameFormat="http://www.hhs.gov/healthit/nhin">
                <Attribute Name="InstanceAccessConsentPolicy"
NameFormat="http://www.hhs.gov/healthit/nhin">
                    <AttributeStatement>
                </Attribute>
            </AttributeStatement>
        </Assertion>
    </Evidence>
</AuthzDecisionStatement>

```

In the above case, the correct format would omit the entire AuthzDecisionStatement element.

Another incorrect form would include one valid and one invalid (i.e. empty) attribute:

?

```

<AttributeStatement>
    <Attribute Name="AccessConsentPolicy"
NameFormat="http://www.hhs.gov/healthit/nhin">
        <AttributeValue>urn:oid:1.2.3.4</AttributeValue>
    </Attribute>
    <Attribute Name="InstanceAccessConsentPolicy"
NameFormat="http://www.hhs.gov/healthit/nhin">
<AttributeStatement>

```

In the above case, the correct format would omit the second Attribute element.

While some gateways are able to handle these errors, they are invalid syntax and are flagged in testing. They could be arbitrarily rejected by responding gateways, impacting the initiator's interoperability.

Finally, if any Instance Access Consent Policies (IACPs) are referenced, they must refer to documents that can be queried and retrieved using TP30 mechanisms. This means they are stored in the document repository and can be retrievable using Query for Documents and Retrieve Documents services. Please see the [Spec Factory wiki](#) page for details.

Assertion Conditions Containing Impossible Times (e.g. NotBefore = NotOnOrAfter)

There are time-based Conditions that cause the assertion to never be valid.

- Specification reference: OASIS Assertions and Protocols for Security Assertion Markup Language (SAML) version 2.0.pdf, Section 2.5.1.2

- XPath: Assertion/Conditions (usually the one at path:
Envelope/Header/Security/Assertion/AuthzDecisionStatement/Evidence/Assertion/Conditions)

In the following example, the problem is that NotBefore = NotOnOrAfter. This means that there is no valid time window for this assertion.

?

```
<Assertion ID="c8ac7d09-cbde-4f10-891e-57a9c336b62f" IssueInstant="2010-07-13T18:10:12.351Z" Version="2.0">
  <Issuer...>...</Issuer>
  <Conditions NotBefore="2010-07-13T18:10:12.351Z" NotOnOrAfter="2010-07-13T18:10:12.351Z"/>
  ...
</Assertion>
```

The other error we see is a little harder to spot. When NotOnOrAfter is before the time that the entire message was created, then the assertion's valid window has already closed:

?

```
<wsse:Security S:mustUnderstand="true">
  <wsu:Timestamp wsu:Id="_1">
    <wsu:Created>2010-12-14T19:31:04Z</wsu:Created>
    <wsu:Expires>2010-12-14T19:36:04Z</wsu:Expires>
  </wsu:Timestamp>
  <saml2:Assertion ID="4e432349-89a4-4fe6-abc1-6b6d80ebb232" IssueInstant="2010-12-14T19:31:04.786Z" Version="2.0">
    ...
    <saml2:Conditions NotBefore="2010-12-14T19:29:32.341Z" NotOnOrAfter="2010-12-14T19:29:32.342Z"/>
  </saml2:Assertion>
</wsse:Security>
```

Some Additional Helpful Tools

- Click on this link to access the Messaging Platform and Authorization Framework **specifications**. They also contain links to related specifications.
- Clickable schemas for **SOAP**, **WS-Addressing**, **WS-Security Utility (Timestamp)** and **SAML**.

Labels parameters

<http://jira.siframe>

5603927

OBTI

Labels:

None



Activation Stage

- Attachments:2
- Added by [Judith Hutman](#), last edited by [Linda Toscano](#) on May 11, 2011 ([view change](#))
[Go to start of metadata](#)

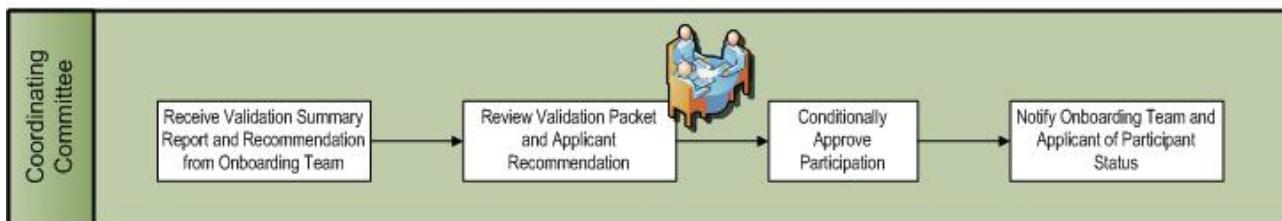
view	7407241
----------------------	---------

Activation Stage

After the Onboarding Team submits the Validation Summary Report to the CC, the Applicant enters the Activation Stage. During this stage, CC reviews the Validation Summary Report which summarizes the results of the Applicant's Conformance and Interoperability testing. CC evaluates these testing results together with the Onboarding Team's recommendation, and determines whether to extend conditional approval for the Applicant to become an Exchange Participant.

Workflow

Onboarding: Exchange Trust Framework Process - Membership Determination



Process

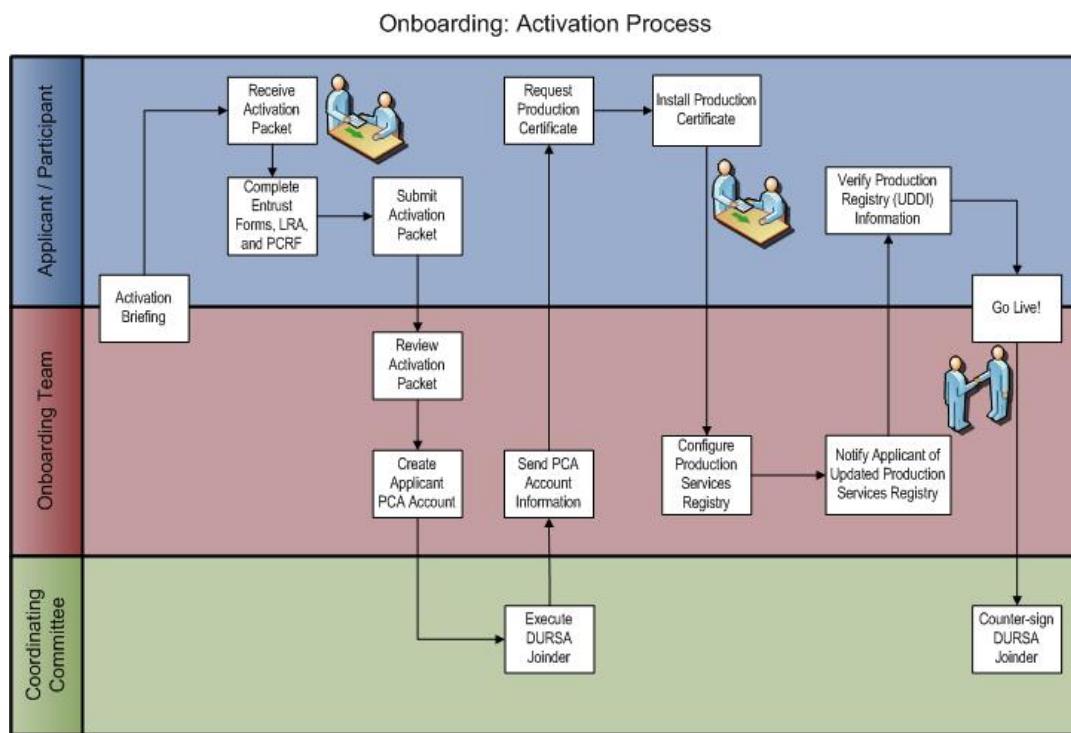
1. CC receives the Applicant's Validation Summary Report and recommendation from the Onboarding Team.
2. CC reviews the Validation Packet and participation recommendation.
3. CC conditionally approves the Applicant to be a Participant.
4. CC notifies the Onboarding Team and the Applicant of conditional approval for participation.

Note: Conditional approval means the Applicant must begin exchanging data in production via the Nationwide Health Information Network within 120 days following CC's approval of the Applicant's Validation Summary Report.

Final Activation

During the Activation Stage, the Onboarding Team and the Applicant exchange required documentation to complete the activation process. This is the final Onboarding stage enabling the Applicant to exchange information using Nationwide Health Information Network standards, services, and policies.

Workflow



Process

1. Onboarding Team conducts the Activation Briefing with the Applicant.
2. Applicant receives the Activation Packet. This packet includes:
 - a. Activation Packet Checklist
 - b. Local Registration Authority (LRA) Appointment Guidelines
 - c. Entrust Managed Services Subscriber Agreement
 - d. Entrust Managed Services Subscriber Identify Verification
 - e. Production Certificate Authority Form (PCAF)
 - f. Production Services Registry Form (PSRF)
3. Using the Activation Checklist as a guide, the Applicant completes the two Entrust forms, the PCAF, and the PSRF.
4. Applicant submits the Activation Packet with the completed forms.
5. Onboarding Team receives the Activation Packet and reviews for completeness.
6. Onboarding Team logs into the Production Certificate Authority (PCA) [Ops:Entrust Authority Administration] and creates an account for the Applicant.
7. CC executes the DURSA Joinder.
8. Onboarding Team sends two emails to the Applicant:

- a. First email provides the PCA URL log on information, instructions, and the reference number.
 - b. Second email provides the PCA Authorization Code.
9. Applicant receives the email, logs into the PCA account, and requests a digital certificate.
 10. Applicant receives the digital certificate from PCA.
 11. Applicant installs the production certificate on the production server.
 12. Onboarding Team configures the Production Services Registry (Production Universal Description Discovery Interface (UDDI)) with the Applicant's PSRF information.
 13. Onboarding Team notifies the Applicant they have updated the Production Services Registry.
 14. Applicant verifies Production Registry (UDDI) information.
 15. Applicant becomes a Nationwide Health Information Network Participant and can start exchanging information with other members of the Nationwide Health Information Network (Go Live!).
 16. CC counter-signs the DURSA Joinder within 30 days of the Applicant's Go-live date.
 17. **Note:** Within 120 days following the CC's approval of the Validation Summary Report, the Applicant must Go Live. If the Applicant's timeline slips and it cannot proceed within 120 days, it must submit an email request to the Onboarding Team POC to request an extension.

Labels parameters

<http://jira.siframes.com:8080/browse/4194744>

OBTI

Labels:

None

Are you sure you want to delete this item? Click to toggle the visibility of this item. Cancel



Frequently Asked Questions (FAQs)

- Added by [Linda Toscano](#), last edited by [Linda Toscano](#) on May 02, 2011 ([view change](#))
[Go to start of metadata](#)

[view](#)

7407241

The Exchange Onboarding Team encourages interested Applicants to ask questions anytime by sending an email to onc.exchangeinfo@hhs.gov. A Team member will respond promptly.

To help direct you to the answers you seek, we divided the FAQs into five sections, General Information, Application Process, Validation Process, All About Certs, and Activation Process. Click on the appropriate topic to proceed to that section.

- **FAQs - General Information** - high-level questions about the Nationwide Health Information Network and the Exchange.
- **FAQs - Application Process** - questions relating to the Application process, an activity that takes place during the Qualification Stage of the Onboarding Process.
- **FAQs - Validation Process** - questions relating to Stage 2 of the Onboarding Process.
- **FAQs - All About Certs** - questions about the certification process.
- **FAQs - Activation Process** - questions relating to Stage 3 of the Onboarding Process.

Labels parameters

<http://jira.siframe>

7898978

OBTI

Labels:

None



FAQs - General Information

- last edited by [Linda Toscano](#) on May 02, 2011 ([view change](#))

[Go to start of metadata](#)

view	7898978
----------------------	---------

- [What is the Nationwide Health Information Network?](#)
- [What is the Nationwide Health Information Network Exchange?](#)
- [What is the Exchange Onboarding Team's role during the Onboarding process?](#)
- [What is the Coordinating Committee's role?](#)
- [What is the Technical Committee's role?](#)
- [What is CONNECT?](#)
- [What are the requirements for Exchange Participants to be Federal Information Processing Standard \(FIPS\) or Federal Information Security Management Act \(FISMA\) compliant?](#)

What is the Nationwide Health Information Network?

The Nationwide Health Information Network is a set of policies, standards, and services that enable Participants to use the Internet for secure and meaningful exchange of health information to improve health and health care. For more information, go to

http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov_nationwide_health_information_network/1142.

[Back to Top](#)

What is the Nationwide Health Information Network Exchange?

The Nationwide Health Information Network Exchange is a confederation of trusted entities, bound by a mission and a common framework of trust, to securely exchange health information using Nationwide Health Information Network standards and specifications. It is a diverse set of entities facilitating information exchange with a broad set of users, systems, geography, or community:

- Internet-based, using common implementation of standards and specifications with secure transport
- Tested for conformance and interoperability
- Enables valid, trusted entities to participate
- Signed trust agreement that allocates responsibilities and accountability to protect information exchanged
- Digital credentials issued to permit only approved Participants to exchange data with other members
- Committee structures to oversee and support activities

For more information about the Exchange, go to

http://healthit.hhs.gov/portal/server.pt?open=512&objID=1407&parentname=CommunityPage&parentid=8&mode=2&in_hi_userid=11113&cached=true.

[Back to Top](#)

What is the Exchange Onboarding Team's role during the Onboarding process?

The Exchange Onboarding Team provides coordination among the stakeholders throughout the Onboarding process. The Exchange Onboarding Team provides step-by-step instructions for the Onboarding Applicant, coordinates Validation activities with the Test Team, and facilitates communication with the Nationwide Health Information Network Coordinating Committee (CC) for review of the application and Validation testing results.

[Back to Top](#)

What is the Coordinating Committee's role?

The Nationwide Health Information Network Coordinating Committee (CC) is provided authority by Exchange Participants to establish and maintain the set of policies, legal agreements, and accountability measures for those entities exchanging data in production today using the Exchange. In an operational role, the CC manages the following responsibilities:

- Committee membership and proceedings
- Admission, suspension, and termination of Participants
- Receiving reports of breaches from Participants and acting upon such reports
- Resolving disputes between Participants
- Determining materiality of proposed new, or changes to technical specifications and testing plans
- Developing and amending operating policies and procedures
- Managing DURSA amendments

[Back to Top](#)

What is the Technical Committee's role?

The Technical Committee (TC) focuses on architectural and technical issues such as approval of new or modified technical requirements, specifications, and testing for the Exchange.

[Back to Top](#)

What is CONNECT?

CONNECT is a software solution that Applicants can use to securely link their existing health IT systems into the health information exchanges. The CONNECT solution enables secure and interoperable electronic health information exchanges with other Nationwide Health Information Network-compliant Participants, including federal agencies, state, tribal and local-level health organizations, and healthcare participants in the private sector. For more information, refer to the CONNECT Community Portal at <http://www.connectopensource.org/>.

[Back to Top](#)

What are the requirements for Exchange Participants to be Federal Information Processing Standard (FIPS) or Federal Information Security Management Act (FISMA) compliant?

The DURSA requires all **federal partners** to be FIPS compliant --

15.06 For Federal Participants only, in addition to complying with Sections 15.01 through 15.05, ensuring that Message Content transmitted adhere to interoperability standards adopted by the Secretary

of Health and Human Services, and the National Institute of Standards and Technology (NIST) and the Federal Information Processing Standards (FIPS), as applicable.

Non-federal partners are not required to be FIPS compliant, nor are they required to be FISMA compliant.

All Exchange Participants are vetted through the Coordinating Committee's established eligibility determination process, which includes:

- Verification that the Participant's Exchange activities are covered under a Federal contract,
- Self-attestation that the Applicant is a valid legal entity in good standing, and
- Self-attestation that the Applicant will be bound by the DURSA.

[Back to Top](#)

Labels parameters

Labels:

None



FAQs - Application Process

- edited by [Linda Toscano](#) on May 02, 2011 ([view change](#))

[Go to start of metadata](#)

View	7898978
------	---------

- [What is the difference between the Application Process and the Qualification Stage?](#)
- [How does the Applicant start the Application process?](#)
- [What application documents does the Applicant need to return?](#)
- [How does the Exchange Onboarding Team want Applicants to return application documents?](#)
- [Original documentation says the Applicant needs Local Registered Authority \(LRA\) forms. How does the Applicant get these forms?](#)
- [What happens after the Applicant submits the application to the Exchange Onboarding Team and NeHC?](#)
- [What happens after the CC meeting?](#)
- [When does the CC meet?](#)
- [What is the timeline for CC notification of eligibility determination?](#)
- [Will the Applicant have regular calls with the Exchange Onboarding Team?](#)

What is the difference between the Application Process and the Qualification Stage?

The Application Process occurs during the Qualification Stage; it is one of the main activities performed by Applicants. Key Applicant activities during the Qualification Stage are:

- Conduct eligibility self-test
- Install compliant gateway
- Attend Kickoff Briefing
- Submit Application Packet

[Back to Top](#)

How does the Applicant start the Application process?

The Applicant should send an email to the Exchange Onboarding Team at onc.exchangeinfo@hhs.gov requesting an Application Packet. The Onboarding Team responds by sending an Application Packet and schedules an Exchange Onboarding Overview briefing with the Applicant.

[Back to Top](#)

What application documents does the Applicant need to return?

The Applicant should return the completed Application, Data Use and Reciprocal Support Agreement (DURSA) contacts page, and DURSA Joinder.

[Back to Top](#)

How does the Exchange Onboarding Team want Applicants to return application documents?

The Applicant returns the electronic documents by email to the Onboarding Team. Following the Onboarding Team's review, the Applicant sends a hard copy of the documents to NeHC (National eHealth Collaborative), ATTN: NwHIN Program Manager, 818 Connecticut Avenue, Suite 500, Washington, DC 20006.

[Back to Top](#)

Original documentation says the Applicant needs Local Registered Authority (LRA) forms. How does the Applicant get these forms?

Following Validation and testing completion, the Exchange Onboarding Team sends the Activation Packet to the Applicant for completion and submission. The LRA form is included in this packet.

[Back to Top](#)

What happens after the Applicant submits the application to the Exchange Onboarding Team and NeHC?

The Exchange Onboarding Team acknowledges receipt, forwards the packet to CC, and advises the Applicant of CC's intent to review the packet during its next meeting.

[Back to Top](#)

What happens after the CC meeting?

CC secretary sends the Applicant a welcome email to let the Applicant know it has been determined eligible to move into validation. The Exchange Onboarding Team is on the email distribution and reaches out to schedule the validation call.

[Back to Top](#)

When does the CC meet?

CC meets once a month.

[Back to Top](#)

What is the timeline for CC notification of eligibility determination?

Three-to-five business days.

[Back to Top](#)

Will the Applicant have regular calls with the Exchange Onboarding Team?

Yes, the Exchange Onboarding Team schedules the following calls: an introduction to Exchange Onboarding, before the start of the Validation Stage, Conformance Testing, Interop Testing, and a call at the start of the Activation Stage.

[Back to Top](#)

Labels parameters

Labels:

None



FAQs - Validation Process

- Added by Linda Toscano, last edited by Linda Toscano on May 02, 2011 (view change)

[Go to start of metadata](#)

view	7898978
----------------------	---------

- [What are the Applicant's key activities during the Validation Stage?](#)
- [Where can I get documentation supporting Onboarding testing?](#)
- [What is the timeline for Onboarding Validation?](#)
- [When an Applicant goes through Onboarding, what specs does testing set them up for implementing?](#)
- [Can an Applicant test for and implement any of the other available specs \(Document Submission, Health Information Event Messaging, or Web Services Registry\) during Onboarding? Or, would they have to do the basic Onboarding testing, get approved, and then retest for the added specs?](#)
- [What about testing future specs?](#)
- [Once an Applicant has received CC approval and is considered an Exchange Participant, what situation would warrant retesting?](#)
- [Can the Applicant do validation with dummy content?](#)
- [Is the Exchange Onboarding Team looking to validate the Applicant's Continuity of Care Document \(CCD\) or the transmission of the CCD?](#)
- [Does the Applicant have immediate access to the Interop Lab?](#)

What are the Applicant's key activities during the Validation Stage?

- Ensure gateway is production-ready
- Submit Validation Packet
- Conduct Connectivity Test
- Conduct Conformance Test and submit logs
- Conduct Interop Test and notify the Exchange Onboarding Team when complete

[Back to Top](#)

Where can I get documentation supporting Onboarding testing?

Click on the [Pre-Validation Testing Tool Kit](#) to access the following documents:

- Conducting Gateway-to-Gateway Exchanges before Entering Validation
- Ensuring Correct Configuration of Certificates
- Confirming Correct CONNECT Configuration
- Ensuring Services Registry Entry is Correct
- Ensuring Correct Formatting of Message Codes
- Using the NIST Tools to Review Messages for Conformance
- Avoiding Common Authorization Framework Conformance Errors

[Back to Top](#)

What is the timeline for Onboarding Validation?

Seven-to-eight weeks; three months for a conservative project plan.

[Back to Top](#)

When an Applicant goes through Onboarding, what specs does testing set them up for implementing?

Onboarding testing verifies an Applicant has successfully implemented the following specs:

- Messaging Framework 2.0
- Authorization Framework 2.0
- Patient Discovery 1.0
- Query for Documents 2.0
- Retrieve Documents 2.0

[Back to Top](#)

Can an Applicant test for and implement any of the other available specs (Document Submission, Health Information Event Messaging, or Web Services Registry) during Onboarding? Or, would they have to do the basic Onboarding testing, get approved, and then retest for the added specs?

Applicants can implement and/or test any of the available specs. However, the Exchange Onboarding Team encourages Applicants to focus on specs required by their federal partner (typically, basic Onboarding testing) so Applicants don't risk unnecessary delays to their Onboarding process.

[Back to Top](#)

What about testing future specs?

Following the Onboarding process, Applicants/Participants would need to return to the process and go back and retest for additional specs.

[Back to Top](#)

Once an Applicant has received CC approval and is considered an Exchange Participant, what situation would warrant retesting?

According to the DURSA, any material change to a Participant's system would require retesting.

[Back to Top](#)

Can the Applicant do validation with dummy content?

Yes, but the content must be a testing edge system (or a mirror).

[Back to Top](#)

Is the Exchange Onboarding Team looking to validate the Applicant's Continuity of Care Document (CCD) or the transmission of the CCD?

Transmission of the CCD.

[Back to Top](#)

Does the Applicant have immediate access to the Interop Lab?

The Exchange Onboarding Team grants access following satisfactory completion of Conformance Testing.



FAQs - All About Certs

- Added by [Linda Toscano](#), last edited by [Linda Toscano](#) on May 02, 2011 ([view change](#))

[Go to start of metadata](#)

view	7898978
------	---------

- [**What are the roles of the Local Registration Authority \(LRA\), administrator, and subscriber?**](#)
- [**When do validation and production certificates expire?**](#)
- [**How do Applicants renew certificates?**](#)
- [**Can the Exchange Onboarding Team provide guidance and tips to assist with the administration of the Certification Authority \(CA\) and certificate lifecycle management?**](#)
- [**On the Administrator Login screen, is the check mark shown in the Remember Entrust Desktop Security Store File Name field required?**](#)
- [**The Create Account screen displays multiple options. Which option should I choose when issuing a server certificate?**](#)
- [**On the Create Account screen, whose email address should I include in the Notification Email field?**](#)
- [**Is there a specific format for an email address?**](#)
- [**On the Create Account - Complete screen, the Reference Number and Authorization Code show that they expire 14 days after the day they were created, but the server certificate expires more than 90 days from the creation date. Why is this?**](#)
- [**On the Edit Account - Search screen, what options can I use to search for an Applicant/Organization?**](#)

What are the roles of the Local Registration Authority (LRA), administrator, and subscriber?

An administrator, also known as a Local Registration Authority (LRA), is the person authorized by his/her organization and the Certification Authority (CA) to make requests to the CA and to provide certificate lifecycle management. The administrator is a standard user who can create a subscriber. A subscriber is a standard user only. An administrator has several important duties, which include making requests to the CA to issue digital certificates to users and recovering, disabling, moving, or deleting users.

[Back to Top](#)

When do validation and production certificates expire?

Validation certificates expire in 90 days; production certificates expire one year from date of issue.

[Back to Top](#)

How do Applicants renew certificates?

Applicants should contact the Exchange Onboarding Team at onc.exchangeinfo@hhs.gov for assistance.

[Back to Top](#)

Can the Exchange Onboarding Team provide guidance and tips to assist with the administration of the Certification Authority (CA) and certificate lifecycle management?

The following screen shots, questions, and answers provide a collection gathered from Applicants as they established their CA. If you have additional questions, send them to the Exchange Onboarding Team at onc.exchangeinfo@hhs.gov. onc.exchangeinfo@hhs.gov

[Back to Top](#)

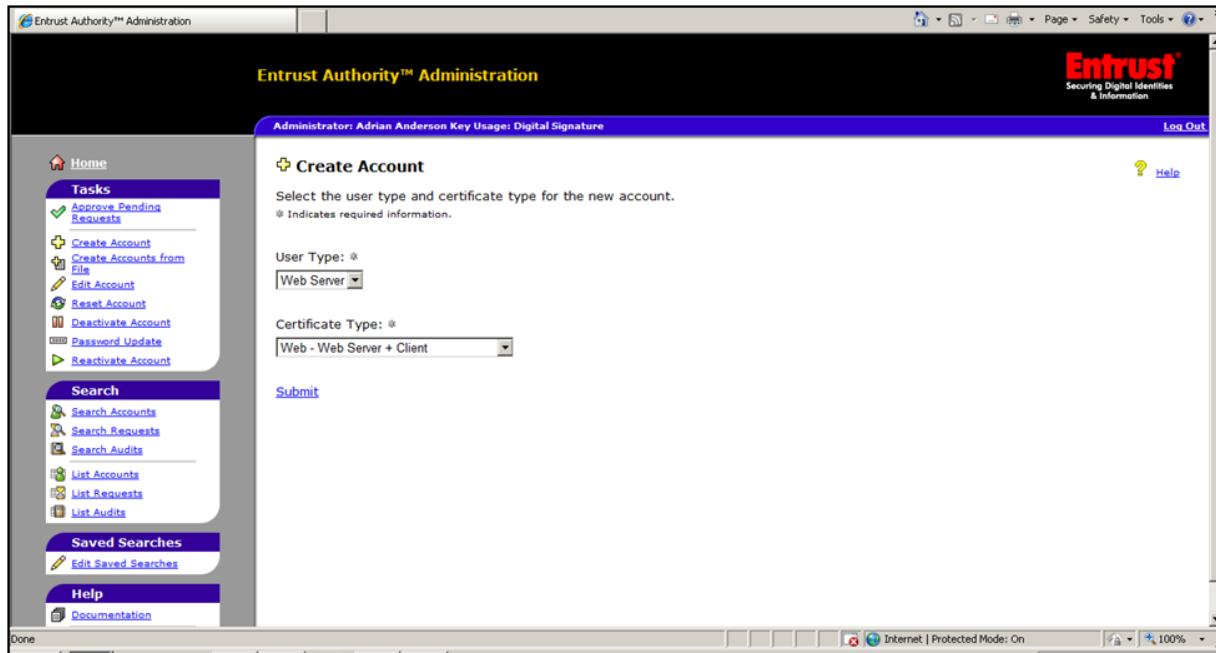
On the Administrator Login screen, is the check mark shown in the Remember Entrust Desktop Security Store File Name field required?

The screenshot shows a web browser window with the URL <https://nfitestadmin.managed.entrust.com/AdminSer...> in the address bar. The page title is "Entrust NFI Test Administration". On the left, there's a sidebar with links: "Need help logging in?", "Create Entrust digital ID", "Recover Entrust digital ID", "Browser requirements", and "Browser Check". Below these is a "français" link. The main content area has a purple header "Administrator Login - Entrust Desktop Security Store". It says "Log in using your Entrust Desktop Security Store (.epf)". Below that, it asks "Please enter your security store name and password and click Log in.". There are two input fields: "Entrust Desktop Security Store File Name:" with a "Browse..." button and a note "Click Browse... to locate your security store.", and "Password:". Below these is a checked checkbox "Remember Entrust Desktop Security Store File Name". At the bottom are "Log in" and "Clear" buttons, and a link "Log in with my [Third-party security store](#) (Microsoft® Windows® security framework)". The status bar at the bottom right shows "Internet" and "100%".

The box is checked by default upon the page loading. This has no affect on the administrator login.

[Back to Top](#)

The Create Account screen displays multiple options. Which option should I choose when issuing a server certificate?

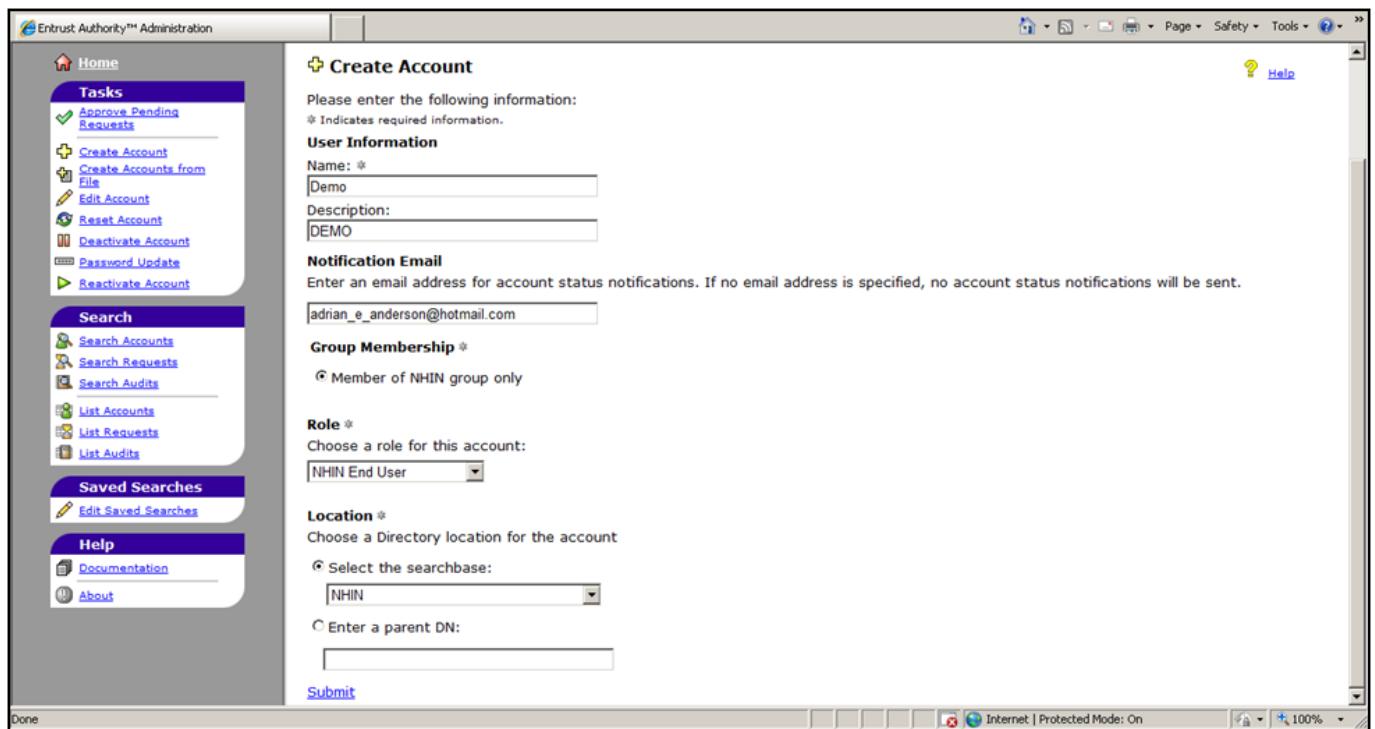


Unless you are creating a certificate for an additional administrator you would select the following:

- User Type: *Web Server*
- Certificate Type: *Web – Web Server + Client*

[Back to Top](#)

On the Create Account screen, whose email address should I include in the Notification Email field?



This should include the email of the Primary Contact as listed on the request form.

[Back to Top](#)

Is there a specific format for an email address?

The email address should be in standard email format. Ex: demo@demo.com

[Back to Top](#)

On the Create Account - Complete screen, the Reference Number and Authorization Code show that they expire 14 days after the day they were created, but the server certificate expires more than 90 days from the creation date. Why is this?

The screenshot shows the Entrust Authority Administration interface. On the left, a sidebar lists various tasks such as Approve Pending Requests, Create Account, Edit Account, and Reset Account. The main content area is titled 'Create Account - Complete' and shows a table of account details:

Name	Notification Email	Group	Role	Status
Demo	adrian_e_anderson@hotmail.com	NHIN	NHIN End User	New

Below the table, a section titled 'Activation Codes' contains the following information:

Activation Codes

Securely distribute these codes to the account holder:

Name: cn=Demo,ou=NHIN,o=HHS-ONC,c=US
Reference Number: 52528623
Authorization Code: 4P8P-DRDN-03C4
Codes were created on: Friday, May 07, 2010 11:58:08 AM
Codes will expire on: Friday, May 21, 2010 11:58:08 AM

[Create Local Digital ID](#) Create Digital ID for this account that will be saved on this computer in an .epf file
[Create Third-Party Security Store](#) Create Digital ID for this account that will be saved in Microsoft Windows security store on this computer or on a smart card

These codes reflect the period of time in which the organization has to install the certificate. If the server install does not occur before their expiration, the Exchange Onboarding Team can create new codes and send them to the Organization.

[Back to Top](#)

On the Edit Account - Search screen, what options can I use to search for an Applicant/Organization?

Administrator: entrust

Edit Account - Search

To edit an account, you must first perform a search
Enter the appropriate search criteria in the following fields.
Note: If no search criteria is entered, the search returns all entries.
Selecting - NA - excludes the field from the search criteria.

Name	<input type="text"/>	Enter part or all of the account name
Current State	<input type="text"/> -- NA --	
Role	<input type="text"/> -- NA --	
Group	<input checked="" type="radio"/> Member of any group <input type="radio"/> Member of all current and future groups <input type="radio"/> Member of selected group <input type="text"/> -- NA --	
Notification Email	<input type="text"/>	
Maximum number of results	<input type="text"/> 100	
<input type="button" value="Submit"/>		

Any of the options can be selected in combination or separately when looking for an Applicant/Organization. If none of the information is known, the fields may be left blank and the Submit button can be selected which lists ALL Organizations and Administrators.

[Back to Top](#)

Labels parameters

<input type="text"/> http://jira.sifframe	<input type="text"/> 10584249	<input type="text"/> OBTI
Labels:		
None		
<input type="checkbox"/> Are you sure you	<input type="button" value="Click to toggle the"/>	<input type="button" value="Cancel"/>



Acronyms and Glossary of Terms

Move Page ñ Ac	Set Page Location	Move	Cancel	Click to select the	Search
Recently View ed	There w ere no re	Know n Location	The specified pag	Brow se	Error reading the
You could try re	HTTP Status	You must make a	Failed to retrieve	There w ere no p	Show ing {0}<
Move failed. Ther	You cannot move	Acronyms and G	Home		OBTI
Exchange Onboa	You cannot move	Page Ordering	Back	Reorder	Move
OBTI	OBTI	Skip to end of metadata			

- Page restrictions apply
- Added by [Linda Toscano](#), last edited by [Linda Toscano](#) on Apr 07, 2011 ([view change](#))

[Go to start of metadata](#)

view	7407241
------	---------

Acronym / Term	Description
Activation Stage	Stage 3 of the Onboarding process. Enables the Applicant to exchange data using Nationwide Health Information Network standards, services, and policies.
Active Test	Set of test scenarios currently executed by the Applicant.
Aegis	Developed and provides assistance to maintain the Nationwide Health Information Network Interoperability Test Lab.
ALM	Application Lifecycle Management
API	Application Program Interface
Applicant	Entity that has developed a technical solution (gateway) it wishes to use to exchange data across the Nationwide Health Information Network; often referred to as organizations, customers, and/or entities. Referred to as Applicant from the time it enters the Onboarding process through the time of approval from CC.
Applicant System	The Applicant's technical solution, which the Applicant is operating and using to undergo Validation testing.
Applicant Test Lead	Individual (user) conducting testing on behalf of the Applicant.
ARRA	American Recovery and Reinvestment Act of 2009. Commonly referred to as the Stimulus or the Recovery Act, it is an economic stimulus package enacted by the 111 th U.S. Congress in February 2009.

ATO	Authority to Operate
Attachment (testing)	Log or other file attached to a scenario for manual verification.
CA	Certification Authority. Issues the digital certificates certifying ownership of a public key by the Applicant.
CC	Nationwide Health Information Network Coordinating Committee. Provided authority by Exchange Participants to establish and maintain the set of policies, legal agreements, and accountability measures for those entities exchanging data in production today using the Exchange. Previously referred to as NCC.
CCD	Continuity of Care Document
CCR	Continuity of Care Record
Closed Test (or Previous Test)	Any of the sets of test scenarios that are no longer active – the Applicant has stopped executing that set of test scenarios.
Conditional Acceptance	Applicant/Participant must be able to begin exchanging data in production via the Nationwide Health Information Network within 120 days following notice from CC.
CONNECT	FHA CONNECT is an open source software and community that promotes IT interoperability in the U.S. health care system.
COTR	Contracting Officer Technical Representative
Cross Gateway Query	Sends a query from one community to another to identify the location of health care information satisfying specific constraints.
Cross Gateway Retrieve	Requests the retrieval of a specific set of health care information (a document or documents) from another community.
DHIMS	Defense Health Information Management System. Provides a trusted, comprehensive health information management system that seamlessly captures, manages, and shares health information from the Theater of Operations to the home front and beyond in support of our service members and our military family.
DURSA	Data Use and Reciprocal Support Agreement. Comprehensive agreement to govern the exchange of health data through the Nationwide Health Information Network. A multi-party agreement, a single agreement that establishes the rules of engagement and obligations to which all Participants agree and that all Participants sign as a condition of joining the community.
EHR	Electronic Health Record

EMR	Electronic Medical Record
ESB	Enterprise Service Bus
Exchange Onboarding Team	The Office of the National Coordinator for Health Information Technology (ONC) and the Exchange Onboarding Contractor (Exchange Onboarding Team or Onboarding Team) offer guidance and assistance to Applicants through the three stages of the Onboarding process.
FAQ	Frequently Asked Question
FHA	Federal Health Architecture. An E-Government Line of Business initiative managed by the Office of the National Coordinator for Health IT.
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
Functional Test	System's ability to ensure the required activities takes place appropriately according to the requirements. Examples of this type of conformance include ensuring correct routing of information, actual delivery of information, and employment of appropriate security measures.
HIE	Health Information Exchange. Mobilization of health care information electronically across Applicants within a region, community, or hospital system.
HIT	Health Information Technology. Umbrella framework to describe the comprehensive management of health information and its secure exchange among consumers, providers, government, quality entities, and insurers.
HITSP	Healthcare Information Technology Standards Panel. Serves as a cooperative partnership between the public and private sectors for the purpose of achieving a widely accepted and useful set of standards specifically to enable and support widespread interoperability among healthcare software applications, as they will interact in a local, regional, and national health information network for the U.S.
HHS	U.S. Department of Health and Human Services. Principal agency for protecting the health of all Americans and providing essential human services, especially for those who are least able to help themselves.
Initiating Gateway	Initiates an inter-community communication across the Nationwide Health Information Network.
Interop Lab	The informal name of the Nationwide Health Information Network Interoperability Test Platform.

IT	Information Technology
Logical Conformance Test	System's ability to ensure the semantically-correct content of the information being exchanged accurately fulfills the intention of the exchange. Examples of this type of conformance include queries for specific information engendering appropriate responses in kind (e.g., ensuring a request for a lab result is not fulfilled with a medication history, or referencing the wrong patient).
LRA	Local Registered Authority. Person authorized by the Applicant and the CA to make requests to the CA to provide certificate lifecycle management. A standard user who can create a subscriber. Makes requests to CA to issue digital certificates to users and can recover, disable, move, and delete users.
MPI	Master Patient Index
Nationwide Health Information Network	The Nationwide Health Information Network is a set of policies, standards, and services that enable Participants to use the Internet for secure and meaningful exchange of health information to improve health and health care.
Nationwide Health Information Network Compliant Gateway	Any compliant instantiation of Nationwide Health Information Network final production specifications and services.
Nationwide Health Information Network Exchange	<p>The Nationwide Health Information Network Exchange (Exchange) is a confederation of trusted entities, bound by a mission and a common framework of trust, to securely exchange health information using Nationwide Health Information Network standards and specifications. It is a diverse set of entities facilitating information exchange with a broad set of users, systems, geography, or community:</p> <ul style="list-style-type: none"> • Internet-based, using common implementation of standards and specifications with secure transport • Tested for conformance and interoperability • Enables valid, trusted entities to participate • Signed trust agreement that allocates responsibilities and accountability to protect information exchanged • Digital credentials issued to permit only approved Participants to exchange data with other members • Committee structures to oversee and support activities
Nationwide Health Information Network Service Set	A role-related grouping of gateway services under which the Applicant may choose to define its intended interaction on the Nationwide Health Information Network, and thus the scope of its interoperability validation.
Nationwide Health Information Network Use Case	Those groups of gateway system functionality, as captured by the Nationwide Health Information Network Spec Factory, which an HIE participant on the Nationwide Health Information Network may be capable of performing.
NCC	Nationwide Health Information Network Coordinating Committee. Provided

	authority by Exchange Participants to establish and maintain the set of policies, legal agreements, and accountability measures for those entities exchanging data in production today using the Exchange. Currently referred to as CC.
NDMS	National Disaster Medical System. Manages the federal government's response to major emergencies and disasters.
NHIE	Nationwide Health Information Network Health Information Exchange
NHIN	Former acronym for Nationwide Health Information Network. Do not use this acronym; ONC is in the process of changing this identifier.
NIST	National Institute of Standards and Technology. A non-regulatory federal agency within the U.S. Department of Commerce. The Exchange Onboarding Team coordinates with NIST to run conformance testing and validate testing results.
NTC	Nationwide Health Information Network Technical Committee. Focuses on architectural and technical issues such as approval of new or modified technical requirements, specifications, and testing for the Exchange. Currently referred to as TC.
OID	Object Identifier or Home Community ID
Onboarding Process	Activities Applicants need to complete as they move through the three Nationwide Health Information Network Onboarding stages to become Participants of the Nationwide Health Information Network Exchange.
ONC	Office of the National Coordinator for Health Information Technology. Principal federal entity charged with coordination of nationwide efforts to implement and use the most advanced health IT and the electronic exchange of health information.
OS	Operating System
Participant	Term used to identify Applicants (organizations, customers, entities) engaged in the Nationwide Health Information Network Exchange (following CC membership approval).
PCA	Production Certificate Authority. Operations and Infrastructure Team logs into the PCA to create a production account for the Applicant.
PCAF	Production Certificate Authority Form. Following conditional acceptance, the Operations and Infrastructure Team uses the completed PCAF to create the Applicant's PCA account.
Performance and Usability Test	System's employment of appropriate and reasonable methods to fulfill the requirements. Examples of this type of conformance include fulfilling service-level agreements for availability, responsiveness, and transaction levels that ensure the overall usability of the system.
PMO	Program Management Office
Previous Test (or Closed Test)	Any of the sets of test scenarios that are no longer active – the Applicant has stopped executing that set of test scenarios.

PSC	Program Support Center. Provides support services to all components of HHS and other federal government agencies worldwide.
PSRF	Production Services Registry Form. Applicant submits the completed PSRF to the Operations and Infrastructure Team to configure the Applicant's Production Services Registry information in UDDI.
Qualification Stage	Stage 1 of the Onboarding process. Ensures the Applicant meets the eligibility criteria to begin using Nationwide Health Information Network standards, services, and policies to securely exchange health information over the Internet with Applicants already engaged in exchanges.
Responding Gateway	Participation in an inter-community communication across the Nationwide Health Information Network initiated by another gateway.
RI	Reference Implementation. The software example of the Nationwide Health Information Network specification. The Applicant's system interacts with the RI for interoperability testing.
Robustness and Stability Test	System's ability to appropriately handle exceptional operational conditions. Examples of this type of conformance include graceful handling of boundary conditions of correct operation (e.g., high loads), negative cases, edge-system malfunction, and attempted security breach.
S&I	Standards and Interoperability
SDK	Software Development Kit
Semantic Conformance Test	System's ability to ensure the syntactically-correct content of the information being exchanged accurately represents the intended concepts. Examples of this type of conformance include referential-integrity checking of informational elements against prescribed vocabulary standards (e.g., a given 5-digit code is actually valid within the endorsed version of the ICD-9 code set).
SOW	Statement of Work
SRT	Stakeholder Request Tracker
SSL	Secure Sockets Layer
Syntactic Conformance Test	System's ability to ensure the correct form of the information being exchanged based on required standards and constraints. Examples of this type of conformance include adherence to the definitions of message or document specifications, such as element length, element order, and inclusion of required elements.
T&R	Tools and Repository
TDL	Technical Direction Letter
TC	Technical Committee. Focuses on architectural and technical issues such as approval of new or modified technical requirements, specifications, and testing for the Exchange. Previously referred to as NTC.
Test Artifacts	System logs created during the Conformance Testing process and submitted by

	the Applicant to the Operations and Infrastructure Team.
Test Case	One path through a Nationwide Health Information Network use case, which the Nationwide Health Information Network Interoperability Test Platform verifies. The test case includes a set of test inputs, execution conditions, and expected results, identified for the purpose of making an evaluation of an Applicant's system with the Nationwide Health Information Network interoperability and for driving the creation of test scenarios.
Test Data	Set(s) of anonymous patient data, which are known to correctly exercise the Nationwide Health Information Network services to produce expected outcomes. Test data is an essential component of both conformance and interoperability testing.
Test Results	Within the Nationwide Health Information Network Interoperability Test Platform Web application, the grouping of a set of runs of test scenarios and test cases for an Applicant, including any attached evidence. The system assigns each set of test results a unique execution ID. Each Applicant may have one set of active test results and may retain previous sets of test results. Applicant may submit any set of test results for validation. An Applicant's setup information may not change within a set of test results, but may be different between test results.
Test Scenario	A set of functionally-related test cases, strung together to exercise a user-relevant business case, which the Nationwide Health Information Network Interoperability Test Platform verifies. The test scenario includes step-by-step instructions (test procedures) that realize a test and enable its execution, including those elements of the test scenario executed by automated elements of the Nationwide Health Information Network Interoperability Test Platform.
Test Scenario – Initiator	An Interop Lab test scenario where the Applicant's system performs in the role of the initiating gateway.
Test Scenario – Responder	An Interop Lab test scenario where the Applicant's system performs in the role of the responding gateway.
TO	Task Order
UDDI	Universal Description Discovery Interface. The selected platform for the Nationwide Health Information Exchange (NHIE) Service Registry is based on the UDDI version 3.0.2 specification.
Validation Stage	Stage 2 of the Onboarding process. Demonstrates the Applicant's exchange complies with Nationwide Health Information Network specifications and verifies the Applicant's system can interact with other Participant systems.
VCA	Validation Certificate Authority. Exchange Onboarding Team logs into VCA to create a validation account for the Applicant.
VCAF	Validation Certificate Authority Form. Following membership eligibility, the Exchange Onboarding Team uses the completed VCAF to create the Applicant's VCA account.
VLER	Virtual Lifetime Electronic Record

VSRF	Validation Services Registry Form. Form the Applicant completes identifying metadata including services to be validated, point of contact, and Community ID. Exchange Onboarding Team configures UDDI with this information.
WBS	Work Breakdown Structure

Labels parameters

<http://jira.siframe>

7406132

OBTI

Labels:

None

Are you sure you

Click to toggle the

Cancel



FAQs - Activation Process

Added by Linda Toscano, last edited by Linda Toscano on May 02, 2011 ([view change](#))

[Go to start of metadata](#)

view	7898978
------	---------

- [When does the Applicant enter the Activation Stage?](#)
- [What are the Applicant's key activities during the Activation Stage?](#)
- [What is meant by conditional approval?](#)
- [What happens if the Applicant/Participant cannot begin exchanging data within 120 days?](#)

When does the Applicant enter the Activation Stage?

After the Onboarding Team submits the Validation Summary Report to the CC, the Applicant enters the Activation Stage.

[Back to Top](#)

What are the Applicant's key activities during the Activation Stage?

- Receive conditional approval
- Start exchanging data within 120 days

[Back to Top](#)

What is meant by conditional approval?

Conditional approval means the Applicant/Participant must begin exchanging data in production via the Nationwide Health Information Network Exchange within 120 days following notice from CC.

[Back to Top](#)

What happens if the Applicant/Participant cannot begin exchanging data within 120 days?

If the Applicant/Participant cannot go live within 120 days, it submits an email requesting an extension to the Exchange Onboarding Team. The Exchange Onboarding Team processes the request with the CC.

[Back to Top](#)

Labels parameters	http://jira.siframe	10584265	OBTI
-------------------	---	----------	------

Labels:

None

Are you sure you	Click to toggle the	Cancel
------------------	-------------------------------------	------------------------

Appendix F. MultiState E-Mall Operating Rules

Attachment 1: Version 1 Operating Rules

Attachment 2: Version 2 Operating Rules

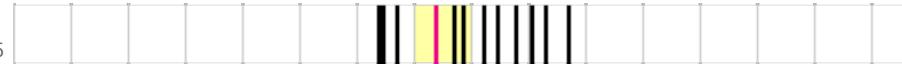
Attachment 3: Version 3 Operating Rules

Attachment 4: Technology Hypothesis and Analysis

Attachment 5: Legal/Business Hypothesis and Analysis

[12 captures](#)

6 May 02 - 21 Sep 05



SEP	MAY	SEP
	22	
2002	2003	2004

[Close](#)[Help](#)

Operating Rules

*For use in the Electronic Procurement Project
Known as the "Multi-State E-Mall™"*

Version 1.0, October 8, 1998
The Current Version of this Document is Available at
<http://e-mall.osd.state.ma.us/or>

COPYRIGHT NOTICE

Copyright © 1998 by the Commonwealth of Massachusetts in its capacity as Policy Authority for the Multi-State E-Mall. All rights reserved. Permission to reproduce this document is hereby granted provided that the following limitations on this right are observed: (1) all copies must clearly indicate that this work is published by and attributed to the Commonwealth of Massachusetts in its capacity as Policy Authority for the Multi-State E-Mall; and (2) all copies must include this notice of copyright.

[A. Scope](#)

[A.1. General](#)

[A.2. Application of these Operating Rules](#)

[A.3. Open Buying on the Internet](#)

[A.4. Contact Information](#)

[B. Authentication: In General](#)

[B.1. Issuance, Use, Modification and Termination of User Name and Passwords](#)

[B.2. Use of SSL](#)

[B.3. Use of S/MIME](#)

[B.4. Use of Fax, Telephone, U.S. Mail, Commercial Couriers, and Unsecured/Unauthenticated E-Mail](#)

[B.4.1. General](#)

[B.4.2. Communication of Agreements and Related Data](#)

[B.4.3. Other Communications](#)

[C. Authentication: Certificate Policy](#)

[C.1. Introduction](#)

[C.2. General Provisions](#)

[C.3. Identification and Authentication](#)

[C.4. Operational Requirements](#)

[C.5. Physical, Procedural, and Personnel Security Controls](#)

[C.6. Technical Security Controls](#)

[C.7. Certificate and CRL Profiles](#)

[C.8. Specification Administration](#)

[D. Roles, Functions and Authorization of Participating Parties](#)

[D.1. General Concepts](#)

[D.2. Role: Policy Authority \(E-Mall Team/Principal\)](#)

[D.3. Role: Business Administrator \(E-Mall Team/Admin.\)](#)

[D.4. Role: Operations Administrator \(E-Mall Team/Admin.\)](#)

[D.5. Role: State Partner MOU Signatory \(State Partner/Principal\)](#)

[D.6. Role: State Coordinator \(State Partner/Contact\)](#)

[D.7. Role: Shopper \(State Partner/User\)](#)

[D.8. Role: Operational Approver \(State Partner/User\)](#)

[D.9. Role: Financial Approver \(State Partner/User\)](#)

[D.10. Role: Receiver \(State Partner/User\)](#)

[D.11. Role: Supplier Partner MOU Signatory \(Supplier Partner/Principal\)](#)

[D.12. Role: Supplier Coordinator \(Supplier Partner/Contact\)](#)

[D.13. Role: Certificate Manufacturer](#)

[D.14. Role: Solution Providers](#)

E. Technical Requirements

[E.1. User Personal Computer](#)

[E.1.1. Internet and World Wide Web Connectivity](#)

[E.1.2. Hardware](#)

[E.1.3. Software](#)

[E.2. Supplier Partner](#)

[E.3. Physical Security of Computing and Network Resources](#)

F. Duties and Obligations of the Parties

[F.1. Electronic Offer and Acceptance](#)

[F.1.1. OBI Order Request](#)

[F.1.2. OBI Order](#)

[F.2. Notice](#)

[F.3. Participation Agreements](#)

[F.4. Confidentiality](#)

[F.5. Intellectual Property](#)

A. Scope

A.1. General

The Multi-State E-Mall Pilot (E-Mall) is an Extranet procurement Web site, hosted by the Commonwealth of Massachusetts and available to participating states. The E-Mall web site provides links to qualified supplier "storefronts" or catalogs, where state procurement staff can browse, shop and create requisitions. Public Key Certificate technology coupled with user name and password ensure that only authorized procurement staff can submit approved OBI Orders to the approved suppliers.

A.2. Application of these Operating Rules

These Operating Rules apply to every participant in the E-Mall. No party may play any role or otherwise act as a participant in the E-Mall without signing a Participation Agreement. Depending on the role a given party plays

(i.e. User, Supplier, Administrator, etc.) a different Participation Agreement with special terms may be required.

A.3. Open Buying on the Internet

The E-Mall is based upon the Open Buying on the Internet (OBI) specification. OBI is an emerging standard that defines the technical requirements for conducting business over the Internet from buyer to seller.

The following definition is copied from the OBI web site:

The OBI standard is an open, flexible design for business-to-business Internet commerce solutions. It is intended for the high-volume, low-dollar transactions that account for 80% of most organizations' purchasing activities. Version 1.0 of the standard document contains an architecture, as well as technical specifications and guidelines. OBI is not a product or a service; it is a freely available standard which any organization can obtain and use.

Information about the OBI standard is available at the website <http://www.openbuy.org>. Version 1.0 and Version 1.1 of the OBI technical specifications are available from this site.

A.4. Contact Information

The Policy Authority promulgating these Operating Rules is the Commonwealth of Massachusetts. A current version of these Operating Rules and related information is available at <http://e-mall.osd.state.ma.us/> or. Signed Participation Agreements of each party performing a role under these Operating Rules are on file with the Policy Authority. For purposes of business communications, parties performing a role in the E-Mall may contact:

Nancy Burke, E-Mall Project Manager,
Commonwealth of Massachusetts, Operational Services Division
One Ashburton Place, Room 1017
Boston, MA 02108
nancy.burke@state.ma.us, 617.727.7500

For questions or comments specifically relating to these Operating Rules, parties performing a role in the E-Mall may contact:

Daniel Greenwood, Deputy General Counsel, Information Technology Division & E-Mall Steering Member
Commonwealth of Massachusetts
One Ashburton Place, Room 801
Boston, MA 02108
dan.greenwood@state.ma.us, 617.973.0071

B. Authentication: In General

B.1. Issuance, Use, Modification and Termination of User Name and Passwords

A Username and Password must be supplied by every User of the E-Mall Server accessing a non-public portion of the system. No User may share or otherwise reveal their Password. Any suspicion that a Password has been compromised must be immediately communicated to the State Coordinator for that user. A Password may be re-set in the event that an authorized user forgets the Password. Upon proper notification by an authorized State Coordinator under these Operating Rules and relevant implementing agreements, a User access to the E-Mall will be terminated and the respective Username and Password combination for a terminated User will no longer be valid.

B.2. Use of SSL

Every person accessing any non-public portion of the E-Mall server must use the Secure Sockets Layer (SSL) protocol. The SSL protocol will be used to authenticate and secure certain communications between Supplier servers and the E-Mall server as well as to encrypt certain session between the browser of a user and the E-Mall server and authenticate the identity of authorized E-Mall users. A web session invoking version 3.x of the SSL protocol requires use of a duly issued Public Key Certificate within the browser of an E-Mall user.

B.3. Use of S/MIME

A Pilot Participant who is duly issued a Public Key Certificate for use in the E-Mall may use that Certificate to "sign" e-mail to another participant. In addition, a Pilot Participant may use the duly issued E-Mall Certificate of another participant to encrypt e-mail using the S/MIME standard, provided each person uses an interoperable e-mail client. In some cases, as determined by an E-Mall Administrator, use of S/MIME may be requested or required to assure official communications via e-mail are confidential and/or authenticatable.

B.4. Use of Fax, Telephone, U.S. Mail, Commercial Couriers, and Unsecured/Unauthenticated E-Mail

B.4.1. General

Access as a User or Administrator to the E-Mall server will require a valid Username and Password as well as a recognized Public Key Certificate. However, many other communications channels will be used for various

other purposes throughout the term of this pilot. It is recognized that implementation of a production system will require greater specificity regarding permitted and prohibited methods of communication and corresponding authentication depending on the purposes of the communications. It is intended that experience gained through this pilot process will demonstrate appropriate guidelines. For purposes of the pilot, however, it is expected that most non-critical communications will occur between pilot participants via phone and e-mail.

B.4.2. Communication of Agreements and Related Data

Communication of the implementing agreements under these Operating Rules and related User designation and authorization data requires greater specificity. Until and unless otherwise specified in future versions of these Operating Rules, delivery of all completed forms, agreements and related data, including all designation of roles and authorities for users of the E-Mall system must be communicated via:

- * Fax, U.S. Mail or Commercial Couriers, or
- * Upon prior approval by the E-Mall Business Coordinator, S/MIME Signed E-Mail, signed by private key corresponding to a validly issued Public Key Certificate for the E-Mall Pilot

Until and unless return receipt is received by phone call back or other agreed methods, sender must consider that such data has not been successfully transmitted.

B.4.3. Other Communications

Unless otherwise specified in these Operating Rules, communications may be conducted by any reasonable means that are appropriate for the purpose.

C. Authentication: Certificate Policy

For purposes of the Multi-State E-Mall Pilot, a Public Key Certificate is a computer-based record which:

- (a) identifies the entity or brand associated with issuance of it;
- (b) names or identifies the person or device associated with the corresponding private key;
- (c) contains the public key corresponding to that private key of that person or device; and
- (d) is digitally signed by the Certificate Manufacturer that creates the Certificate.

In transacting business over the Internet, it is critical that both the seller and buyer be assured that the transactions exchanged are secure. Public key encryption coupled with Public Key Certificates can

provide part of this security by ensuring the confidentiality and/or authentication of electronic business exchanges. When Public Key Certificates are attached to transactions, users on each side of a purchase can be assured of who the message came from and that it was not tampered with. The E-Mall pilot uses Certificates to bolster the authentication provided by the Password and Username in the E-Mall system. A Certificate is not, by itself, sufficient to gain access or perform any transactions within the E-Mall system.

Public Key Certificates are used to authenticate Web servers and their clients via protocols such as SSL 3.0. A Public Key Certificate is analogous to an identification card issued by a third party. Each User participating in the E-Mall pilot must have at least one Public Key Certificate. Certificates will be issued at no cost by a designated and trusted third party known as a Certificate Manufacturer (CM). The CM will issue a Certificate to Users who have been identified by their respective State Coordinators and accepted by the E-Mall Administrator.

The browser specifications as noted in the technical requirements' section accommodates the use of Public Key Certificates.

A technical resource for each State Partner will be needed to install the Certificates for each user. This technical resource must have an adequate understanding of the technical, operational and legal requirements and responsibilities associated with managing, issuing and maintaining Public Key Certificates.

This Certificate Policy section of these Operating Rules governs creation, delivery and other aspects of the Certificate Manufacturing process as well as the proper use of Public Key Certificates. This section follows the format of the Internet Engineering Task Force PKIX Part 4 Framework (available at <http://www.ietf.org/internet-drafts/draft-ietf-pkix-ipki-part4-03.txt>) and is in general accord with the guidance provided by Version 1.0 of the draft "Guidelines for Constructing Policies Governing the Use of Identity-Based Public Key Certificates" by the Certificate Authority Ratings and Trust Task Force of the Internet Council of the National Automated Clearinghouse Association (available at <http://internetcouncil.nacha.org/CARAT/>).

NOTE: The public release of Version 1.0 of these Operating Rules will not contain the Certificate Policy due to concern for maintaining control over disclosure of information revealing sensitive security processes. Parties that have a need to know some or all of the information contained within the Certificate Policy may request such information from the Policy Authority. For the purpose of indicating the general form and scope of the Certificate Policy, certain section headings have not been redacted, but no content will be published under any heading in this section.

C.1. Introduction

Note: Content redacted from this draft for purpose of maintaining security of sensitive processes.

C.2. General Provisions

Note: Content redacted from this draft for purpose of maintaining security of sensitive processes.

C.3. Identification and Authentication

Note: Content redacted from this draft for purpose of maintaining security of sensitive processes.

C.4. Operational Requirements

Note: Content redacted from this draft for purpose of maintaining security of sensitive processes.

C.5. Physical, Procedural, and Personnel Security Controls

Note: Content redacted from this draft for purpose of maintaining security of sensitive processes.

C.6. Technical Security Controls

Note: Content redacted from this draft for purpose of maintaining security of sensitive processes.

C.7. Certificate and CRL Profiles

Note: Content redacted from this draft for purpose of maintaining security of sensitive processes.

C.8. Specification Administration

Note: Content redacted from this draft for purpose of maintaining security of sensitive processes.

D. Roles, Functions and Authorization of Participating Parties

D.1. General Concepts

Party: A legal entity. A natural person can be a party. Certain organizations, such as corporations, trusts and governments may also be recognized as a legal person and therefore can be a party.

Each party will be identified by name in relevant documents and agreements.

Functions: The particular duties and obligations entered into within a business and technical system. A Party will perform several functions. These sets of functions are put together based on technical, legal and business needs of the enterprise.

Role: Each *role* is named according to the nature of the functions in each set. By naming roles, and associating functions with roles, it is not suggested that in every business model sets of functions will be divided in the same manner as here. Further, it is not suggested that there will be one-to-one correlation between roles and parties. Indeed, it is envisioned that a *party* may perform one or more roles. The purpose for naming roles in this document is primarily to provide a vocabulary for creating modular parts that can be performed by a given party entering the E-Mall system and to organize the obligations and related documents associated with a given party.

For example, rather than call the administration role by the name Commonwealth of Massachusetts, it is convenient to name it based on the relevant suite of functions so that any party could perform the role more easily within the system of documents and business arrangements herein. Similarly, while particular parties perform the role of service providers, there may be additional and/or different parties playing those roles in the future, hence we use terms like "solution provider" and "Certificate Manufacturer." The usage of roles under these Operating Rules is intended to reflect and support the potential evolution of this project from a relatively closed and small pilot to a scalable production system in which many more parties may perform the roles noted herein.

Documents and Agreements: In many cases, a party will have to sign a document or submit a particular form as part of the functions associated with a given role. These documents might be contracts, memoranda of understanding, applications, reports and so on. These documents hold a particular legal importance as the glue that hold together parties, roles and functions in a predictable and enforceable system.

D.2. Role: Policy Authority (E-Mall Team/Principal)

Functions

- * Sponsor of the Multi-State E-Mall Pilot;
- * Makes all policy decisions related to the Multi-State E-Mall Pilot;
- * Designates, and delegates appropriate authority to E-Mall Administrators;
- * Agrees to accept the MOU of State Partners; and

- * Selects and arranges for technology products and services necessary for hosting the E-Mall OBI-Compliant server on behalf of State Partners as buying organizations.

Relevant Documents and Agreements

- * Promulgates, or delegates authority to promulgate, these **Operating Rules** and all other official agreements or documents related to the Multi-State E-Mall.

D.3. Role: Business Administrator (E-Mall Team/Admin.)

Functions

- * Receives names/contact data of each State Coordinator from each designated Partner State (from person(s) who signed the MOU);
- * Gives the State Coordinator contact information to the Operations Administrator;
- * Reviews and submits for processing all security related applications and forms, including those related to Public Key Certificates, which are forwarded by the State Coordinator; and
- * Securely maintains all applications and forms for related Public Key Certificate requests before and after processing by the E-Mall Operations Administrator.

Relevant Documents and Agreements

- * Agrees to abide by these **Operating Rules**.
- * Must sign **Business Administrator Agreement**.

D.4. Role: Operations Administrator (E-Mall Team/Admin.)

Functions

- * Responsible for administering the E-Mall servers, including the IEC Server and the Database Server;
- * Responsible for creating and/or amending and/or terminating user accounts and related user authorizations on E-Mall system in accordance with instructions from authorized E-Mall State Coordinators; and
- * Responsible for requesting Certificate Manufacturer to create and deliver a Certificate to each authorized user.

Relevant Documents and Agreements

Page 807 of 1794

- * Agrees to abide by these **Operating Rules**.
- * Must sign **Operations Administrator Agreement** governing authorization rights and responsibilities to the E-Mall Server and related matters.

D.5. Role: State Partner MOU Signatory (State Partner/Principal)

Functions

- * Agrees to be an E-Mall Pilot Participant by signing the State MOU;
- * Designates the authorized Coordinator for the participating state government; and
- * Sponsors a Supplier for participation in the E-Mall with a valid, current contract with that state.

Relevant Documents and Agreements

- * Signs the **State MOU** that includes reference to agreement with policy materials (herein known as these **Operating Rules**).

D.6. Role: State Coordinator (State Partner/Contact)

Functions

- * Primary Operations and Business point of contact for communications with E-Mall Administrators;
- * Designates state users and their respective authorization rights, including designation as a Shopper, Approver, or Receiver;
- * Assists users in application process and with use of the E-Mall system;
- * Designates authorized Supplier Partner(s); and
- * Immediately notifies the E-Mall Operations Administrator of changes in authority (including termination) for any user.

Relevant Documents and Agreements

- * Agrees to abide by these **Operating Rules**. Signs **State Coordinator Agreement** and **User Designation and Authorization** forms for each authorized user.

D.7. Role: Shopper (State Partner/User)

NOTE: The role of Shopper is also known as "Requisitioner" for certain technical purposes within the I.E.C. application and the E-Mall system.

Functions

- * May shop on and through the E-Mall system;
- * Must use system only for authorized purposes and not use Public Key Certificate for any non-E-Mall pilot purpose;
- * For purposes of this pilot, using an approved Internet Browser, as defined in the Technical Requirements Section below, the Shopper will:
 - * shop available E-Mall catalogs on the Web to determine best value;
 - * select a participating Supplier;
 - * access the Supplier's storefront (electronic catalog) with contracted pricing in the E-Mall;
 - * select items to be purchased;
 - * create an OBI Order Request with the Supplier;
 - * verify in-house inventory availability as appropriate;
 - * adjust the OBI order request as necessary; and
 - * complete the OBI Order, flagging the OBI Order for operational approval.

Relevant Documents and Agreements

- * Agrees to abide by these **Operating Rules**.
- * Signs **User Agreement**.

D.8. Role: Operational Approver (State Partner/User)

Functions

- * May shop and must process approved OBI Orders created by other Shoppers;
- * No Approver may approve an OBI Order that they placed themselves unless they have been specifically authorized by the appropriate personnel at their state and that authorization has been successfully communicated to the E-Mall Administrator by the Approver's State Coordinator (note: this exception will be approved in appropriate circumstances, such as when a user works in a one person departments);
- * For purposes of this pilot, using an approved Internet Browser, as defined in the Technical Requirements Section below, the Operational Approver will:

- * review the OBI Order Request;
- * adjust the OBI Order Request as necessary; and
- * approve or deny the OBI Order Request on-line, flagging the OBI Order for Financial Approval.

Relevant Documents and Agreements

- * Agrees to abide by these **Operating Rules**.
- * Signs **User Agreement**.

D.9. Role: Financial Approver (State Partner/User)

Functions

- * May shop and must verify that the appropriate "encumbrance" and payment related financial controls for their state have been satisfied and documented;
- * This role may be combined with the Operational Approver;
- * Must enter relevant "legacy system" encumbrance and payment related numbers into the E-Mall system;
- * For purposes of this pilot, using an approved Internet Browser, as defined in the Technical Requirements Section below, and /or the legacy accounting system as appropriate, the Financial Approver will:
 - * verify funds availability;
 - * process an encumbrance in the legacy accounting system known as: legacy system;
 - * cross-reference the legacy system encumbrance and OBI Order Request for audit purposes and release the detailed OBI Order for EDI 850 Transmission;
 - * review and adjust invoices submitted for payment electronically in the EDI 810 format through the E-Mall
 - * process payment in the legacy accounting system known as: legacy system;
 - * update payment information on the OBI Order;
 - * financial approval must ensure that an appropriate legacy system entry has been made before an OBI Order is sent to the Supplier.

Relevant Documents and Agreements

- * Agrees to abide by these **Operating Rules**.
- * Signs **User Agreement**.

D.10. Role: Receiver (State Partner/User)

Functions

- * Must indicate in the system when commodities shipped as a result of an E-Mall OBI Order have been received in full and/or part, making notations as appropriate concerning the exceptions noted at the time of delivery;
- * For purposes of this pilot, using an approved Internet Browser, as defined in the Technical Requirements Section below, the Receiver will:
 - * physically accept and verify commodities received;
 - * record receipt of commodities in the E-Mall.

Relevant Documents and Agreements

- * Agrees to abide by these **Operating Rules**.
- * Signs **User Agreement**.

D.11. Role: Supplier Partner MOU Signatory (Supplier Partner/Principal)

Functions

- * Makes catalogs available according to the OBI specification as implemented for E-Mall through the E-Mall Operating Rules;
- * Is an authorized Supplier for purposes of doing business with participating E-Mall Partner States.
- * Accepts the E-Mall server Certificate and their own approved server Certificate as a secure, authenticated and binding method of transmitting quotes, orders (also known as OBI Order Requests and OBI Orders) through the E-Mall system, as specified under these Operating Rules;
- * Designates Supplier Coordinator.

Relevant Documents and Agreements

- * Agrees to abide by these **Operating Rules**.
- * Signs **Supplier MOU** and the **Electronic Commerce Supplier Partner Agreement**.
- * Signed respective **contracts** with the sponsoring state pursuant to applicable procurements laws for purposes of doing business with that state.

D.12. Role: Supplier Coordinator (Supplier Partner/Contact)

Functions

- * Primary Operations and Business point of contact for E-Mall communications with the Supplier Partner.

Relevant Documents and Agreements

- * Agrees to abide by these **Operating Rules**.

D.13. Role: Certificate Manufacturer

Functions

- * Creates Public Key Certificates as requested by E-Mall Operations Administrator;
- * Creates said Certificates according to the Certificate profile specified by E-Mall Policy Authority;
- * Abides by the Certificate Policy section of these Operating Rules governing creation, delivery and other aspects of Certificate Manufacture as documented agreed by the Policy Authority, following the format of the Internet Engineering Task Force PKIX Part 4 Framework (available at <http://www.ietf.org/internet-drafts/draft-ietf-pkix-ipki-part4-03.txt>) and in accord with the general guidance provided by Version 1.0 of the draft "Guidelines for Constructing Policies Governing the Use of Identity-Based Public Key Certificates" by the Certificate Authority Ratings and Trust Task Force of the Internet Council of the National Automated Clearinghouse Association (available at <http://internetcouncil.nacha.org/CARAT/>).

Relevant Documents and Agreements

- * Agrees to abide by these **Operating Rules**, including the **Certificate Policy**, and warrants that any internal documented practices, such as a Certificate Practice Statement, are consistent with these Operating Rules and Certificate Policy.
- * Signs **Certificate Manufacturer Agreement**.

D.14. Role: Solution Providers

Functions

- * Provide products and services necessary for State Partners to conduct OBI-Compliant transactions via the E-Mall;
- * Conduct initial system set up and testing;
- * Upon agreement and request, provide ongoing support to the E-Mall Operations Administrator as contracted and/or on a time and materials basis.

Relevant Documents and Agreements

- * Agrees to abide by the **Operating Rules**.
- * Signs contract and agrees to Task Order with Policy Authority for provision of services and related products.

E. Technical Requirements

For this pilot, the State User Department agrees to comply with the technical standards which are detailed below:

E.1. User Personal Computer:

The minimum computer requirements and configuration is detailed below:

E.1.1. Internet and World Wide Web Connectivity

A computer capable of accessing the World Wide Web (WWW), which implies connectivity to the Internet using the TCP/IP protocol.

E.1.2. Hardware:

- Pentium Processor
- 32MB memory
- 10 MB of available disk space on the hard drive
- 10/100 Ethernet network interface card

- A mouse
- Year 2000 compliant
- Monitor: 17 inch or greater SVGA monitor, with a minimum of 800X600 pixels of resolution
- ADA compliant

E.1.3. Software:

- Windows 95 or Windows NT 4.0 Workstation
- A 4.0 or higher version of the Netscape Navigator or Internet Explorer browser to allow the use of Secure Sockets Layer (SSL) 3.0
- A Public Key Certificate to be installed within the user's browser and used to authenticate the identity of a User will be issued by the Certificate Manufacturer contracted to provide services to the E-Mall
- Year 2000 compliant.
- ADA compliant

Comparable hardware and software is acceptable but resolution of problems arising from their use is the sole responsibility of the user department.

E.2. Supplier Partner

Every party that agrees to perform the role of a Supplier Partner must, at a minimum, provide a web-based catalog that is compliant with the OBI 1.1 specification, as referenced under these Operating Rules.

E.3. Physical Security of Computing and Network Resources

The E-Mall Web Server must be kept in a physically secure location such that unauthorized persons can not gain physical access to the server without breaking and entering. There are no physical security requirements for Users during the course of the pilot, however, no User may permit an unauthorized person to gain access to a computer that is currently accessing a restricted area of the E-Mall server (that is, once a user logs onto the system with a username, password and Certificate, that user should not leave their computer accessible to any other person until logging off the E-Mall server). There are no physical security requirements for Suppliers during the course of the pilot. The Certificate Manufacturer must assure that no unauthorized personnel may gain physical access to the private key for the root Certificate for this pilot or may otherwise become capable of manufacturing unauthorized Certificates.

F. Duties and Obligations of the Parties

F.1. Electronic Offer and Acceptance

The terms **OBI Order Request** and **OBI Order** are to be construed in accordance with the OBI 1.1 specification, as referenced in these Operating Rules. For purposes of this section, the term **E-Mall Server** shall mean the web server hosted on behalf of the State Partners for the purpose of conducting OBI-compliant transactions. For purposes of this section, the term **Supplier Server** shall mean the web server of a Supplier Partner for the purpose of conducting OBI-compliant transactions.

F.1.1. OBI Order Request

An OBI Order Request shall constitute a contractual offer by the Supplier Partner to sell the specified commodities at the specified price and other included terms once it has been successfully posted by the Shopper's web browser to the E-Mall Server at the agreed upon post-back URL.

F.1.2. OBI Order

An OBI Order shall constitute a contractual acceptance by the State Partner once it has been successfully posted by the E-Mall Server to the Supplier Server at the agreed upon post-back URL.

F.2. Notice

Every party that has been approved as a participant after having signed and delivered a participation agreement for the E-Mall Pilot is entitled to notice of any proposed amendment to these Operating Rules at least 14 calendar days prior to said amendments taking effect, unless otherwise agreed by all the parties. In the case of a State Partner, the person(s) who sign the State MOU and each authorized State Coordinator are entitled to receive notice and may be requested or required to pass along such notice to each subordinate user within their state if appropriate.

F.3. Participation Agreements

As noted under these Operating Rules, a party that performs an authorized role within the E-Mall must sign an agreement, known generally as a Participation Agreement. A key function of each Participation Agreement is to signify the assent of each party to abide by these Operating Rules. Parties who will assume a role within the E-Mall Pilot may retrieve a current version of their respective agreements in PDF form from the official E-

Mall web site. These agreements must be completed, signed, and returned to the E-Mall Business Administrator in order for any person to become an authorized E-Mall participant.

F.4. Confidentiality

Unless otherwise specified in these Operating Rules and related agreements and to the extent permitted under applicable law, all personally identifiable information related to the E-Mall pilot, including User information, usage statistics related to an individual user, the names of administrators, any telephone, address or other individually identifiable data should be considered confidential and should not be disclosed to any person outside of the E-Mall pilot. Similarly, no Pilot Participant should make any public statements including press releases, information available on a web site and slide presentation related to the E-Mall pilot or about any other person or organization's participation in the E-Mall pilot, unless that statement has first:

- * appeared on the official E-Mall web site, or
- * appeared in the public press, or
- * been approved by an E-Mall Administrator

F.5. Intellectual Property

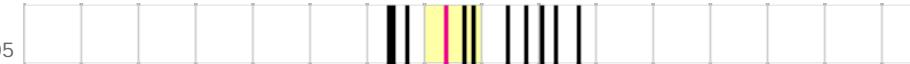
These Operating Rules are subject to Copyright by the Commonwealth of Massachusetts in its capacity as sponsor of the Multi-State E-Mall. All rights reserved. Permission to reproduce this document is hereby granted provided that the following limitations on this right are observed: (1) all copies must clearly indicate that this work is published by and attributed to the Commonwealth of Massachusetts in its capacity as sponsor of the Multi-State E-Mall; and (2) all copies must include this notice of copyright.

"Multi-State E-Mall" is a trademark of the Commonwealth of Massachusetts in its capacity as sponsor of the Multi-State E-Mall.



[11 captures](#)

6 May 02 - 21 Sep 05



SEP	MAY	SEP
	22	
2002	2003	2004

[Close](#)[Help](#)

Operating Rules

*For use in the Electronic Procurement Project
Known as the "Multi-State E-Mall"™*

Version 2.0

The Current Version of this Document is Available at:

<http://email.isa.us/or>

COPYRIGHT NOTICE

Copyright © 1999 by the Commonwealth of Massachusetts. All rights reserved. Permission to reproduce this document is hereby granted provided that the following limitations on this right are observed: (1) all copies must clearly indicate that this work is published by and attributed to the Commonwealth of Massachusetts, as Policy Authority for the Multi-State EMall; and (2) all copies must include this notice of copyright.

Table of Contents

A. Scope

[A.1. General](#)

[A.2. Application of these Operating Rules](#)

[A.3. Open Buying on the Internet](#)

[A.4. Contact Information](#)

B. Authentication: In General

[B.1. Issuance, Use, Modification and Termination of User Name and Passwords](#)

[B.2. Use of SSL](#)

[B.3. Use of S/MIME](#)

[B.4. Use of Fax, Telephone, U.S. Mail, Commercial Couriers, and Unsecured/Unauthenticated E-Mail](#)

[C. Authentication: Certificate Policy](#)

[C.1. Introduction](#)

[C.2. General Provisions](#)

[C.3. Identification and Authentication](#)

[C.4. Operational Requirements](#)

[C.5. Physical, Procedural, and Personnel Security Controls](#)

[C.6. Technical Security Controls](#)

[C.7. Certificate and CRL Profiles](#)

[C.8. Specification Administration](#)

[D. Roles, Functions and Authorization of Participating Parties](#)

[D.1. General Concepts](#)

[D.2. Role: Policy Authority \(EMall Team/Principal\)](#)

[D.3. Role: Business Administrator \(EMall Team/Admin.\)](#)

[D.4. Role: Operations Administrator \(EMall Team/Admin.\)](#)

[D.5. Role: State Partner MOU Signatory \(State Partner/Principal\)](#)

[D.6. Role: State Coordinator \(State Partner/Contact\)](#)

[D.7. Role: Shopper \(State Partner/User\)](#)

[D.8. Role: Operational Approver \(State Partner/User\)](#)

[D.9. Role: Financial Approver \(State Partner/User\)](#)

[D.10. Role: Receiver \(State Partner/User\)](#)

[D.11. Role: Supplier Partner MOU Signatory \(Supplier Partner/Principal\)](#)

[D.12. Role: Supplier Coordinator \(Supplier Partner/Contact\)](#)

[D.13. Role: Certificate Manufacturer](#)

[D.14. Role: Solution Providers](#)

[E. Technical Requirements](#)

[E.1. User Personal Computer](#)

[E.2. Supplier Partner](#)

[E.3. Physical Security of Computing and Network Resources](#)

[F. Duties and Obligations of the Parties](#)

[F.1. Creation of Legally Binding Purchases](#)

[F.2. Notice](#)

[F.3. Participation Agreements](#)

[F.4. Confidentiality](#)[F.5. Intellectual Property](#)[F.6. Alternative Dispute Resolution](#)[F.7. Governing Law](#)

A. Scope

A.1 General

The Multi-State Email pilot (Email) is an Extranet procurement Web site, hosted by the Commonwealth of Massachusetts and available to participating states (known as State Partners in this document). The Email web site provides links to qualified Supplier "storefronts" or catalogs, where state procurement staff (known as authorized State Users) can browse, shop and create requisitions. Public Key Certificate technology coupled with user name and password ensure that only authorized State Users can submit approved OBI Orders to the approved suppliers (known as authorized Supplier Partners). In addition, casual, non-priviliged Internet users can access certain public portions of the site, but can not engage in binding transactions unless they are authorized participants in this pilot and agree to accept these Operating Rules.

A.2 Application of these Operating Rules

These Operating Rules apply to every participant in the Email. No party may play any role or otherwise act as a participant in the Email without signing a Participation Agreement. Depending on the role a given party plays (i.e. User, Supplier, Administrator, etc.) a different Participation Agreement with special terms may be required.

A.3 Open Buying on the Internet

The Email is based upon the Open Buying on the Internet (OBI) specification. OBI is an emerging standard that defines the technical requirements for conducting business over the Internet from buyer to seller.

The following definition is copied from the OBI web site:

The OBI standard is an open, flexible design for business-to-business Internet commerce solutions. It is intended for the high-volume, low-dollar transactions that account for 80% of most organizations' purchasing activities. Version 1.0 of the standard document contains an architecture, as well as technical specifications and guidelines. OBI is not a product or a service; it is a freely available standard which any organization can obtain and use.

Information about the OBI standard is available at the web site <http://www.openbuy.org>. Version 1.0 and Version 1.1 of the OBI technical specifications are available from this site.

A.4 Contact Information

The Policy Authority promulgating these Operating Rules is the Commonwealth of Massachusetts. A current version of these Operating Rules and related information is available at <http://email.isa.us>.

Signed Participation Agreements of each party performing a role under these Operating Rules are on file with the Policy Authority.

For purposes of business communications, parties performing a role in the EMall may contact:

Nancy Burke, EMall Project Manager,
Commonwealth of Massachusetts, Operational Services Division
One Ashburton Place, Room 1017
Boston, MA 02108
nancy.burke@osd.state.ma.us, 617.720.3187

For questions or comments specifically relating to these Operating Rules, parties performing a role in the EMall may contact:

Daniel Greenwood, Deputy General Counsel, Information Technology Division & EMall Counsel and Steering Committee Member
Commonwealth of Massachusetts
One Ashburton Place, Room 801
Boston, MA 02108

dan.greenwood@state.ma.us, or dan@civics.com, 617.973.0071

B. Authentication: In General

B.1. Issuance, Use, Modification and Termination of User Name and Passwords

A User name and Password must be supplied by every User of the EMall Server accessing a non-public portion of the system. No User may share or otherwise reveal their Password or other authorized Personal

Identification Number (PIN). Any suspicion that a Password has been compromised must be immediately communicated to the State Coordinator for that User. A Password may be re-set in the event that an authorized User forgets the Password. A User should contact their State Coordinator, who can authorize a password reset from the Operations Administrator. Upon proper notification by an authorized State Coordinator under these Operating Rules and relevant implementing agreements, a User's access to the EMall will be terminated and the respective User name and Password combination for a terminated User will no longer be valid.

In addition to transmission of the valid Public Key Certificate, User identification for access to the EMall server also requires presentation of a user name that corresponds with the Common Name of the Subscriber as listed in the Public Key Certificate (and that is unique within the EMall User profiles) and must be transmitted with the corresponding valid password or PIN.

B.2. Use of SSL

Every person accessing any non-public portion of the EMall server must use the Secure Sockets Layer (SSL) protocol. The SSL protocol will be used to authenticate and secure certain communications between Supplier servers and the EMall server as well as to encrypt certain session between the browser of a User and the EMall server and authenticate the identity of authorized EMall Users. A web session invoking version 3 of the SSL protocol requires use of a duly issued Public Key Certificate within the browser of an EMall User. SSL 3 is also required to authenticate and secure the transmission of a valid OBI Order from the EMall server to the server of a Supplier.

B.3. Use of S/MIME

A Pilot Participant who is duly issued a Public Key Certificate for use in the EMall may use that Public Key Certificate to "sign" e-mail to another participant. In addition, a Pilot Participant may use the duly issued EMall Public Key Certificate of another participant to encrypt e-mail using the S/MIME standard, provided each person uses an interoperable e-mail client. In some cases, as determined by an EMall Administrator, use of S/MIME may be requested or required to assure official communications via e-mail are confidential and/or authenticatable.

B.4. Use of Fax, Telephone, U.S. Mail, Commercial Couriers, and Unsecured/Unauthenticated E-Mail

B.4.1. General

Access as a User or Administrator to the EMall server will require a valid User name and Password as well as a recognized Public Key Certificate. However, many other communications channels will be used for various other purposes throughout the term of this pilot. It is recognized that implementation of a production system will require greater specificity regarding permitted and prohibited methods of communication and corresponding authentication depending on the purposes of the communications. It is intended that

experience gained through this pilot process will demonstrate appropriate guidelines. For purposes of the pilot, however, it is expected that most non-critical communications will occur between pilot participants via phone and e-mail.

B.4.2. Communication of Agreements and Related Data

Communication of the implementing agreements under these Operating Rules and related User designation and authorization data requires greater specificity. Until and unless otherwise specified in future versions of these Operating Rules, delivery of all completed forms, agreements and related data, including all designation of roles and authorities for Users of the EMall system must be communicated via:

- * Fax, U.S. Mail or Commercial Couriers, or
- * Upon prior approval by the EMall Business Coordinator, S/MIME Signed E-Mail, signed by private key corresponding to a validly issued Public Key Certificate for the EMall pilot

Until and unless return receipt is received by phone call back or other agreed methods, sender must consider that such data has not been successfully transmitted.

B.4.3. Other Communications

Unless otherwise specified in these Operating Rules, communications may be conducted by any reasonable means that are appropriate under the circumstances..

C. Authentication: Certificate Policy

C.1. Introduction

For purposes of the Multi-State EMall pilot, a Public Key Certificate (Certificate) is a computer-based record which:

- (a) identifies the entity or brand associated with issuance of it;
- (b) names or identifies the person or device associated with the corresponding private key;
- (c) contains the public key corresponding to that private key of that person or device; and
- (d) is digitally signed by the Certificate Manufacturer that creates the Certificate.

In transacting business over the Internet, it is critical that both the seller and buyer be assured that the transactions exchanged are secure. Public key encryption coupled with Public Key Certificates can provide part of this security by ensuring the confidentiality and/or authentication of electronic business exchanges. When Public Key Certificates are attached to transactions, parties on each side of a purchase have some evidence of who the message came from and that it was not tampered with. The EMall pilot uses Certificates to bolster the authentication provided by the Password and User name in the Email system. A Certificate is not, by itself, sufficient to perform any transactions within the EMall system.

Public Key Certificates are used to authenticate Web servers and their clients via protocols such as SSL 3.0. A Public Key Certificate is analogous to an identification card issued by an employer or membership organization. Each User participating in the EMall pilot must have at least one Public Key Certificate. Certificates will be issued at no cost by a designated and contracted party known as a Certificate Manufacturer (CM). The CM will issue a Certificate to Users who have been identified by their respective State Coordinators and accepted by the EMall Administrator.

The browser specifications, as noted in the Section E Technical Requirements, accommodates the use of Public Key Certificates. A technical resource for each State Partner will be needed to assist each User with the installation of that User's Certificate. This technical resource and/or the state coordinator must have an adequate understanding of the technical and operational requirements and responsibilities associated with managing, issuing and maintaining Public Key Certificates. The technician shall not have knowledge of any User's password.

This Certificate Policy section of these Operating Rules governs creation, delivery and other aspects of the Certificate Manufacturing process as well as the proper use of Public Key Certificates. This section follows the format of the Internet Engineering Task Force PKIX Part 4 Framework (available at <http://www.ietf.org/internet-drafts/draft-ietf-pkix-ipki-part4-03.txt>) and is in general accord with the guidance provided by Version 1.0 of the draft "Guidelines for Constructing Policies Governing the Use of Identity-Based Public Key Certificates" by the Certificate Authority Ratings and Trust (CARAT) Task Force of the Internet Council of the National Automated Clearinghouse Association (NACHA) available at <http://internetcouncil.nacha.org/CARAT/>. Please note that many of the basic business and legal terms surrounding each party's role within the EMall are properly addressed in other sections of these Operating Rules and will either supplement or replace information reserved under IETF PKIX-4 headings (such as "liability" and "financial responsibility" etc.).

C.2. General Provisions

C.2.1 Obligations

C.2.1.1 Policy Authority Obligations

The Policy Authority pays for most or all of the EMall pilot and has initiated the effort to create this pilot.

The chief obligation of the Policy Authority is to sponsor and organize the EMall pilot, to set policy, including this certificate policy, and to assure the smooth and successful operation of the pilot. The policies are set in a manner that affords input and comment from State Partners and other Pilot Participants.

C.2.1.2 PKI Service Providers

C.2.1.2.1 Registrars

The Registrar, is the sole point of contact between the PA and the CM for purposes of requesting the issuance of certificates. The Registrar is ordinarily the EMall Business Administrator. However, when necessary, the EMall Operations Administrator may act as Registrar. The Registrar must keep records of each application request and valid certificates issued. Each State Coordinator shall also act as a Local Registrar for purposes of designating authorized Users and therefore certificate subscribers.

C.2.1.2.2 Operations Administrators

The Operations Administrator (OA) sets the EMall server to grant access authorized subscribers based on the unique information in each subscriber's certificate. The OA is responsible for acquiring and installing "commercial off the shelf" server certificates on the main EMall server as well as training and development servers, as needed. In addition, the Operations Administrator is responsible for installing the CM's root certificate on each EMall server that will process subscriber certificates and for the distribution of root certificates to each authorized Supplier that will act as a Relying Party.

C.2.1.2.3 Certificate Manufacturers

The Certificate Manufacturer (CM) only has duties and responsibilities toward the Policy Authority and duly designated Administrators and not directly toward any other pilot participant, other than as specified in this section of the Operating Rules or as agreed upon by and between the CM, the PA and each such other party. The CM shall manufacture Public Key Certificates according to the certificate profile contained in this Certificate Policy upon the request of the Registrar. Each such certificate shall reflect accurately the information contained in the certificate application, including the Common Name and the State associated with each applicant.

C.2.1.3 End Entities (Parties or Their Devices that Use or Rely Upon Certificates)

C.2.1.3.1 Subscribers

C.2.1.3.1.1 Users

Each EMall User (including Shoppers, Approvers and Receivers) shall be issued a Public Key Certificate upon designation and authorization by their respective State Coordinator and successfully completing and submitting their User Agreement. A User's EMall certificate does not represent a generic identification or authorization credential for use outside the EMall. A User is obligated to refrain from using their EMall certificate in any communications with non-EMall Pilot Participants or for non-EMall related business. A User must provide accurate information in the User Agreement and related forms and to their respective State Coordinator with respect to EMall activities. A User must immediately notify their State Coordinator upon notice or reasonable suspicion that information within their certificate is no longer accurate, including upon the termination of their employment. A User must immediately notify their State Coordinator upon notice or reasonable suspicion that the private key corresponding to their certificate has been compromised (see User Documentation and User Agreement for more information). A User must abide by the terms and conditions of their User Agreement.

C.2.1.3.1.2 EMall Server Certificate for User Sessions

The EMall server and such other training or support servers as are designated by the EMall Operations Administrator shall have installed a valid Server Certificate. To be valid, under this section, a Server Certificate must be signed by a CM whose certificate signing key is recognized (without further customization) by each Browser that is supported for use within the EMall (see Section E. of these Operating Rules). That means that the public key that corresponds to the private key used to sign the Server Certificate must be embedded within each such browser at the time the Browser software is distributed and requires no further installation of a root certificate or other prefatory work in order to invoke an SSL session. In addition, a valid certificate must be used only within the starting and ending dates designated in the Server Certificate and must be replaced prior to expiration of said ending date.

C.2.1.3.1.3 EMall Transaction Server Certificate for OBI Order Transmissions

The EMall Server Transaction Certificate shall be a public key certificate used to initialize an encrypted http session and to identify the EMall server to authorized Supplier transaction server for the purpose of sending Valid OBI orders using SSL 3. The Operations Administrator shall assure that a valid EMall Server Transaction Certificate is installed on the EMall server and will make sufficient information about the contents of that certificate known to each authorized Supplier who will act as a Relying Party upon that certificate.

C.2.1.3.1.4 Other Pilot Participants

For purposes of testing, support and other activities approved by the PA or authorized Administrator, any other EMall Pilot Participant may be issued a Public Key Certificate. Where an individual other than a User issued a certificate, that person must first agree to abide by relevant sections of these Operating Rules and any other terms and conditions deemed appropriate by the PA or its authorized Administrator. These

additional terms must, at a minimum, specify the purpose and authorized uses of the certificate within the EMall pilot.

C.2.1.3.2 Relying Parties

C.2.1.3.2.1 Administrators

The Operations Administrator must require and accept valid EMall certificates as part of the initial authentication of authorized Users of the EMall server. Use of a certificate alone shall not be sufficient proof of identity for purposes of gaining access to User-only section of the EMall server, but must be accompanied by the authentication requirements specified in Part B. of these Operating Rules.

C.2.1.3.2.2 Suppliers

Suppliers may rely upon valid EMall certificates to identify and authenticate a subscriber as an authorized Shopper, as that role is defined under these Operating Rules. Suppliers must rely upon a certificate to authenticate and secure valid OBI Orders from the EMall server. Suppliers may rely upon certificates to identify a subscriber via S/MIME signed e-mail, but may not assume any authorization based solely upon usage of a certificate used for this purpose. Suppliers may not rely upon EMall certificates for any other purposes than those specified in these Operating Rules.

C.2.1.3.2.2.1 Shopper Browser Certificate Used for Authentication to Supplier Web Catalog

A Supplier should, but need not utilize a subscriber certificate of a Shopper for authentication. A Supplier that does not rely upon the subscriber certificate for authentication directly may rely upon certificate and other User authentication performed by the EMall server and securely passed on to the Supplier at the beginning of a web catalog session for purposes of shopping. A Supplier that uses a subscriber certificate for purposes of authentication must, at a minimum:

* assure that the certificate was manufactured by the authorized CM for the EMall, based upon the root certificate distributed by the Operations Administrator; and

* identify the State of the Shopper from within the certificate for purposes of assuring the correct contracted items and prices are displayed and that the correct OBI Order Request information is transmitted.

C.2.1.3.2.2.2 EMall Server Transaction Certificate for OBI Orders Used for Authentication to Supplier Transaction Server

The EMall Server Transaction Certificate shall be a public key certificate used to identify the EMall server to authorized Supplier transaction server for the purpose of sending Valid OBI orders. All Suppliers must utilize a secure and authenticated SSL 3 (dual authenticated) session for the transmission of valid OBI Orders from the EMall server. If the SSL 3 session necessary to commence transmission of an OBI Order to a Supplier transaction server is invoked without a Public Key Certificate or via a Public Key Certificate other than that provided for under section C.2.1.3.1.3 of these Operating Rules (EMall Server Transaction Certificate), then the resulting transaction must be regarded as invalid. The risk that an unauthorized OBI Order could be generated that conforms with the format, content and other process constraints comprising a valid EMall OBI Order is extremely low, but the risk does exist. If a Supplier wishes to further minimize this risk, then the Supplier should configure their transaction server to accept EMall OBI Orders only from the pre-authorized EMall Server Transaction Certificate, based upon certificate information provided to the Supplier by the EMall Operations Administrator under section C.2.1.3.1.3.

C.2.1.3.2.3 Pilot Participants

No Pilot Participant may use their certificate to authenticate themselves to any person or device outside of the EMall pilot. All Pilot Participants can use their Public Key Certificates to send signed e-mail to any other Pilot Participant. In addition, any Pilot Participant may use the Public Key Certificate of another pilot participant to send encrypted e-mail to that person. Not all Pilot Participants are necessarily entitled to an EMall certificates.

C.2.2 Liability

Liability is not dealt with in the Certificate Policy, rather it is governed by the underlying business contracts and other relevant business agreements between parties participating in this pilot. This Certificate Policy exists for the purpose of further defining and clarifying details of this authentication method and does not comprise the business relationship between the parties.

C.2.5 Fees

Certificates are provided at no cost to Pilot Participants.

C.2.6 Publication and Repository

The CM maintains a non-public, web-accessible repository of valid and revoked certificates. For security purposes no further information on this repository is available in these Operating Rules. From time to time the PA or its designated Administrators may request access to this repository according to terms and processes as mutually agreed between the PA and the CM.

C.2.7 Compliance Audit

No Compliance Audit is necessary under these Operating Rules. More detailed duties and obligations between the PA and the CM can be found in the Implementing Contract between those parties by which the CM is contracted to provide certificate manufacturing services.

C.2.8 Confidentiality

See section F.4 of these Operating Rules.

C.2.9 Intellectual Property Rights

See section F.5 of these Operating Rules.

C.3. Identification and Authentication

The process and practices governing identification and authentication of subscribers are determined by the EMall Business Administrator, with the knowledge and assent of the EMall Steering Committee and the agreement of each State Partner Coordinator. The Business Administrator may customize these processes and practices to conform to different management and organizational environments among the various State Partners and other authorized Subscribers. Material procedures must be documented and available for review by the EMall Steering Committee and any other party with a business need or legal right of access to that information. Documented processes and relevant practices may be changed throughout the pilot, but any material changes must require the knowledge and consent of the EMall Steering Committee.

C.4. Operational Requirements

See Section C.2 of these Operating Guidelines for relevant Operational Requirements.

C.5. Physical, Procedural, and Personnel Security Controls

The CM, PA and relevant Administrators shall agree upon appropriate physical, procedural and personnel security controls, as needed.

C.6. Technical Security Controls

The CM, PA and relevant Administrators shall agree upon appropriate technical security controls, as needed.

C.7. Certificate and CRL Profiles

Note: Content redacted from this draft for purpose of maintaining security of sensitive processes. The syntax and semantics underlying the EMall Certificate Profile is available, to the extent necessary, upon request from any authorized Relying Party who needs the information to accept or process Public Key Certificates and to conform to relevant Risk Management guidelines, as provided under these Operating Rules and by the Policy Authority.

C.8. Specification Administration

The Policy Authority is the Specification Administration. Matters such as publication, notice of change and rights to comment on rules changes are dealt with throughout these Operating Rules and are not unique or specific to the use of any one authentication method for this business system. The use of public key certificates, and the policies related to such use, is part of the overall business system underlying the EMall pilot. General issues related to Notice of change of these Operating Rules, including any changes to the Certificate Policy sections of these Operating Rules, can be found in Section F.2.

D. Roles, Functions and Authorization of Participating Parties

D.1. General Concepts

Party: A legal entity. A natural person can be a party. Certain organizations, such as corporations, trusts and governments may also be recognized as a legal person and therefore can be a party. Each party will be identified by name in relevant documents and agreements. Actions of an automated program, including an electronic agent, are deemed to be the actions of a party that used the program for that purpose, under these Operating Rules.

Functions: The particular duties and obligations entered into within a business and technical system. A Party will perform several functions. These sets of functions are put together based on technical, legal and business needs of the enterprise.

Role: Each *role* is named according to the nature of the functions in each set. By naming roles, and associating functions with roles, it is not suggested that in every business model sets of functions will be divided in the same manner as here. Further, it is not suggested that there will be one-to-one correlation between roles and parties. Indeed, it is envisioned that a *party* may perform one or more roles. The purpose for naming roles in this document is primarily to provide a vocabulary for creating modular parts that can be performed by a given party entering the EMall system and to organize the obligations and related documents associated with a given party.

For example, rather than call the administration role by the name Commonwealth of Massachusetts, it is convenient to name it based on the relevant suite of functions so that any party could perform the role more easily within the system of documents and business arrangements herein. Similarly, while particular parties perform the role of service providers, there may be additional and/or different parties playing those roles in the future, hence we use terms like "solution provider" and "Certificate Manufacturer." The usage of roles under these Operating Rules is intended to reflect and support the potential evolution of this project from a relatively closed and small pilot to a scalable production system in which many more parties may perform the roles noted herein.

Documents and Agreements: In many cases, a party will have to sign a document or submit a particular form as part of the functions associated with a given role. These documents might be contracts, memoranda of understanding, applications, reports and so on. These documents hold a particular legal importance as the glue that hold together parties, roles and functions in a predictable and enforceable system.

Pilot Participants: Every party that agrees to be bound by the Operating Rules is considered to be a "Pilot Participant." This general designation defines the closed community of people who are part of the EMall pilot. All of the parties whose roles are described below (not limited to Users alone) are also considered Pilot Participants because they all agree to be bound by these Operating Rules and to operate within the pilot in some authorized manner.

D.2. Role: Policy Authority (EMall Team/Principal)

Functions

- * Sponsor of the Multi-State EMall pilot;
- * Makes all policy decisions related to the Multi-State EMall pilot;
- * Designates, and delegates appropriate authority to EMall Administrators;
- * Agrees to accept the MOU of State Partners; and
- * Selects and arranges for technology products and services necessary for hosting the EMall OBI-Compliant server on behalf of State Partners as buying organizations.

Relevant Documents and Agreements

- * Promulgates, or delegates authority to promulgate, these **Operating Rules** and all other official agreements or documents related to the Multi-State EMall.

D.3. Role: Business Administrator (EMall Team/Admin.)

Functions

Page 830 of 1794

- * Receives names/contact data of each State Coordinator from each designated Partner State (from person(s) who signed the MOU);
- * Gives the State Coordinator contact information to the Operations Administrator;
- * Reviews and submits for processing all security related applications and forms, including those related to Public Key Certificates, which are forwarded by the State Coordinator; and
- * Securely maintains all applications and forms for related Public Key Certificate requests before and after processing by the EMall Operations Administrator.

Relevant Documents and Agreements

- * Agrees to abide by these **Operating Rules**.
- * Must sign **Business Administrator Agreement**.

D.4. Role: Operations Administrator (EMall Team/Admin.)

Functions

- * Responsible for administering the EMall servers, including the IEC Server and the Database Server;
- * Responsible for creating and/or amending and/or terminating User accounts and related User authorizations on EMall system in accordance with instructions from EMall Business Administrator; and
- * Responsible for accurately ascertaining the identity of an authorized User prior to performing a password reset. Calling the purported User back at the pre-authorized telephone number designated by that User's State Coordinator is a reasonable basis for confirming the identity of an EMall User.
- * Responsible for requesting Certificate Manufacturer to create and deliver a Public Key Certificate to each authorized User.

Relevant Documents and Agreements

- * Agrees to abide by these **Operating Rules**.
- * Must sign **Operations Administrator Agreement** governing authorization rights and responsibilities to the EMall Server and related matters.

D.5. Role: State Partner MOU Signatory (State Partner/Principal)

Functions

- * Agrees to be an EMall Pilot Participant by signing the State MOU;

- * Designates the authorized Coordinator for the participating State Partner; and
- * Sponsors a Supplier for participation in the EMall with a valid, current contract with that state.

Relevant Documents and Agreements

- * Signs the **State MOU** that includes reference to agreement with policy materials (herein known as these **Operating Rules**).

D.6. Role: State Coordinator (State Partner/Contact)

Functions

- * Primary Operations and Business point of contact for communications with EMall Administrators;
- * Designates state Users and their respective authorization rights, including designation as a Shopper, Approver, or Receiver;
- * Assists User in application process and with use of the EMall system;
- * Designates authorized Supplier Partner(s); and
- * Immediately notifies the EMall Operations Administrator of changes in authority (including termination) for any User or Supplier.

Relevant Documents and Agreements

- * Agrees to abide by these **Operating Rules**. Signs **State Coordinator Agreement** and **User Designation and Authorization** forms for each authorized User.

D.7. Role: Shopper (State Partner/User)

NOTE: The role of Shopper is also known as "Requisitioner" for certain technical purposes within the I.E. C. application and the EMall system.

Functions

- * May shop on and through the EMall system;
- * May act, with the prior permission of the EMall Operations Administrator, as a User of the EMall system through the use of an Electronic Agent, as defined under the most current draft or applicable enacted Uniform State Law, including Article 2 of the Uniform Commercial Code, draft proposed Article 2B and the draft proposed Uniform Electronic Transactions Act [links to official current drafts and related information is available at: <http://www.state.ma.us/itd/legal/agents>);

- * Must use system only for authorized purposes and not use Public Key Certificate for any non-EMall pilot purpose;
- * For purposes of this pilot, using an approved Internet Browser, as defined in the Technical Requirements Section below, the Shopper will:
 - * shop available EMall catalogs on the Web to determine best value;
 - * select a participating Supplier;
 - * access the Supplier's storefront (electronic catalog) with contracted pricing in the EMall;
 - * select items to be purchased;
 - * create an OBI Order Request with the Supplier;
 - * verify in-house inventory availability as appropriate;
 - * adjust the OBI order request as necessary; and
 - * complete the OBI Order, flagging the OBI Order for operational approval.

Relevant Documents and Agreements

- * Agrees to abide by these **Operating Rules**.
- * Signs **User Agreement**.

D.8. Role: Operational Approver (State Partner/User)

Functions

- * May shop and must process approved OBI Orders created by other Shoppers;
- * May act, with the prior permission of the EMall Operations Administrator, as a User of the EMall system through the use of an Electronic Agent, as defined under the most current draft or applicable enacted Uniform State Law, including Article 2 of the Uniform Commercial Code, draft proposed Article 2B and the draft proposed Uniform Electronic Transactions Act [links to official current drafts and related information is available at: <http://www.state.ma.us/itd/legal/agents>);
- * No Approver may approve an OBI Order that they placed themselves unless they have been specifically authorized by the appropriate personnel at their state and that authorization has been successfully communicated to the EMall Administrator by the Approver's State Coordinator (note: this exception will be approved in appropriate circumstances, such as when a User works in a one person departments);
- * For purposes of this pilot, using an approved Internet Browser, as defined in the Technical Requirements Section below, the Operational Approver will:
 - * review the OBI Order Request;
 - * adjust the OBI Order Request as necessary; and

- * approve or deny the OBI Order Request on-line, flagging the OBI Order for Financial Approval.

Relevant Documents and Agreements

- * Agrees to abide by these **Operating Rules**.
- * Signs **User Agreement**.

D.9. Role: Financial Approver (State Partner/User)

Functions

- * May shop and must verify that the appropriate "encumbrance" and payment related financial controls for their state have been satisfied and documented;
- * May act, with the prior permission of the EMall Operations Administrator, as a User of the EMall system through the use of an Electronic Agent, as defined under the most current draft or applicable enacted Uniform State Law, including Article 2 of the Uniform Commercial Code, draft proposed Article 2B and the draft proposed Uniform Electronic Transactions Act [links to official current drafts and related information is available at: <http://www.state.ma.us/itd/legal/agents>
- * This role may be combined with the Operational Approver;
- * Must enter relevant "legacy system" encumbrance and payment related numbers into the EMall system;
- * For purposes of this pilot, using an approved Internet Browser, as defined in the Technical Requirements Section below, and /or the legacy accounting system as appropriate, the Financial Approver will:
 - * verify funds availability;
 - * process an encumbrance in the legacy accounting system known as: legacy system;
 - * cross-reference the legacy system encumbrance and OBI Order Request for audit purposes and release the detailed OBI Order for EDI 850 Transmission;
 - * review and adjust invoices submitted for payment electronically in the EDI 810 format through the EMall;
 - * process payment in the legacy accounting system known as: legacy system;
 - * update payment information on the OBI Order;
 - * financial approval must ensure that an appropriate legacy system entry has been made before an OBI Order is sent to the Supplier.

Relevant Documents and Agreements

- * Agrees to abide by these **Operating Rules**.
- * Signs **User Agreement**.

D.10. Role: Receiver (State Partner/User)

Functions

- * Must indicate in the system when commodities shipped as a result of an EMall OBI Order have been received in full and/or part, making notations as appropriate concerning the exceptions noted at the time of delivery;
- * Must document exceptions within the EMall system and any necessary legacy system;
- * May act, with the prior permission of the EMall Operations Administrator, as a User of the EMall system through the use of an Electronic Agent, as defined under the most current draft or applicable enacted Uniform State Law, including Article 2 of the Uniform Commercial Code, draft proposed Article 2B and the draft proposed Uniform Electronic Transactions Act [links to official current drafts is available at: <http://www.law.upenn.edu/library/ulc/ulc.htm>) and additional non-binding, but helpful information can be found at: <http://www.tiac.net/biz/danielg/agents/>);
- * For purposes of this pilot, using an approved Internet Browser, as defined in the Technical Requirements Section below, the Receiver will:
 - * accept and verify commodities received;
 - * record receipt of commodities in the EMall.

Relevant Documents and Agreements

- * Agrees to abide by these **Operating Rules**.
- * Signs **User Agreement**.

D.11. Role: Supplier Partner MOU Signatory (Supplier Partner/Principal)

Functions

- * Makes catalogs available according to the OBI specification as implemented for EMall through the EMall Operating Rules;
- * Is an authorized Supplier for purposes of doing business with the EMall Partner state that sponsored that Supplier and with such other participating EMall Partner States as agreed by the parties;
- * Accepts the EMall transactional system (including the various usages of authorized Public Key Certificates) and their own authorized transaction server as a valid and binding method of transmitting quotes and receiving orders (also known as OBI Order Requests and OBI Orders, respectively), as specified under these Operating Rules;
- * Designates Supplier Coordinator.

Relevant Documents and Agreements

Page 835 of 1794

- * Agrees to abide by these **Operating Rules**.
- * Signs **Supplier MOU** and the **Electronic Commerce Supplier Partner Agreement**.
- * Signed respective **contracts** with the sponsoring state pursuant to applicable procurements laws for purposes of doing business with that state.

D.12. Role: Supplier Coordinator (Supplier Partner/Contact)

Functions

- * Primary Operations and Business point of contact for EMall communications with the Supplier Partner;
- * Responsible for responding to delivery or payment inquiries and disputes, including by use of the query function, as available, within the EMall system.

Relevant Documents and Agreements

- * Agrees to abide by these **Operating Rules**.

D.13. Role: Certificate Manufacturer

Functions

- * Creates Public Key Certificates as requested by EMall Operations Administrator;
- * Creates said Certificates according to the Certificate profile specified by EMall Policy Authority;
- * Abides by the Certificate Policy section of these Operating Rules.

Relevant Documents and Agreements

- * Agrees to abide by these **Operating Rules**, including **Section C. Authentication Certificate Policy** (Certificate Policy), and warrants that any internal documented practices, such as a Certificate Practice Statement, are consistent with these Operating Rules and the included Certificate Policy.
- * Signs **Certificate Manufacturer Agreement**.

D.14. Role: Solution Providers

Functions

- * Provide products and services necessary for State Partners to conduct OBI-Compliant transactions via the EMall; Page 836 of 1794

- * Conduct initial system set up and testing;
- * Upon agreement and request, provide ongoing support to the EMall Operations Administrator as contracted and/or on a time and materials basis.

Relevant Documents and Agreements

- * Agrees to abide by the **Operating Rules**.
 - * Signs contract and agrees to Task Order with Policy Authority for provision of services and related products.
-

E. Technical Requirements

For this pilot, the State User Department agrees to comply with the technical standards which are detailed below:

E.1. User Personal Computer:

The minimum computer requirements and configuration is detailed below:

E.1.1. Internet and World Wide Web Connectivity

A computer capable of accessing the World Wide Web (WWW), which implies connectivity to the Internet using the TCP/IP protocol.

E.1.2. Hardware:

- Pentium Processor
- 32MB memory
- 10 MB of available disk space on the hard drive
- 10/100 Ethernet network interface card
- A mouse
- Year 2000 compliant
- Monitor: 17 inch or greater SVGA monitor, with a minimum of 800X600 pixels of resolution
- ADA compliant

E.1.3. Software:

- Windows 95 or Windows NT 4.0 Workstation

- A 4.0 or higher version of the Netscape Navigator or Internet Explorer browser to allow the use of Secure Sockets Layer (SSL) 3.0
- A Public Key Certificate to be installed within the User's browser and used to authenticate the identity of a User will be issued by the Certificate Manufacturer contracted to provide services to the EMall
- Year 2000 compliant.
- ADA compliant

Comparable hardware and software is acceptable but resolution of problems arising from their use is the sole responsibility of the User's department.

E.2. Supplier Partner

Every party that agrees to perform the role of a Supplier Partner must, at a minimum, provide a web-based catalog that is compliant with the OBI 1.1 specification, as referenced under these Operating Rules.

E.3. Physical Security of Computing and Network Resources

The EMall Web Server must be kept in a physically secure location such that unauthorized persons can not gain physical access to the server without breaking and entering. There are no physical security requirements for Users during the course of the pilot, however, no User may permit an unauthorized person to gain access to a computer that is currently accessing a restricted area of the EMall server (that is, once a User logs onto the system with a user name, password and Public Key Certificate, that User should not leave their computer accessible to any other person until logging off the EMall server). There are no physical security requirements for Suppliers during the course of the pilot. The Certificate Manufacturer must assure that no unauthorized personnel may gain physical access to the private key for the root Certificate for this pilot or may otherwise become capable of manufacturing unauthorized Public Key Certificates.

F. Duties and Obligations of the Parties

F.1. Creation of Legally Binding Purchases

A valid OBI Order must be generated as the result of the authorized approval process specified in Section D of these Operating Rules. Every valid and enforceable sale of goods through the EMall pilot resulting from an OBI Order shall be subject primarily to the underlying contracts between the relevant Supplier and State User and also shall be subject to these Operating Rules and related agreements as well as the terms

and conditions within the OBI Order itself. In order to be merged into the final terms of a purchase, any provisions inserted into an OBI Order Request must conform to the OBI Specification as implemented within the EMall pilot. The terms ***OBI Order Request*** and ***OBI Order*** are to be construed in accordance with the OBI 1.1 specification, as referenced in these Operating Rules. For purposes of this section, the term ***EMall Server*** shall mean the web server hosted on behalf of the State Partners for the purpose of conducting OBI-compliant transactions and shall include the EMall Transaction Server referenced in Section C of these Operating Rules. For purposes of this section, the term ***Supplier Server*** shall mean the web server of a Supplier Partner for the purpose of conducting OBI-compliant transactions, including the Supplier Transaction Server referenced in Section C. of these Operating Rules.

F.1.1. OBI Order Request

An OBI Order Request shall constitute a contractual offer by the Supplier Partner to sell the specified commodities at the specified price and other included terms once it has been successfully posted by the Shopper's web browser to the EMall Server at the agreed upon post-back URL.

F.1.2. OBI Order

An OBI Order shall constitute a contractual acceptance by the transacting State Partner once it has been successfully posted by the EMall Server to the Supplier Server at the agreed upon post-back URL.

F.2. Notice

Every party that has been authorized as a participant after having signed and delivered a participation agreement for the EMall pilot is entitled to notice of any proposed amendment to these Operating Rules at least 14 calendar days prior to said amendments taking effect, unless otherwise agreed by all the parties. In the case of a State Partner, the person(s) who sign the State MOU and each authorized State Coordinator are entitled to receive notice and may be requested or required to pass along such notice to each subordinate User within their state if appropriate. Notice may be communicated via e-mail, fax or other reasonable means, however, unless notice is delivered via U.S. Postal Mail, the Policy Authority must confirm that each party so entitled has in fact received notice. An e-mailed reply confirming receipt by a party to the Policy Authority is a valid means to confirm delivery of notice to that party.

F.3. Participation Agreements

As noted under these Operating Rules, a party that performs an authorized role within the EMall must sign an agreement, known generally as a Participation Agreement. A key function of each Participation Agreement is to signify the assent of each party to abide by these Operating Rules. Parties who will assume a role within the EMall pilot may retrieve a current version of their respective agreements in PDF form from the official EMall web site. These agreements must be completed, signed, and returned to the EMall Business Administrator in order for any person to become an authorized EMall Pilot Participant.

F.4. Confidentiality

Unless otherwise specified in these Operating Rules and related agreements and to the extent permitted under applicable law, all personally identifiable information related to the EMall pilot, including User information, usage statistics related to an individual User, the names of administrators, any telephone, address or other individually identifiable data should be considered confidential and should not be disclosed to any person outside of the EMall pilot. Similarly, no Pilot Participant should make any public statements including press releases, information available on a web site and slide presentation related to the EMall pilot or about any other person or organization's participation in the EMall pilot, unless that statement has first:

- * appeared on the official EMall web site, or
- * appeared in the public press, or
- * been authorized by an EMall Administrator, or
- * is a matter of public record under applicable law

F.5. Intellectual Property

These Operating Rules are subject to Copyright by the Commonwealth of Massachusetts in its capacity as sponsor of the Multi-State EMall. All rights reserved. Permission to reproduce this document is hereby granted provided that the following limitations on this right are observed: (1) all copies must clearly indicate that this work is published by and attributed to the Commonwealth of Massachusetts in its capacity as Policy Authority for and sponsor of the Multi-State EMall; and (2) all copies must include this notice of copyright.

"Multi-State EMall" is a trademark of the Commonwealth of Massachusetts.

F.6. Alternative Dispute Resolution

Disputes between a State User and a Supplier regarding the purchase of goods, including pricing, quality or service guarantees and remedies, shall be governed according to the terms and conditions contained within the underlying contract for the purchase of goods as between those parties. Disputes arising out of or related to the application of these Operating Rules and related Participation Agreements shall be resolved in accordance with the provisions of these Operating Rules and related agreements, and by agreement between the parties, where possible, through direct negotiation or, if appropriate, through voluntary mediation by a mutually agreed upon Mediator.

Depending upon the nature and gravity of a given dispute, as well as the geographic distance of the parties, use of Online Alternative Dispute services may be appropriate. Such services include the Virtual Magistrate program (<http://vmag.vcilp.org/>) and, generally, the services referred to in the Massachusetts Information Technology Division's background paper on Online ADR (<http://www.state.ma.us/>

[itd/legal/adr.htm](#)). Use of Online Alternative Resolution services is explicitly permitted under these Operating Rules, if otherwise agreed upon by all the parties. In the event that parties are unable to reach agreement directly or through the use of mediation or other voluntary methods of Alternative Dispute Resolution, then, to the extent permitted by law and relevant regulation, all such disputes shall be subject to binding arbitration by a mutually agreed upon arbitrator of the American Arbitration Association. The costs of any form of Alternative Dispute Resolution shall be paid equally by the disputants or as otherwise agreed by the parties.

F.7. Governing Law

Disputes between a State User and a Supplier regarding the purchase of goods, including pricing, quality or service guarantees and remedies, shall be governed according to the law of jurisdiction so noted in the underlying contract for the purchase of goods between those parties, or, if no such jurisdiction is so noted, then it shall be deemed to be the laws of the state of the User. Disputes arising out of or related to the application of these Operating Rules and related Participation Agreements shall be governed according to the law of the Commonwealth of Massachusetts.



[10 captures](#)

6 May 02 - 21 Sep 05



SEP	MAY	NOV
	22	
2002	2003	2004

[Close](#)

[Help](#)

Operating Rules

*For use in the Electronic Procurement Project
Known as the "Multi-State E-Mall"™*

Draft Version 3.0
July 18, 2000

COPYRIGHT NOTICE

Copyright © 2000 by the Commonwealth of Massachusetts. All rights reserved. Permission to reproduce this document is hereby granted provided that the following limitations on this right are observed: (1) all copies must clearly indicate that this work is published by and attributed to the Commonwealth of Massachusetts, and (2) all copies must include this notice of copyright.

A. Scope

These Operating Rules govern use of the Multi-State EMall (the EMall). These Operating Rules apply to every participant in the EMall. No party may play any role or otherwise act as a participant in the EMall without the prior approval of the Community Sponsor, currently the Commonwealth of Massachusetts Operational Services Division (OSD). The Commonwealth of Massachusetts possesses sole ownership, management and control over participation within the EMall and the Commonwealth shall be the final arbiter of all questions, issues, disputes and controversies arising out of or related to the EMall.

A.1 Intended Purpose and Authorized Use

The intended use of the EMall is for electronic procurement by participating public entities of goods and services from private suppliers who are legally authorized to sell in accordance with valid underlying contracts. The EMall may only be used for authorized purposes. The OSD may modify

Page 842 of 1794

these Operating Rules with two weeks notice by publishing the proposed revised draft at the EMall URL. The OSD may modify these Operating Rules at any time and without notice when it believes there is it is necessary to protect the right or property of the Commonwealth of Massachusetts.

A.2 Electronic Form of Operating Rules, Contracts and Agreements

These Operating Rules and associated contracts or agreements may exist solely in electronic form and shall not be unenforceable or invalid solely on the grounds that they do not constitute a writing.

B. Boundary of EMall Community

All buyers and other users must receive approval to participate in the EMall from the OSD directly, which may include an online registration process if authorized by OSD. Upon being approved as a buyer in the EMall, a party shall receive a user name and password allowing secure, authenticated transactions within the EMall. It is incumbent upon every buyer to safeguard their password and user name. The user name and password combination are created to designate an authorized member of the EMall community. Unauthorized use of a parties password could result in binding quotes by suppliers or binding purchase orders by buyers.

C. Creation of Legally Binding Quotes and Purchases

A valid OBI Order must be generated as the result of the authorized approval process specified by the OSD. Every valid and enforceable sale of goods or services through the EMall resulting from an OBI Order shall be subject primarily to the underlying contracts between the relevant Supplier and State User and also shall be subject to these Operating Rules and related agreements as well as the terms and conditions within the OBI Order itself. In order to be merged into the final terms of a purchase, any provisions inserted into an OBI Order Request must conform to the OBI Specification as implemented within the EMall system. The terms ***OBI Order Request*** and ***OBI Order*** are to be construed in accordance with the OBI 1.1 specification. For purposes of this section, the term ***EMall Server*** shall mean the EMall server or servers hosted by Intelisys for the purpose of conducting OBI-compliant transactions. For purposes of this section, the term ***Supplier Server*** shall mean the web server of a Supplier Partner for the purpose of conducting OBI-compliant transactions.

C.2 OBI Order Request and Quotes

Subject to applicable law and the pre-existing contracts for procurement between the parties, an OBI Order Request and any related Quote shall constitute a contractual offer by the Supplier Partner to sell the specified commodities at the specified price and other included terms once it has been successfully posted by the Shopper's web browser to the EMall Server at the agreed upon

Page 843 of 1794

post-back URL.

C.2 OBI Order

Subject to applicable law and the pre-existing contracts for procurement between the parties, an OBI Order shall constitute a contractual acceptance by the transacting State Partner once it has been successfully posted by the EMall Server to the Supplier Server at the agreed upon post-back URL, provided that an obligation to pay for goods is contingent upon delivery and acceptance of conforming goods.

D. Intellectual Property and Confidentiality

D.1 Copyright and Trademark

These Operating Rules are subject to Copyright by the Commonwealth of Massachusetts and the "Multi-State EMall" is a trademark of the Commonwealth of Massachusetts.

D.2 Ownership

It is acknowledged that the Community Sponsor owns all right and interest in the ecPortal Transaction data and content, except for IEC's rights to include such data in the aggregate transactive information. The details of individual transactions, including but not limited to the buyers names, phone number, shipping address, billing codes, products, product costs, est. will not be disclosed outside the Community, absent a valid court order or other legally binding requirement to disclose.

D.2 Confidentiality and Disclosure

Unless otherwise specified in these Operating Rules and related agreements and to the extent permitted under applicable law, all personally identifiable information related to the EMall pilot, including User information, usage statistics related to an individual User, the names of administrators, any telephone, address or other individually identifiable data should be considered confidential and should not be disclosed to any person outside of the EMall system. Similarly, no EMall Participant should make any public statements including press releases, information available on a web site and slide presentation related to the EMall or about any other person or organization's participation in the EMall pilot, unless that statement has first:

- * appeared on the official EMall web site, or
- * appeared in the public press, or
- * been authorized by an EMall Administrator, or
- * is a matter of public record under applicable law

E. Governing Law

Disputes between a State User and a Supplier regarding the purchase of goods or services via the EMall, including pricing, quality or service guarantees and remedies, shall be governed under the laws of the Commonwealth of Massachusetts.

F. Liability Disclaimer

EXCEPT AS EXPRESSLY PROVIDED IN THESE OPERATING RULES, ALL WARRANTIES, CONDITIONS, REPRESENTATIONS, INDEMNITIES AND GUARANTEES WITH RESPECT TO THE EMAIL, WHETHER EXPRESS OR IMPLIED, ARISING UNDER LAW, CUSTOM, PRIOR ORAL OR WRITTEN STATEMENTS BY THE COMMONWEALTH, ITS AGENTS OR OTHERWISE (INCLUDING, BUT NOT LIMITED TO ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT) ARE HEREBY OVERRIDDEN, EXCLUDED AND DISCLAIMED.

-- end --

IS TECHNOLOGY FOR SECURITY ADEQUATE?.....	125
BACKGROUND.....	125
Security Requirements for the EMall.....	125
RESULTS.....	127
User Authentication and Authorization.....	127
Server Authentication and Transmission Security.....	128
Data Security.....	130
Was the security implementation adequate?.....	130
SUMMARY.....	131
RECOMMENDATIONS.....	132
Security Administration Should be Decentralized.....	132
Client Certificate Implementation Should be Reconsidered.....	132

Hypothesis Eight

Is technology for security adequate?

Background

Shopping, requisitioning, and ordering in the EMall take place over the public Internet utilizing browsers and servers. It follows that ensuring the security and integrity of all activities and transactions is key to acceptance and widespread adoption of the EMall concept by all parties involved. Further, given that Users are conducting real buy-sell transactions during the EMall pilot, strong security is a prerequisite to the states' ability to exercise their fiduciary responsibilities to taxpayers.

Security Requirements for the EMall

There are two major categories of security requirements for the EMall. The first category includes the requirements specified by the Open Buying on the Internet (**OBI**) standard v1.1. The second category includes all the pre-existing security requirements encompassed by the business processes and systems infrastructure. These two sets of requirements are discussed briefly below. The EMall Operating Rules document provides a greater level of detail about these security requirements.

The OBI v1.1 specification requires the use of X.509 v3 digital certificates for certain communications between Buyers and Sellers. Specifically, authentication via digital certificates are required for Shopping sessions, also referred to as Requisitioning, and for Ordering, or sending back approved Orders to a Supplier. Specifications require that Communications during these sessions are secured via SSL3 encryption.

The business processes automated by the EMall and the network infrastructure within which the EMall exists have various pre-existing security requirements that must be integrated into the application. The business process security requirements encompass many business rules and internal control principles that assure the privacy and legitimacy of transactions conducted via the EMall.

Following are examples of business process security requirements:

- Shoppers can only view those items in a Supplier's catalog that correspond to the contracts and pricing agreements which the Supplier has with the Shopper's state.
- Only authorized Shoppers can complete Order Requests with Suppliers.

- Before an Order Request, or Requisition, can become a transmitted Order, it must be forwarded to and approved by as many authorized Approvers as each state's internal control procedures dictate.
- The application must maintain an audit trail of provable events to assist in any Order dispute resolution.

Participating states access the EMall server via the Internet. To maintain the security of the Commonwealth of Massachusetts' internal networks, the EMall application must comply with the Commonwealth's Public Access Architecture. Compliance with these requirements also insures that the EMall database is appropriately secured from possible infiltration from the Internet and other unauthorized users. Finally, the application must also take into account various security and internal control requirements dictated by back end systems such as payment and accounting applications.

Results

This section describes the actual security implementation for the pilot and identifies some of the major issues encountered. For ease of discussion the security implementation is divided into three categories – user authentication and authorization, server authentication and transmission security, and data security. It should be noted there is considerable overlap among these areas.

User Authentication and Authorization

User authentication ensures that access to the EMall is restricted to only authorized users. Authentication is also an integral part of access control or authorization that limits the types of activities individual Users are allowed to conduct, as well as insuring that unauthorized visitors are not allowed access to privileged information. However, it's important to remember that authentication and authorization are not the same thing and that one should not be confused with the other.

Authentication for access to the EMall server is implemented via browser certificates, also referred to in this document as client certificates, and via user ID and Password. This implementation provides "two-factor" security since it requires something you have, that is, the individual certificate, and something you know, that is, the user ID and Password. Authorization is handled by the EMall application utilizing the user ID and Password in combination with the access control database where roles and permissions are specified for each user.

Motorola provided client certificates for EMall users in its capacity as Certificate Manufacturer. The EMall project manager served as "Registrar," or the person from whom authorized users request certificates, and forwarded requests for certificates for authorized users to the Certificate Manufacturer. The Operating Rules, Section C, describes the Certificate Policy in detail. The Operating Rules are available at <http://emall.isa.us/operatingrules.asp>.

Following are the major user authentication and authorization issues encountered during the EMall pilot implementation.

- The public/private key pairs corresponding to the Motorola certificates were generated off site at Motorola and not on the User's PC. Consequently, Users with Microsoft Internet Explorer browsers were not able to employ the security feature that prompts a User for a password before they can access the certificate. For enhanced security, it is preferable for the keys to be generated and stored in the individual User's PC.
- The Motorola client certificates were sent to users in floppy disks via mail. A letter containing the access password was forwarded to the user separately. A faster and less costly solution is to

provide an online request and access mechanism. This would improve not only the security of the certificates which can get lost on route or be delivered to the wrong recipient, but also would facilitate the management of users and certificates.

- A number of installation problems were encountered when loading client certificates into PCs. Most of these problems could be traced back to browser versions and, in the case of Microsoft Internet Explorer, the need for registry edits. To enhance security and for compatibility with the Motorola certificates, specific versions of 128 bit browsers were required. This meant that most users had to upgrade or reload browsers. Microsoft Internet Explorer further required that edits be done on the system registry after browser installation. All this required system staff intervention, thereby increasing resource costs as well as creating another potential security problem. In some states, after securing the correct browser environment, system staff went on to load the certificates for users compromising the secrecy of the user's certificate password.
- The IEC application version used for the EMall does not have password expiration parameters nor does it have rules regarding minimum password length. Both these features would enhance authentication and authorization security.

Server Authentication and Transmission Security

In order to ensure message and session privacy, server certificates are installed in the EMall server and Supplier servers to enable Secure Sockets Layer (**SSL**) encryption. To ease implementation on the part of Suppliers, a Certificate Authority (**CA**) whose root is widely recognized by most browsers issued the EMall server certificate. Likewise, it is expected that widely recognized CA's also issue certificates installed in Supplier servers to avoid having to import special roots into the EMall server. While these so-called "public label certificates" do ease distribution of the root certificate, they also raise concerns regarding bounding the community of trust among business partners (see [Hypothesis Nine](#)).

The OBI v1.1 specification requires that communications during certain sessions between Buyers and Sellers be authenticated and encrypted via SSL3. SSL3 requires mutual authentication between browser and server (please see <http://home.netscape.com/eng/ssl3/> for more detailed information). The sessions that require SSL3 are Shopping sessions and Ordering. Because the EMall server is accessible to Users in participating states via the Internet, the initial user log-in session is also authenticated and encrypted using SSL3.

A number of issues were encountered in the implementation of server authentication and transmission security. These issues could be traced back to a lack of documentation and functionality regarding the IEC Enterprise software version used in the EMall's handling of SSL3 sessions as dictated by the OBI specification as well as customization required by the EMall's need to secure user log-ins via SSL3. In addition, some of the issues encountered were due to the idiosyncrasies of the various Web servers used by Suppliers and their varying treatment of CA roots. Following are the major issues encountered:

- The EMall implementation of the IEC Enterprise application was the first instance where a server certificate was utilized with this product. The implementation was problematic requiring Internet Explorer v3.0 for installation while Internet Explorer v4.0 was required for the operation of the IEC application.
- When a user attempts to log into the EMall, the application takes the client certificate's common name and matches it against a valid user name in the application database. However, initially the application did not check the CA name to verify that the EMall authorized certificate issuer supplied the client certificate. This functionality had to be programmed.
- There was one instance in which a Supplier used a server certificate that was issued internally and not generally recognized by the EMall server. The certificate's root had to be imported into the EMall server.
- The implementation of SSL3 for Order transmissions from the EMall to a Supplier was very problematic. It was assumed that the presence of server certificates on both the EMall Server and the Supplier server would be sufficient to establish the SSL3 sessions. However, after several weeks of unsuccessful transmissions and trouble-shooting with the Suppliers involved, it was discovered that the IEC application on the EMall server needed a client certificate in addition to the server certificate. This undocumented requirement necessitated the creation of an "Intelysis Service" user account to associate with the client certificate and the creation of a new NT user profile.
- Motorola manufactured the User certificates employed in the EMall. Since Motorola's root is not generally available in browsers and Web servers, Suppliers had to install the root in their servers. Some early versions of Web servers could not install the subordinate EMall root and instead required installation of the original Motorola root. This highlighted the importance of specifying baseline Web application versions for Suppliers.
- SSL3 sessions by themselves do not verify identity or authenticate users. Once the client and server recognize each other's certificates as being "trusted" and keys are exchanged, the encrypted session can begin. To verify identity and use other information contained in the client certificate, the application on the server must be programmed to "parse" the certificate. OBI recommends that the Supplier use the common name and organization information to authenticate Shoppers and establish the appropriate catalog profile. The majority of EMall pilot suppliers chose not to incur the additional development costs entailed by parsing certificate information. Only four EMall Suppliers are parsing the certificate information during the pilot. Instead, User information contained in the IEC application database is used to identify users and to route them to appropriate catalog profiles.

- A similar issue was encountered during SSL3 sessions established to secure the sending of transactions between Supplier servers and the EMall server. Suppliers should be parsing the EMall client certificate to authenticate the identity of the server. No Supplier is parsing certificates for verifying server identity as part of the transmission of transactions during the pilot.

Data Security

The EMall databases are stored in a server located inside the internal firewall that does not permit inbound HTTP traffic from external sources. These databases are physically separate from the EMall application server located in the DMZ. One issue of concern was identified through the pilot experience and is described below. We believe this issue is now satisfactorily addressed in a subsequent version of IEC Enterprise:

- Changes made by administrators to the databases are not audited by the application. This affects both our ability to execute change control and to create an audit trail of changes to the databases.

Was the security implementation adequate?

Before this question can be addressed fully it is important to remember that the EMall pilot implementation utilized two layers of often-redundant security. The first layer was provided by the security features of the IEC application such as user IDs and passwords, access control lists, and hidden code transmitted during transactions. The second layer was provided by the use of client and server certificates as specified in the OBI v.1.1 specification.

Given this scenario, we can say that the security implementation was adequate with a few issues identified above concerning functionality limitations of the IEC Enterprise application version used in the pilot. Given the closed nature of the EMall community and the identification of identities and roles for each EMall participant within the IEC application databases, the use of client and server certificates, other than for the establishment of SSL2 encryption, seems a bit redundant. In fact, during the pilot only four of the participating Suppliers chose to parse client certificates for identity information and state affiliation.

The most significant security flaw encountered during the pilot involves the possibility of internal threats due to the fact that the application does not audit administrative changes. As mentioned previously, this limitation has been addressed in subsequent versions of the application.

Summary

While the OBI v.1.1 specification requires the use of certificates during Shopping Sessions and Order transmissions, the value certificates add above and beyond the security features of the IEC application is questionable. The authentication and access control features of the application appear to be sufficient to satisfy the identified security requirements. The only exception to this is the encryption function (SSL2) that server certificates make possible which is crucial in securing transmissions that are conducted via the Internet. This function, however, does not require the use of client certificates.

Our experience with certificates during the EMall pilot has reinforced several impressions from previous experiences with pilot certificate implementations to date:

- The operating environments within which certificates function are of prime importance. Browser versions, Web server software versions and application characteristics all play important roles in determining whether certificates will load and operate as intended.
- The application programming required to parse certificates so that their contents can be used for authentication and other purposes is not trivial and requires additional resource commitments on the part of business partners.
- The management of certificates (including request, issuing, installation, revocation and audit trails) is also not trivial. Management overhead is eased to the extent that processes can be automated.
- The amount of support required by users and business partners during certificate implementations is considerable.

In conclusion, while the non-certificate technology for security is adequate for the implementation of the EMall, the use of certificates for security (other than SSL2 encryption) is a resource-intensive endeavor, is not seamless and requires considerable custom programming. Further, the authentication functionality provided by certificates appears to be redundant with the security functionality available in the application.

Recommendations

1. Security Administration Should be Decentralized

The administrative approach to security was very centralized in the pilot. The management and technical aspects of security administration will have to be distributed in a production system in order to make it more manageable and efficient. Specifically,

- The EMall production system's technical architecture should reflect distributed responsibilities for user authentication.
- A set of flexible but minimum standards for user identity proofing should be made part of the Operating Rules.

2. Client Certificate Implementation Should be Reconsidered

Given the onerous nature of implementing client certificates, as evidenced by the need for increased local technical staff support, inordinate central administrative support and significant additional custom coding needed to provide core functionality, the advisability of end-user certificate implementation as part of the EMall should be re-considered. The following issues should be kept in mind:

- In the context of a sound, distributed organization-to-organization security system utilizing protocols such as IP-Sec, client certificates to authenticate individual Buyers to external Suppliers may be unnecessary.
- The cost of a full-blown client certificate “solution” must be weighed against both the benefit provided by this redundant level of security and the business and legal risks resulting from breaches to authentication mechanisms. It should be noted that other potential benefits derived from client certificates such as confidentiality, non-repudiation, and message integrity are provided in the EMall by a variety of other application, system and legal rules.
- Should the EMall production system continue to support the OBI standards, the Commonwealth, as a member of the OBI Consortium, should communicate the potential need to revise the certificate requirements in view of our difficult experience in implementing this aspect of version 1.1 of the OBI standard.

IS THE LEGAL/BUSINESS MODEL ADEQUATE?.....	133
BACKGROUND.....	133
The EMall Legal and Business Model.....	134
Existing Context: Procurement Statutes, Regulations and Policies.....	134
Legal and Business Model Architecture for the Pilot.....	136
Designating Roles and Functions.....	136
Operating Rules and "Opt In" Agreements.....	137
RESULTS.....	139
Individual User Opt In Contracts Too Cumbersome for B2B	139
Flexibility of Model Can Facilitate Potential Outsourcing.....	139
Operating Rules Revision and Notice Process Works Well.....	140
State Digital Signature Statutes Can Be a Barrier to Entry.....	140
Use of Client Certificates Pose Unnecessary Problems.....	141
The Pre-Packaging of Public Label Root Certificates Creates Business, Legal and Technical Problems.....	142
EMall Server Root Certificate Issues.....	144
EMall Supplier Public Label Server Certificates and Public Label Roots in User Browsers.....	145
EMall Transaction Server Certificate Issues.....	145
SUMMARY.....	146
RECOMMENDATIONS.....	147
The EMall business/legal framework of Operating Rules and Opt-In Agreements should be retained with appropriate modifications.....	147
The use of digital certificates should be carefully reconsidered.....	147
Contractual agreements for EMall products and services will have to be revised.....	148

Hypothesis Nine

Is the legal/business model adequate?

Background

The EMall Pilot, an innovative government initiative, is in line with current business trends toward electronic commerce. Business-to-business electronic commerce (B2B) comprises the vast majority of the emerging digital economy, according to commercial and other data tracked by the U.S. Department of Commerce (see, for example, www.ecommerce.gov for recent government studies). Retail e-commerce may constitute only between seven and fifteen percent of the estimated \$102 billion in e-commerce activity in 1998, with the rest conducted between businesses. While this new method of conducting business is already significant and has expanded rapidly by ordinary standards, most commentators predict that we still stand at the cusp of truly remarkable growth in this market. In its 1999 prospectus of the Emerging Digital Economy, the Department of Commerce cites estimates that B2B commerce will top \$1.2 trillion by the year 2003. More recent estimates are even more optimistic.

As a Massachusetts state government initiative to facilitate multi-state, web-based procurement, the EMall pilot is a type of business-to-business electronic commerce application. In most ways, the EMall pilot is representative of B2B transactions, however, there are some aspects of this pilot which are not typical of most private sector applications. One of the important ways in which the EMall pilot differs from nearly all other e-commerce is that one party in each transaction is a government, the state buyer, and the other party is a private company, the contracted Supplier. Another way in which the EMall Pilot differs from most e-commerce activity is that it constitutes an aggregation of Buyers who act together within a single technical, business and legal system to effect their online commerce. Finally, the EMall Pilot is distinct in that it has been sponsored, subsidized, and administered by a single government entity, the Commonwealth of Massachusetts.

The following section describes the EMall business and legal model in some detail.

The EMall Legal and Business Model

Existing Context: Procurement Statutes, Regulations and Policies

As the sponsoring state, Massachusetts had to observe applicable procurement rules in the selection of the technology provider, Intelisys, and the integrator, **SAIC**. These companies became the legal entities responsible for the EMall system delivery based upon a competitive selection among Vendors who had already been awarded contracts to provide such products and services to Massachusetts. These "blanket" vendors had already signed standard terms and conditions necessary to establish a relationship with the Commonwealth, including such terms as liability allocation, indemnification and assignment rights.

SAIC became the primary contracted party. SAIC sub-contracted to Intelisys, and Intelisys sub-contracted to Motorola, the company that provided certificate manufacturing services for the EMall pilot. Within these sub-contracting arrangements, the Commonwealth required each party to demonstrate a capacity to meet the business and technical requirements of the EMall pilot prior to permitting them to provide any service or product. Once these government procurement formalities were in place, each vendor agreed to contracts through which they opted into the same types of trading partner Operating Rules as is typical in private e-commerce systems.

The basis of public procurement law in the Commonwealth of Massachusetts is that purchases of goods and services be conducted in an open, fair and competitive fashion. It is a key tenet of the procurement rules that the Commonwealth achieves "best value" as a result of a procurement. This may be achieved by such criteria as attaining the lowest price, or it may be the result of higher levels of quality or an ability to deliver the product or service more quickly - depending upon the circumstances relevant to a given procurement.

Other states also have procurement requirements for competitive bidding prior to awarding a contract, as well as other requirements. Maverick buying and incidental purchases aside, it is typical that no state may purchase goods from a Supplier that has not first been awarded a contract by that state pursuant to applicable procurement processes. Some states will allow the purchase of goods from a Supplier that has been awarded a contract to sell such goods to another state if that state has substantially similar procurement regulations. States that have entered into joint purchasing agreements, also known as cooperative procurement agreements, may also purchase from Suppliers that are primarily associated with another state or with a joint venture among several states (see [Hypothesis Two, Existing Cases](#)).

Since the transactions conducted via the EMall system constitute the purchase of goods, it was necessary to assure that the EMall sufficiently accommodate each state's procurement requirements. These requirements created some additional legal and technical overhead beyond what would have been required by non-public buying entities. Although large private organizations also become encumbered by

inordinate and unnecessary layers of processes related to procurement of goods, government remains the widely accepted leader in this area.

The EMall system was designed so that it could support and reflect quite rigorous requirements for any given Buyer without slowing or complicating the procurement process for other Buyers using the same system. Different workflow, approval chains to sign off on purchases, and other unique procurement-related requirements can be flexibly accommodated as part of the core functionality of the Intelysis system. Other requirements necessitated custom coding, kept to a minimum in the pilot, and new business practices surrounding the use of the EMall system.

The perceived need for "browse-only" functionality on the part of some of the participating states illustrates the type of novel legal and business issues raised in the EMall Pilot. The "browse only" Shopper is typically a User who only wants to access a contracted Supplier's catalog, but does not want to build a shopping basket, return a Requisition or place an Order. Perhaps this User simply wants to compare pricing, or look at specific offerings available from the Supplier.

A work-around was needed within the IEC application to accommodate this role during the pilot period because technically there is no way to distinguish a "browser" from a Shopper, that is, one whose goal it is to place an Order with the Supplier. The work-around relied on Supervisor/Approver intervention through the Cancel Request functionality to enforce the "browse only" rules. The procedure included setting up the "browser" as a Shopper with a zero dollar-spending limit. This meant that the "browser" was allowed to fill a shopping cart and bring it back to the EMall for approval. The IEC application then would route the Order to an appropriate Approver. The Approver would then be required to identify the Order as coming from a "browse only" Supplier and cancel the Order.

Under this work-around, it is possible that an Order could be sent to a Supplier from a "browse-only" User without authorization to conduct a purchase. Due to the risks associated with this work-around, a decision was made to suspend "browse only" implementation during the pilot. If states feel that allowing all EMall Users to access all contracted Suppliers' sites is a requirement for the production system, then a solution maintaining approval integrity will need to be developed.

In some cases, a Supplier and a State already had an EDI (Electronic Data Interchange) system in place. A version of the Model Trading Partner Agreement of the American Bar Association had been executed between the parties to such systems in the Commonwealth. Upon evaluation, it was determined that these agreements were not suitable as a basis for articulating the legal relationships among EMall Pilot participants. Among other shortcomings, contracts based upon the Model Trading Partner Agreement envision one to one relationships rather than the many-to-many relationships characterizing the EMall system. In addition, these EDI contracts assumed an outsourced value added network acting as a secure and reliable communications intermediary among the trading partners. By contrast, the EMall required

legal arrangements that were responsive to the special risks and processes associated with transferring business information via the Internet. In addition, the EMall legal structure had to be scalable and extensible, that is capable of supporting an ever growing population of users and of supporting dynamic and evolving business practices and modifications in technical processes.

Legal and Business Model Architecture for the Pilot

The legal model was designed primarily to support and reflect the business model for the EMall Pilot, which consisted of a Massachusetts sponsored and run e-procurement system in which other states could participate as buyers and through which a number of private vendors could sell their wares as suppliers. One of the implications of the fact that Massachusetts sponsored this pilot was that executive decisions regarding the technical, legal and business aspects of this project were in the domain of the Commonwealth. Similarly, an implication of the fact that Massachusetts ran the pilot rather than outsourcing the administration of the project was that the Commonwealth also made day-to-day operations and implementation decisions.

During the pilot, Massachusetts served as the Policy Authority, through the EMall Steering Committee, and developed the scope of work for the providers of the technical solution and integrator services as well as the certificate manufacturer. Massachusetts also drafted the Operating Rules that governed the EMall pilot.

Designating Roles and Functions

Though Massachusetts ran the EMall the decision was made to simulate, to the greatest degree practicable, a business and legal model that could be used after the Pilot. Such a model required that one or more additional or alternative parties be capable of carrying out several of the administrative and executive roles that were performed by the Commonwealth. To this end, the major roles were described separately with the various functions grouped accordingly under each role. Likewise, the Operating Rules were crafted with the goal in mind of becoming extensible to different governance combinations among states. Therefore, though the Commonwealth of Massachusetts played several roles in the pilot, each department, division and individual was required to observe all the rights and duties associated with business conducted under each role, just as though a different state or a private sector outsourced entity had performed the role.

By way of illustration, a number of departments within the Commonwealth agreed to participate as EMall Users. These departments were required to sign the same Memorandum of Agreement as executives from other states and each state employee of each such department was required to sign and observe the same terms and conditions. Similarly, some individuals within the Operational Services Division for the Commonwealth sat both on the Steering Committee for the EMall, which acted in the Role of Policy Authority, and also performed as the Technical Administrator or the Business Administrator. These

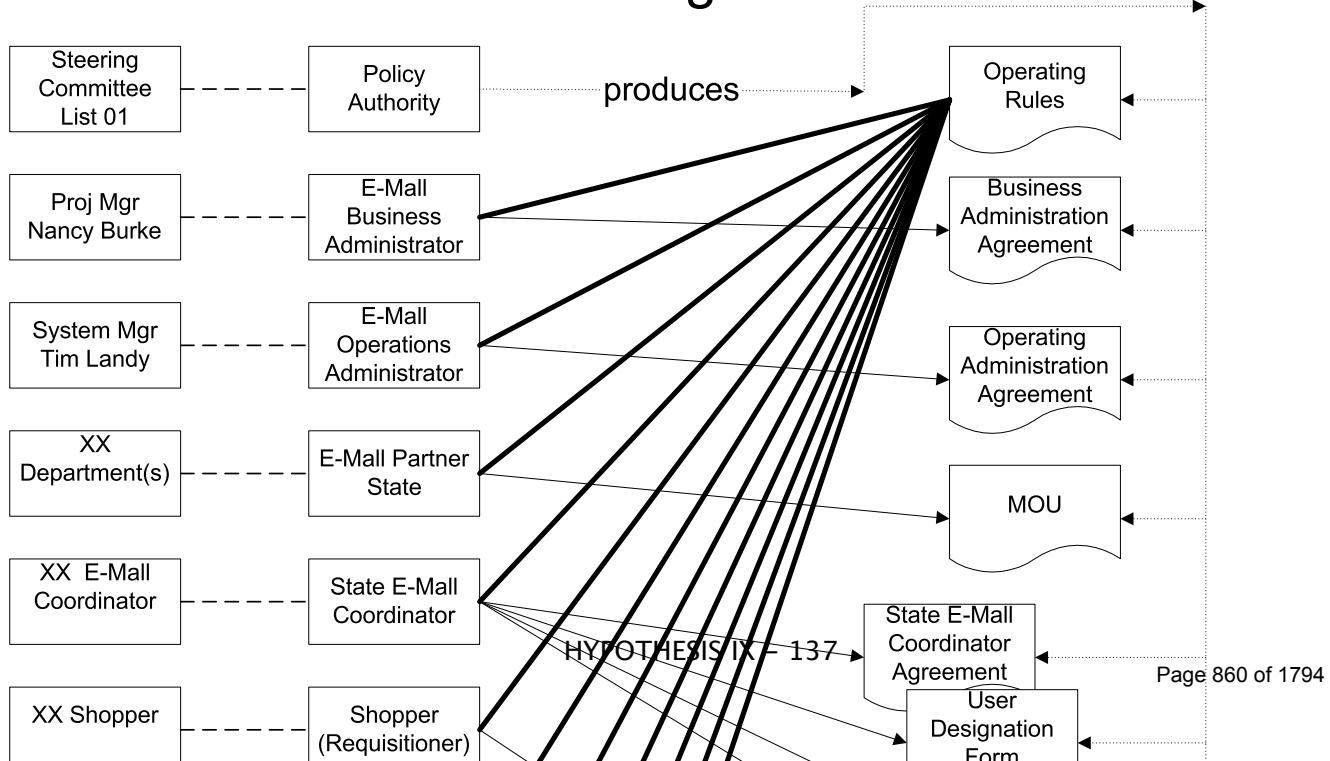
individuals were required to sign an agreement and observe security requirements and to create the same audit trails that are similar to what an outsourced third party administration service would have had to sign. Again, these formalities were carried out primarily for the purpose of describing, testing and assessing the problems and prospects associated with carrying out each role within an EMall environment. They also helped us to better prepare a set of Operating Rules that would need minimal revision if other business parties were to assume any executive or administrative role within the system.

Operating Rules and "Opt In" Agreements

The EMall legal model was premised upon the assumption that parties to this e-commerce system can and should use contractual mechanisms to structure secure, enforceable and reliable business transactions among themselves. To enhance the ease of administration and simplicity of the legal documents, a single overarching set of Operating Rules, rather than many individual long contracts with each participating party, was developed for the EMall Pilot. Each party signed a relatively small "opt in" agreement whereby they agreed to abide by the terms and conditions in the Operating Rules. In this way, as the changing technical or business situations required amendments to the terms and conditions, it was not necessary to re-execute hundreds of individual contracts. Rather, under the "Notice" and amendment provisions of the Operating Rules, every party is given notice of proposed changes and an opportunity to comment and discuss. Once consensus is reached, the Steering Committee (Policy Authority) may execute a change to the Operating Rules. By virtue of each signed opt in agreement, all parties then become subject to the then current terms.

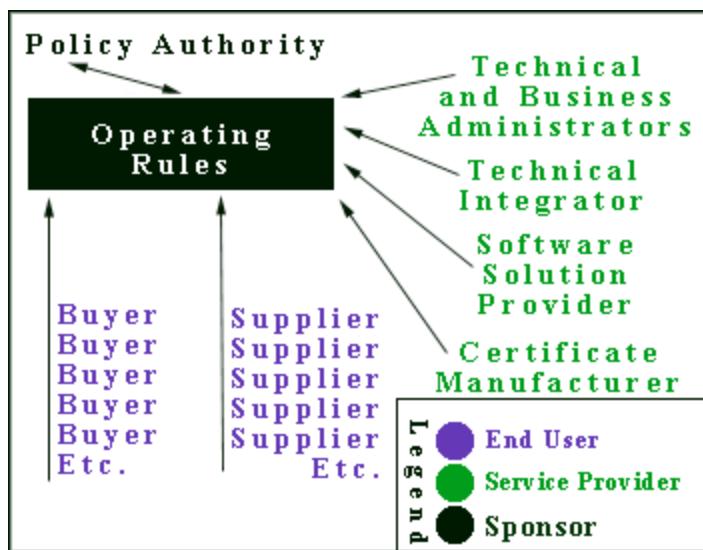
Below, included for purposes of illustration, is a pictorial representation of the interlocking agreements among the parties to the EMall Pilot. Note that any given state actually executes several documents. In

E-Mall Pilot Agreements



addition, buyers and sellers have pre-existing contracts for the sale of goods upon which the EMall legal arrangements rest.

The illustration below clarifies the types of parties based upon their "role" under the Operating Rules. The parties in green are service providers. During the pilot, some service provision was outsourced to external parties (e.g.: the Integrator SAIC, the Certificate Manufacturer Motorola) and others were performed in-house, such as the Technical and the Business Administrator roles which were conducted by staff from the Massachusetts Operational Services Division. The blue represents end users. The buyers are states and the suppliers are private vendors who have contracts to sell to one or more participating states. The black is the policy authority, which was the Commonwealth of Massachusetts during the pilot because the Commonwealth initiated, subsidized and administered the project. The policy authority produced and also agreed to abide by the Operating Rules. The other parties signed agreements whereby they opted into a promise to abide by the Operating Rules and thereby enjoy the benefits of the EMall system. The arrows pointing toward the Operating Rules designate an agreement to abide by the rules.



Results

This section evaluates the EMall Legal/Business model in light of the pilot experiences. The following observations were made:

- Individual User Opt-In contracts are too cumbersome for this business-to-business e-commerce application
- The flexibility of the model can facilitate potential outsourcing
- The Operating Rules revision and notice process works well
- State digital signature statutes can be a barrier to entry
- The use of client certificates pose unnecessary business, legal and technical problems
- The pre-packaging of public label root certificates in web browsers and servers created business, legal and technical problems

Individual User Opt In Contracts Too Cumbersome for B2B

The legal contracts underlying the EMall were, in retrospect, over inclusive and over numerous in view of the costs, benefits and risks associated with the system. While this has the potential to be a multi-million dollar system, the best models in the private sector of similar scope and depth suggest that there is no need for a central intermediate entity to keep signed contracts for every individual buyer within every participating buying institution. The overhead associated with distributing, retrieving, correcting, storing and accessing each such contract was inordinate. The Pilot was of relatively limited scope and it included hundreds of individual user contracts. An implementation system with thousands or more such contracts would be costly and unnecessary in a B2B environment.

Rather, it seems adequate to include additional provisions within the general contracts executed by the buying institutions wherein the executives agree to manage their users. The executives are made responsible to notify each user of certain relevant facts such as obligations to safeguard passwords, duties to maintain integrity of system, and legally binding result of using system to purchase goods. The institution would also have to agree to stand behind the actions of each of its own users to the extent it created certain types of liabilities within the EMall system. Beyond this point, however, each institution should have the flexibility to manage its own users as it sees fit and in accordance with its existing management and technical support systems. In short, a more distributed legal system for individual end buyers is appropriate for the EMall system because the fundamental legal entities that agree to participate are business or government entities and not individuals. Hence, only the organizations should be dealt with directly in future EMall legal arrangements.

Flexibility of Model Can Facilitate Potential Outsourcing

As has been noted, the Operating Rules and the business relationships were designed to allow maximum flexibility in mixing and matching different parties to different roles within the EMall. Outsourcing some of these functions, where economically advantageous, should be eased by the flexible design built into the model.

With the prospect of significant growth in the number of EMall participants in a production system, it may be desirable for the administrative roles such as business manager and technical administrator to be outsourced in a future implementation. The functional processes required for each role have already been established through the course of the pilot, a fact that should ease any potential outsourcing of these roles. It should be noted that the execution of these administrative duties is different from the executive decision making duties associated with the role of Policy Authority - which can not and should not be outsourced. However, a future implementation model may require that additional parties join directly or indirectly through advisory or other committees in the duties of the policy authority.

Operating Rules Revision and Notice Process Works Well

The EMall Operating Rules went through a revision process from version 1.1 to version 2.0 of the Operating Rules during the course of the Pilot. The system notice and comment period operated in a timely and efficient manner. The current version of the Operating Rules is 2.0. It may be advisable to facilitate further automation of the notice, comment and approval process for revision of the Operating Rules through use of e-mail (pushed) and web (pulled) notices, as well as web-based discussion. More automated processes should also be reviewed as part of the contractual opt in process for agreeing to the Operating Rules.

State Digital Signature Statutes Can Be a Barrier to Entry

When the state of Washington was considering joining the EMall pilot, its digital signature legislation posed problems because it required that a licensed "certificate authority" be used to issue certificates for any official business conducted with the state in which a digital certificate was used. The general business and legal model underlying a "certificate authority" is different from the B2B business and legal models that characterize the EMall Pilot.

The B2B relationships in the EMall rely on contracts, agreements and Operating Rules that describe the duties, processes, liabilities and rights of each party. In order to use a Washington state-licensed CA, parties must become subject to the legal rules governing the use of certificates under the digital signature law of that state. That law would create non-standard and problematic legal terms that would conflict with the desired and contracted terms for B2B commerce under the EMall Pilot. Following are some examples:

- The Washington law would require that there be a rebuttable presumption that a document was digitally signed under certain circumstances. The EMall Operating Rules set the terms differently.
- The Washington law would have created a liability limitation for the entity issuing certificates. The EMall contracts set the liabilities differently based on the negotiated terms between the parties.
- The Washington law envisions an "open" use of issued certificates with potentially any party in the world. These terms were different from the bounded and closed use of certificates within the EMall system - where parties are supposed to limit use of certificates only to use with other authorized EMall Parties.
- None of the nationally known certificate providers with whom the EMall Steering Committee discussed outsourcing certificate services have chosen to become licensed under the Washington law. The market has not generally opted to follow the regulatory direction of the Washington law.

Since Washington law restricted their state government from conducting official state business with certificates issued by companies that were not licensed under the law of that state, Washington was unable to participate. The other states that participated in or observed the EMall have no such restrictions and were fully able to agree to the business agreements with the private suppliers and the other participating states. In fact, as far as we know, Washington is the only state that requires that a licensed CA be used with their state government. It is unclear whether Washington would have opted to join the EMall even if the CA problem had been overcome, however, that became a moot point in view of the restrictions under Washington law.

The underlying purpose of these regulatory, technology-specific laws was to bolster use of public-label certificate authorities. The EMall pilot revealed that use of such public label root certificates is itself problematic in a bounded B2B e-commerce environment, as detailed later in this Section of the Evaluation. This session of Congress, legislation in both the U.S. House and the U.S. Senate has been filed and has been reported out of sub-committees which would have the effect of preempting certain types of digital signature specific state statutes. Massachusetts has sent representatives to both chambers of Congress to testify in favor of such a legislative result. Florida has recently captured the distinction of being the first state to voluntarily repeal its CA licensing statute. Though only a few states have such laws in effect, the repeal of the remaining such statutes would simplify and improve the legal environment surrounding use of public key certificate systems like the EMall.

Use of Client Certificates Pose Unnecessary Problems

The use of client certificates presented several difficult and unnecessary legal, business and technical problems. In short, the end user software is not sufficiently mature to warrant use of this technology nor are the business practices. For a full discussion of the use of digital certificates in the EMall please see

Hypothesis Eight. This discussion will concentrate on the legal and business issues raised by the use of client certificates.

Because the pilot used client certificates in its security implementation it became necessary to develop appropriate content for each field in the certificate such as the syntax of the name, the place, and the associated organizations. It quickly became apparent that the X.509v3 field definitions raise far more questions than they answer. For instance, there are no generally recognized conventions regarding the type of content that is supposed to occupy several fields or what that content is supposed to mean. The country code for an institution, for instance, may mean the place it is incorporated, or its primary place of business, or where a particular computer resides, or any other semantic meaning an individual chooses to assume when filling that field with data.

An even clearer example of this difficulty was illustrated in a recent debate among technologists, academics and lawyers participating in the Internet Engineering Task Force PKI group and related groups' e-mail lists on the topic of the "non-repudiation" bit field in an X509v3 digital certificates. If a certificate had the field turned "on" one might wonder if transactions associated with the certificate could not be repudiated. Perhaps even more interestingly, if the field is "off" - does that mean transactions may, will or must be repudiated?

The question of whether a transaction may or may not be repudiated depends on a complex and voluminous array of factors, and the existence of a single bit (on or off) with no additional context is likely to obfuscate rather than clarify the expectation of the parties. A person receiving a certificate with such information out of context in a public system may not correctly guess the meaning intended by the user or issuer of that certificate. It should be noted that this is not as likely in a bounded system, like the EMall, where a finite number of parties agree to details of meanings and processes. The confusion surrounding the presence of these types of fields demonstrates the relatively immature state of public key certificate usage in open systems.

In short, the semantics of the X.509 certificate profiles are not widely understood or accepted and had the effect of slowing rather than facilitating secure electronic commerce in the case of the EMall. In the end, the EMall system used pseudonyms to designate each user rather than using the person's real name. The pseudonym was a user number given by the EMall system much like an account number associated with a bank account.

The Pre-Packaging of Public Label Root Certificates Creates Business, Legal and Technical Problems

The EMall pilot encountered significant difficulties as a result of the inclusion of so called "trusted roots" in off-the-shelf web software. This issue is related to the decision by the major Web browser manufacturers and Web server manufacturers to include root certificates in their software. The result of this decision is that web communications that are authenticated by use of a digital certificate issued by one of the

companies with an embedded root are automatically "trusted." In other words, the web server and/or web browser will indicate that the digital certificate has been issued by a trusted entity and, by implication, may legitimately be relied upon.

This assumption is false in the context of the typical bounded B2B system, and it caused business and legal disruptions in the Pilot. In the EMall, the EMall server and supplier servers use certificates from public label CAs. The primary criteria for judging whether a person or entity is "trusted" to do business within the EMall is whether they have agreed to abide by the Operating Rules and whether they have been accepted by the EMall Administrators as a business partner after due diligence review of application materials. Nothing in the issuance or use of a public label digital certificate qualifies a person or entity to do business within the EMall or to be considered "trusted" in any way. More information on the definitions and implications of public label, or "open" versus "bounded" certificate systems, can be found in the Certificate Authority Rating and Trust Guidelines, issued by NACHA, and available through <http://www.state.ma.us/itd/legal>.

The mere fact that a certificate has been issued by one of the several entities that happen to have a root certificate embedded in commercially available software does not in any way qualify the user of such a certificate to do business in the EMall system. As a business grade application, the EMall requires that parties sign contracts, accept certain liabilities, and otherwise conform to an array of duties and expectations. The use of a certificate was intended to bolster the authentication of parties who were already part of the EMall system.

Even if a so-called "public certificate authority" had issued a certificate to an entity called, say, Universal, Inc., which would not necessarily mean that entity was the same Universal, Inc. with whom the EMall has a business relationship. There are many other such companies that legitimately use the same name such as Universal Studios, Universal Plumbing, and Universal Software Company. The other data beyond the name which may be gleaned from a certificate such as date of issue, and country code does not provide sufficient information from which to make a judgement about whether to rely upon the certificate.

In a non-trivial application like the EMall that supports hundreds of thousands of dollars in trade among hundreds of entities, parties conduct transactions based on trust. Trust-worthiness is determined through actual business reputation, prior course of dealing, recommendation by peers, pre-determined liability allocation and other elements upon which trust is built. A generic public label certificate cannot impart this type of trust.

Just because a certificate authority issued a certificate to an entity with which the EMall has no prior course of dealing, the software should not create an assumption that the person's digital certificate is "trusted" for any business transaction. That person or entity must first be accepted as a business partner,

must sign an agreement to abide by the rules of the system and otherwise meet certain minimal due diligence requirements.

Similarly, even if a certificate were issued by a public CA to an individual or business that had already been accepted as a business partner in the EMall, unless that CA itself agreed to follow the business rules of the EMall, it would be nearly impossible to correlate the issued certificate to the business partner. How many people by the name of John Smith exist in the United States? The underlying agreements for every CA to use the same unique identifier for every individual are years away from coming into existence.

Further, current wisdom regarding privacy of individual information suggests that a single identifier for every individual poses more problems than it solves. Rather, it seems more cost effective and consistent with sound public policy to issue certificates based upon pre-existing relationships. For instance, the EMall came to agreement with an entity, Motorola, to issue unique branded "EMall" certificates to the users of this system. Only legitimate users are entitled to receive EMall certificates for authentication, as with an EMall password.

The premise underlying this decision is that certificates should follow trust, and trust should not follow from a certificate alone. That is, after a business trust relationship is demonstrated, a certificate and other technical means of authentication are appropriate to confirm the identity of the individual or entity that was deemed trusted. No external "third party" certificate authority can make the determination of who or what the EMall will deem as trusted. The definition of a "third party" public certificate authority is antithetical to the business grade requirements of an e-commerce application like the EMall. Only first or second parties to the system have the knowledge to identify any given party as trusted or not trusted.

EMall Server Root Certificate Issues

One of the several difficulties that emerged from the inclusion of trusted roots within server software was that any certificate that was issued by one of the several included CAs would automatically be accepted. Additional custom programming was necessary to block out non-EMall authorized certificate manufacturers. In one test, a VeriSign certificate was acquired in which the name field included the same name as an accepted EMall user. In a test, that certificate was accepted into the EMall application on the EMall server. This was considered to be a serious flaw, since no public label CA does or should restrict issuance of certificates that happen to contain the same names as are correlated to EMall users. However, only legitimate EMall users may gain access to the EMall system.

The EMall system was designed to allow users from across the country and in large numbers to opt into the project. The scalability requirements, however, do not mean that a public label CA is in any way adequate or appropriate to fulfill the business and legal requirements of the EMall. Rather, a genuinely

trusted certificate manufacturer is needed - one that is trusted because it agrees to abide by the business, technical and legal practices designated by the Policy Authority for the commercial system. The critical point here is that if a public label CA were to agree to such requirements, and if it were accepted as a partner, then it would actually be a Certificate Manufacturer and not a Certificate Authority. This is because the "Authority" in a bounded B2B system does not reside with the party that happens to make certificates, rather it resides with the Policy Authority, whom pays for and governs the technical and business processes. Again, for more information on these models and definitions, please see the Certificate Authority Ratings and Trust (CARAT) Guidelines, at www.state.ma.us/itd/legal.

EMall Supplier Public Label Server Certificates and Public Label Roots in User Browsers

The only context in which public label certificates and roots were not problematic involved creation of secure sessions between users with browsers and some web servers of suppliers. In order to set up an encrypted session between the user's browser and the supplier's server, Secure Sockets Layer (SSL) encryption was implemented. Supplier servers with public label server certificates like VeriSign or GTEI CyberTrust could create an SSL session with any commercial off the shelf browser, since the browser already had the root certificate of the public label CA pre-packaged into the software. In this case, however, all that is really needed is encryption and the data in the server certificate was not especially important to users which is typical among all browser users connecting to public label server certificates. Nonetheless, since SSL does not allow encrypted sessions without a server certificate (browser certificates are optional), it was generally easier to use the public label server certificates since they did not require installation of yet another root on each desk top PC of each user in the EMall pilot.

EMall Transaction Server Certificate Issues

In order for an EMall purchase order - also referred to as an "OBI Order" under our technical specifications - to be legally binding, a supplier must be able to determine that it originated from the EMall transaction server. In addition to such data as the IP address and certain message content in the OBI Order, suppliers were directed to check the certificate of the EMall transaction server to assure authentication of origin. The EMall Operating Rules clearly spell out the timing and circumstances upon which allocation of loss rules will shift the legal burden to make good on orders from the seller to the buyer. After an order has been received in accordance with the technical specifications discussed in the Operating Rules, the buyers are "on the hook" to be bound by the transaction.

A public label certificate was used to authenticate the transaction server because a Motorola certificate could not be embedded in the transaction server due to technical configuration limitations. The result of using this public label certificate was that the transaction servers of the suppliers would automatically accept as "trusted" any facially valid order of goods that was transmitted from a source that happened to have a certificate from this public label CA. The public label CA does not constrain its practices to check whether a certificate applicant is a member of the EMall, nor does the public CA accept liability for

transactions gone bad as a result of such reliance. This made it especially worrisome that any EMall supplier may actually trust the so-called "trusted" root. This security and risk-management problem was handled during the pilot by adding certain internal controls and through specially crafted multi-party agreements specifying confidential data associated with valid OBI EMall orders.

The "trusted" roots, in practice, designate certificates that should NOT be trusted, in the context of the EMall Pilot. Ultimately, it was required that the suppliers spend more resources for additional custom programming to parse the certificates in order to distinguish the valid EMall certificate from all others issued by the public label CA. If the public label CA happens to issue another certificate with the same name as the EMall transaction server, then this control will be useless. Whether the public label CA does issue such a certificate is totally out of the control of the Policy Authority or any of the parties participating in the EMall. Motorola, the Certificate Manufacturer for the EMall agreed by contract to stand behind relevant business and technical practices and issued certificates that conformed to the policy requirements of this e-commerce application.

Summary

The advent of e-commerce and the new digital economy is causing a fundamental restructuring of institutions and practices in the public and private sectors. In many ways, the EMall pilot reflects these broader changes in prevailing business models and novel relationships between commercial parties.

The Pilot has shown that the new general business/legal framework developed for the EMall implemented through the Operating Rules and Opt-In Agreements has worked well. The most significant business, legal and technical issues encountered during the Pilot are attributable to the implementation of client and server digital certificates. Following are the specific observations that can be made as a result of the Pilot experience:

- Individual Opt-In contracts are too cumbersome for business-to-business e-commerce
- The flexibility of the model can facilitate potential outsourcing
- The Operating Rules revision and notice process works well
- State digital signature statutes can be a barrier to entry
- The use of client certificates pose unnecessary business, legal and technical problems
- The pre-packaging of public label root certificates in web browsers and servers creates business, legal and technical problems

Recommendations

1. The EMall business/legal framework of Operating Rules and Opt-In Agreements should be retained with appropriate modifications.

The EMall business/legal framework appeared to work well under the Pilot and should be followed in a production system. For purposes of streamlining the process, it is desirable to require opt in contracts only from the participating institutions and not from each individual employee. The institution's contract should include clauses regarding minimum duties with respect to the management of their internal users.

2. The use of digital certificates should be carefully reconsidered

The use of certificates presented inordinate legal and business problems and should be completely re-examined based upon an analysis of the benefits and the costs of such technology as well as the underlying transaction risks associated with the business. The use of internal passwords for users within an institution and of institution to institution authentication (such as with the IPSEC protocol) may be sufficient. Use of certificates simply to authenticate institutional servers, such as with IPSEC, server to server SSL and the like, does not involve the same administrative overhead and can be limited to private label certificates with ease. In this way, local IT administrators may continue to handle individual internal passwords for various systems on their site, but such data as the identities, private authentication data and sensitive security information related to individuals will not flow beyond each institution.

If certificates are used more broadly, it will be important to avoid use or acceptance of so called "public label" certificates or any so-called "trusted root" that is pre-installed in software. Rather, it is important to bring the entity that issues certificates under contract to abide by the policies and business practices associated with the EMall system. Finally, the possibility of using online dispute resolution as provided under the current Operating Rules should be more fully explored as a way to manage risks and to reduce costs.

3. Contractual agreements for EMall products and services will have to be revised.

The contractual agreements through which EMall products and services are provided will have to be considerably revised in view of the fact that the scope of work contemplated was carefully tailored for a pilot only. The need to revisit these underlying contracts will be especially pronounced if a future implementation will entail any change in any product or service provider, or if the Commonwealth is no longer the primary or sole entity responsible for procuring these products or services.

Appendix G: InCommon Federation Attachment

Attachment 1: By Laws of the InCommon LLC

Attachment 2: Operating Agreement

Attachment 3: Federation Operating Policies and Practices

Attachment 4: Federation Participation Agreement

Attachment 5: Federation Participant Operational Practices

Attachment 6: Identity Assurance Assessment Framework

Attachment 7: Identity Assurance Profiles Bronze and Silver

Attachment 8: Federation SAML 2.0 Profiles

Attachment 9: Certification Practices Statement for Client Certificates

BYLAWS OF THE INCOMMON LLC

August 17th, 2005

These Bylaws implement, clarify, and supplement the “Limited Liability Company Agreement of InCommon LLC” (“Agreement”) which created the InCommon LLC (“Company”) under the laws of the state of Delaware. Nothing in these Bylaws shall be construed to be in conflict with the Agreement.

1. MISSION AND PURPOSE

The mission of the InCommon LLC (§3.01)¹ is to create and support a common framework for trustworthy shared management of access to on-line resources. Executive management of the InCommon LLC is carried out by or under the direction of a Steering Committee (“SC”).

In furtherance of its mission, InCommon LLC shall offer, support, and manage a participatory shared identity management federation, the InCommon Federation (“Federation”), for the benefit of education and research in the United States. The Federation will support a community-based common trust fabric sufficient to enable participants to make appropriate decisions about access to on-line resources based in part on information provided to them by other participants. The Federation is intended to enable production-level end-user access to a wide variety of protected resources.

The Steering Committee shall adopt and maintain a set of Federation Operating Practices and Procedures (“FOPP”) that define clearly the goals of the Federation and all important aspects of how the Federation operates. Participants in the Federation will have access to this document and will be expected to base their trust in the Federation organization in part on the practices and procedures described therein.

2. STEERING COMMITTEE

The Steering Committee governs the affairs of the InCommon LLC (§6.01). The Steering Committee acts on behalf of and has the authority to exercise all of the powers of the InCommon LLC except for such authority reserved to The Member in the Agreement. The Steering Committee’s responsibilities include, but are not limited to:

- (i) Promoting the mission of the InCommon LLC;
- (ii) Establishing policies, and delegating authority to and advising the Operations Unit on management and operational procedures of the Federation;
- (iii) Defining levels and classes of Participants in the Federation, as well as the requirements, responsibilities and restrictions associated with each class of Participant;
- (iv) Overseeing the financial affairs of the InCommon LLC and planning for recovery of its operating costs;

¹ All references of this form are to Articles in the Agreement of the InCommon LLC dated Dec 10, 2004.

- (v) Handling dispute resolution for issues arising in connection with the operations of the Federation.

a. Members and Composition of the Steering Committee

The Steering Committee is composed of SC Members nominated by the SC and approved by the InCommon LLC Member (“The Member”) which is Internet2 (§6.01(b)(iii)). The Member appoints the initial steering committee as described in the Agreement. SC Members need not be associated with an InCommon Federation Participant organization.

The Steering Committee must consist of at least seven (7) persons but no more than thirteen (13) persons. If at any time the SC consists of fewer than seven persons due to resignation or other circumstances, the only order of business that may be conducted is nomination of new SC Members.

SC Members shall serve for a three (3) year term. Terms will be staggered so that no more than 1/3 of the Steering Committee is replaced each year. SC Members may serve no more than two consecutive full terms on the Steering Committee. Terms of the initial SC Members are defined in the Agreement.

Members of the Steering Committee are nominated in accordance with procedures established by the Steering Committee. At least two (2) persons shall be nominated for each vacant position. The Member shall nominate and select the Internet2 SC Member. Nomination of new SC Members shall occur prior to the first SC meeting in each fiscal year, or as soon as possible should an SC seat become vacant for any other reason.

SC Members may be removed, with or without cause, only by The Member.

b. Officers

Officers of the Steering Committee serve one (1) year terms. Officers, except for the Chair (see (ii) below), are elected by majority vote of the SC Members prior to any other business at the beginning of each fiscal year. Candidates must be SC Members and may be nominated by any SC Member without second. No SC Member may serve more than three (3) consecutive terms in the same Officer role.

(i) Chair of the Steering Committee

The Chair of the SC shall schedule and call meetings, develop the agenda, conduct business, settle disputes that may arise within the Company, and officially represent, or designate an alternate representative for, InCommon in discussions or other forums. The Chair may call upon the Operations Unit for staff support, including but not limited to scheduling and logistics of meetings and other business.

(ii) Vice Chair of the Steering Committee

The Vice Chair shall act in the absence of the Chair but only at the request of the Chair unless such communication is not possible. The Vice Chair will become the Chair at the beginning of the next fiscal year unless the Vice Chair position is vacant

at the beginning of that fiscal year in which case the Chair shall be elected at the same time and in the same manner as other Officers.

(iii) Secretary

The Secretary is responsible for all documents and official correspondence of the Steering Committee. These responsibilities include, but are not limited to:

- preparation of and distribution to each SC Member an agenda in advance of each meeting;
- preparation of and distribution to each SC Member written minutes of all meetings of the Steering Committee;
- preparation of and distribution to the SC Members any notices received by the Company or otherwise called for by this Agreement to be given by the Company;
- preparation and approval of official correspondence from the SC to the Operations Manager and other parties.

The Secretary may call upon the Operations Unit for staff support, including but not limited to taking and transcribing minutes of SC meetings, and distribution of materials to the SC Members and Federation Participants.

(iv) Assistant Secretary

The Assistant Secretary shall act in the absence of the Secretary at the request of the Chair.

(v) Treasurer

The Treasurer is responsible for the fiscal affairs of the Company. The Treasurer shall report quarterly to the SC on the financial state of the InCommon LLC. The Treasurer shall work with the Operations Manager to review financial reports of income, fund accounts, and expenditures and annual financial audits. The Treasurer shall bring to the attention of the SC any potential issue or concern that might impact the fiscal soundness of the InCommon LLC. The Treasurer may call upon the Operations Unit for staff support as needed. All decisions as to accounting matters, except as specifically provided to the contrary in the Agreement or herein, shall be made by the Steering Committee (§7.03).

c. Meetings

The Steering Committee shall meet regularly no less frequently than each quarter of each fiscal year at a time and place to be determined by the SC. Additional meetings may be called upon request to the Chair by at least two SC Members, The Member, or the Operations Manager. Such additional meetings shall require at least ten (10) days advance notice to all SC Members, except in the case of an emergency as described below. Meetings may be held in person or by conference call or other electronic means that allow full participation by Steering Committee Members, or any combination of the foregoing.

The Chair may declare an emergency meeting of the SC to address any issue for which, in the sole discretion of the Chair, it is critical that the advice or decision of the SC be obtained in fewer than 10 days. No other business may be conducted at such a meeting. The Chair, and/or his or her designee(s), shall use their best efforts to contact all SC Members to schedule and/or declare the date and time of the emergency meeting prior to the meeting.

A quorum of the SC, defined as more than 50% of the SC Members, is required in order to take action on matters before the InCommon SC. Any authority to take action ascribed to the SC in these Bylaws may be taken by a quorum of the SC unless explicitly stated otherwise. If a quorum is not present at the time designated for a meeting, discussion may still take place but no minutes of that meeting need be made available to parties external to the SC. If the meeting thus abrogated was one of the required periodic meetings of the SC, the Chair shall schedule another SC meeting as soon as possible to satisfy the required meeting frequency.

A roll and minutes of each SC meeting shall be kept and delivered to each SC Member and The Member within fifteen (15) calendar days following the meeting. If a quorum was present, a redacted, as necessary, copy of the minutes shall be made available to InCommon Federation Participants within thirty (30) days of the SC meeting.

d. Voting

A vote may be called by the Chair on any issue brought before the Steering Committee whenever a quorum is present. Unless defined elsewhere in these Bylaws, issues of InCommon LLC business, such as financial or personnel matters, shall require a simple majority of the quorum for approval. Approval of the nomination of new SC Members, new qualification rules for InCommon Federation Participants, or a recommended Participant dispute resolution per Section 5 of these Bylaws shall require affirmative vote by two-thirds of the quorum.

Any action to be taken by the Steering Committee or a subcommittee thereof may be taken without a meeting if all Members of the Steering Committee or subcommittee, as the case may be, consent thereto to the Chair (or Vice-Chair) by telephone, Facsimile, or digitally signed electronic mail.

SC Members must vote individually. Voting by proxy is not allowed. If an SC Member cannot attend a meeting at which a vote is anticipated, that Member may deliver his or her vote to the Chair in writing prior to the meeting.

e. Miscellaneous

Except where specified otherwise in these Bylaws, electronic copies of documents in a form interpretable by the recipient shall be considered equivalent to paper copies.

Each SC Member shall be provided with a copy of and will be assumed to be familiar with the InCommon LLC Agreement.

Each SC Member shall sign a statement of compliance with the InCommon LLC Conflict of Interest Policy annually (Agreement: Exhibit B, §VI)

The fiscal year of InCommon shall be the calendar year unless defined otherwise by The Member (§7.05)

InCommon shall maintain liability insurance for Members of the Steering Committee. (§6.03(d))

Other parties may be invited to participate in discussions and meetings of the SC or any SC subcommittee or advisory committee at the discretion of the Chair of the relevant body. The presence of such parties shall be noted in any minutes kept of the meeting. Such parties shall not be eligible to vote or move any action by the relevant body.

3. COMMITTEES

a. Subcommittees of the Steering Committee

The Steering Committee may designate one or more subcommittees that, to the extent provided by the Steering Committee, shall have and may exercise all the power and authority of the Steering Committee. Such subcommittees shall consist of only SC members and shall include the Internet2 SC Member plus at least two other SC Members.

No action may be taken at a meeting of any subcommittee unless a quorum consisting of more than 50% of the subcommittee Members is present. All actions of a subcommittee shall require an affirmative vote by a majority of the total number of subcommittee members.

All actions taken by a subcommittee must be documented in writing and that document delivered to the Secretary of the SC. The Secretary shall include a notice of any such actions in the minutes of the next SC meeting.

b. Advisory Committees

The Steering Committee may establish one or more advisory committees, each of which shall include at least one Steering Committee Member. Advisory Committees are composed of individuals nominated by SC Members and affirmed by a majority vote of the SC. Nominees may be from among SC Members, representatives of InCommon Participants, or other individuals deemed to bring value to the work of the committee.

Advisory Committees are intended to help the Steering Committee develop policy, standards, documentation and best practices, and to represent the interests of Participants who are not otherwise represented on the Steering Committee. Advisory Committees do not exercise any authority of the Steering Committee.

Any action taken or recommendation made at a meeting of any advisory committee shall require the presence of a quorum consisting of more than 50% of the members of the Committee. All actions of an advisory committee shall require the affirmative vote of a majority of a quorum of the advisory committee members.

4. OPERATIONS

The day to day operations of the InCommon LLC and InCommon Federation are handled by an Operations Unit under the direction of an Operations Manager (“OM”).

a. Operations Manager

Subject to the supervision and authority of the Steering Committee, the Operations Manager :

- (i) shall have responsibility and authority for management of the day-to-day operations of the InCommon LLC, and
- (ii) may execute agreements and contracts on behalf of the InCommon LLC.

The OM shall keep, or cause to be kept, accurate, full and complete books and accounts showing assets, liabilities, income, operations, transactions and the financial condition of the Company. Such books and accounts shall be prepared on the accrual basis of accounting. Any SC Member or his or her designee shall have access thereto at any reasonable time during regular business hours and shall have the right to copy said records at its expense.

b. Delegation of Authority

The Steering Committee may delegate to the OM the authority to develop business plans and projections, prepare annual budgets and financial statements, acquire and manage assets, execute contracts, manage staff resources as needed to ensure the reliable operation of the Federation services, and to assume any other duties necessary for the conduct of InCommon LLC business as determined by the Steering Committee.

The Steering Committee may not delegate its authority to:

- define who may be a Participant in the Federation;
- resolve Participant disputes involving the Federation;
- take actions that might affect the financial stability of the InCommon LLC; or
- establish policies, rules and obligations governing the Federation.

5. DISPUTE RESOLUTION

The Steering Committee shall establish and document in the InCommon FOPP a Dispute Resolution Process to address disputes between or among Federation Participants and between any Participant and InCommon arising out of or pertaining to their participation in the Federation. The Steering Committee shall resolve the dispute in the best interests of InCommon. All decisions by the Steering Committee concerning disputes involving the Federation shall be final.

6. AMENDMENTS OR CHANGES TO THE INCOMMON LLC AGREEMENT

Amendments or changes to the InCommon LLC Agreement may be proposed by any SC Member. Proposed amendments or changes shall be considered by the Steering Committee if seconded by two (2) other SC Members. Proposed amendments or changes that receive an

affirmative vote of 75% of the SC Members shall be forwarded by the Secretary to The Member for consideration.

7. AMENDMENTS OR CHANGES TO THESE BYLAWS

Amendments or changes to these Bylaws may be proposed by any SC Member. Proposed amendments or changes shall be considered by the Steering Committee if seconded by one other SC Member. Amendments or changes that receive an affirmative vote of 75% of the SC Members shall become part of these Bylaws. Changes made to these Bylaws shall be made available to Participants within thirty (30) days of approval by the SC.

BY MY SIGNATURE BELOW I CONFIRM THAT THESE BYLAWS FOR THE
INCOMMON LLC ARE ADOPTED BY NO LESS THAN 75% AFFIRMATIVE
VOTE OF THE INCOMMON LLC STEERING COMMITTEE MEMBERS, EFFECTIVE THIS
DAY _____

Name, Chair of the InCommon LLC Steering Committee

Signature, Chair of the InCommon LLC Steering Committee

**LIMITED LIABILITY COMPANY AGREEMENT
OF
INCOMMON LLC**

**ARTICLE 1
THE COMPANY**

1.1 Definitions.

The following terms shall have the meanings set forth herein (such definitions to be equally applicable to both the singular and plural forms of the terms defined):

Act: The Delaware Limited Liability Company Act, as amended from time to time.

Agreement: This Limited Liability Company Agreement, as it may be further amended or supplemented from time to time.

Annual Meeting: As defined in Section 6.01.

Steering Committee: As defined in Section 6.01.

Capital Contribution: Any property (including cash) contributed to the Company by or on behalf of a Member.

Certificate: The Certificate of Formation, and any and all amendments thereto, filed on behalf of the Company with the Recording Office as required under the Act.

Code: The Internal Revenue Code of 1986, as in effect and hereafter amended, and, unless the context otherwise requires, applicable regulations thereunder. Any reference herein to a specific section or sections of the Code shall be deemed to include a reference to any corresponding provision of future law.

Company: InCommon , LLC.

Company Assets: All assets and property, whether tangible or intangible and whether real, personal, or mixed, at any time owned by or held for the benefit of the Company.

Fiscal Year: As defined in Section 7.05.

Member: University Corporation for Advanced Internet Development, Inc. d/b/a Internet2 ("Internet2").

Membership Interest: As defined in Section 4.01.

Person: Any individual, corporation, association, partnership, limited liability company, joint venture, trust, estate, or other entity or organization.

Recording Office: The office of the Secretary of State of the State of Delaware.

Related Party: With regard to a Member, officer, or other Person in question, any Person directly or indirectly controlling, controlled by, or under common control with the Person in question; if the Person in question is a corporation, any executive officer or director of the Person in question or of any corporation directly or indirectly controlling the Person in question. As used in this definition of “Related Party”, the term “control” means the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of a Person, whether through the ownership of voting securities, by contract, or otherwise.

SC Member: Any member of the Steering Committee.

1.2 Title to Property.

All property owned by the Company shall be owned by the Company as an entity and no Member shall have any ownership interest in such property in its individual name, and each Member’s interest in the Company shall be personal property for all purposes. At all times after the Effective Date, the Company shall hold title to all of its property in the name of the Company and not in the name of any Member.

1.3 Payments of Individual Obligations.

The Company’s credit and assets shall be used solely for the benefit of the Company, and no asset of the Company shall be transferred or encumbered for, or in payment of, any individual obligation, of any Member or any other Person.

ARTICLE 2 GENERAL PROVISIONS

2.1 Ratification of Prior Acts

The Member of the Company hereby ratifies and approves all actions taken by the Company, its sole incorporator, and any officer prior to this Agreement.

2.2 Name of Company

The name under which the Company shall conduct its business is “InCommon, LLC”. The business of the Company may be conducted under any other name permitted by the Act that is selected by the Steering Committee, in its sole and absolute discretion. The Steering Committee promptly shall execute, file, and record any assumed or fictitious name certificates required by the laws of the State of Delaware or any state in which the Company conducts business.

2.3 Term

The term of the Company commenced on the date upon which the Certificate was duly filed with the Recording Office and shall continue until dissolved and liquidated. The existence of the Company as a separate legal entity shall continue until the Certificate's cancellation.

2.4 Place of Business

The location of the principal place of business of the Company shall be as determined by the Steering Committee. The Steering Committee may change the principal place of business of the Company to such other place or places within the United States as the Steering Committee may from time to time determine, in its sole and absolute discretion, provided that the Steering Committee shall give written notice of the change to the Member within thirty (30) days after the effective date of the change and, if necessary, the Steering Committee shall amend the Certificate in accordance with the applicable requirements of the Act. The Steering Committee may, in its sole and absolute discretion, establish and maintain such other offices and additional places of business of the Company, either within or without the State of Delaware, as it deems appropriate.

2.5 Registered Office and Registered Agent

The location of the registered office and the name of the registered agent of the Company in the State of Delaware shall be as stated in the Certificate, as determined from time to time by the Steering Committee .

ARTICLE 3 PURPOSES AND POWERS

3.1 Purposes

The purposes of the Company shall include:

- (a) to facilitate collaboration through the sharing of protected network-accessible resources by means of an agreed upon trust fabric;
- (b) to acquire, hold, own, operate, manage, finance, encumber, sell, or otherwise dispose of, assign, or otherwise use the Company Assets; and
- (c) to enter into any lawful transaction and engage in any lawful activities in furtherance of the foregoing purposes and as may be necessary, incidental or convenient to carry out the business of the Company as contemplated by this Agreement.

3.2 Powers

The Company shall have the power to do any and all acts and things necessary, appropriate, advisable, or convenient for the furtherance and accomplishment of the purposes of the Company, including, without limitation, to engage in any kind of activity and to enter into and perform obligations of any kind necessary to or in connection with, or

incidental to, the accomplishment of the purposes of the Company, so long as said activities and obligations may be lawfully engaged in or performed by a limited liability company under the Act.

3.3 Tax Classification

The Company shall be operated in a manner consistent with its classification as a disregarded entity for federal and state tax purposes.

ARTICLE 4 MEMBERS

4.1 Membership Interests

Equity interests in the Company shall consist of the Membership Interests, which shall all be owned by Internet2.

4.2 Issuance of Membership Interests

No new Membership Interest shall be issued.

ARTICLE 5 CAPITAL

5.1 Liability of the Member and the Steering Committee

Except as otherwise provided in the Act, the debts, obligations and liabilities of the Company, whether arising in contract, tort or otherwise, shall be solely the debts, obligations and liabilities of the Company, and neither the Member nor the SC Members shall be obligated personally for any such debt, obligation or liability of the Company solely by reason of being a Member or a SC Member. The failure of the Company to observe any formalities or requirements relating to the exercise of its powers or management of its business or affairs under the Act or this Agreement shall not be grounds for imposing personal liability on the Member or the SC Members for liabilities of the Company.

ARTICLE 6 GOVERNANCE

6.1 Management of the Company by the Steering Committee

(a) Management by the Steering Committee. Except as otherwise provided for herein, the Member hereby unanimously agrees that the responsibility for management of the business and affairs of the Company shall be delegated to a group of individuals designated as the Steering Committee pursuant to Section 18-402 of the Act (the

“Steering Committee”). The initial members of the Steering Committee shall be comprised of the individuals listed on Exhibit A hereto.

(b) Composition of Steering Committee; Appointment and Removal

- (i) The Steering Committee shall at all times be composed of at least seven (7) and not more than thirteen (13) individuals (each individual referred to as a “SC Member”). At least one SC Member shall always be an employee, officer, or director of Internet2 (referred to as the “Internet2 Member”). The Steering Committee shall appoint a secretary of the Company (the “Secretary”). The Secretary, at the direction of the Steering Committee, shall prepare and distribute to each SC Member an agenda in advance of each meeting and shall prepare and distribute promptly to each SC Member written minutes of all meetings of the Steering Committee. The Secretary shall also be responsible for preparing and distributing to the SC Members any notices received by the Company or otherwise called for by this Agreement to be given by the Company. The Steering Committee may appoint officers of the Steering Committee (including, but not limited to, a chair, one or more vice chairs, a treasurer and an assistant secretary) upon terms and conditions the Steering Committee deems necessary and appropriate.

Terms of Office. Any officer shall hold his or her respective office unless and until such officer is removed by the Steering Committee.

- (ii) SC Members shall be divided into three classes, Class A, Class B, and Class C, as equal in number as possible. Each year, the terms of one of these groups of SC Members shall expire, such that the SC Members serve staggered terms and one-third of the SC Members' positions are subject to reelection. SC Members shall be elected for a three-year term, with the exception of the initial SC Members designated as Class A and Class B on Exhibit A, who shall serve for one-year and two-year terms, respectively. SC Members shall serve no more than two full consecutive three-year terms. When an SC Member is named to the Steering Committee to fill the unexpired term of a predecessor, the SC Member may serve out the unexpired term plus two full terms.
- (iii) Each such SC Member shall serve until the expiration of his or her term or, if earlier, at such time as he or she resigns, retires, dies or is removed. Any SC Member may be removed with or without cause only by the Member. Upon the expiration of the SC Member's term or upon the resignation, retirement, death or removal of any SC Member, the Steering Committee shall nominate at least two replacement SC Members to fill each vacancy. The Member shall select from the nominees recommended by the Steering Committee an individual to serve as an SC Member. The Internet2 Member shall be nominated and selected by the Member.

(c) Meetings and Actions

- (i) The Steering Committee shall meet (A) at least once each Fiscal Year (such annual meeting, the “Annual Meeting”); (B) at such other times as may be determined by the Steering Committee or the Member; or (C) upon the request of at least two SC Members or the Operations Manager upon ten (10) days’ notice to all SC Members. Meetings may be held by telephone.
 - (ii) The Steering Committee shall cause written minutes to be prepared of all actions taken by the Steering Committee and shall cause a copy thereof to be delivered to each SC Member and the Member within fifteen (15) days thereof.
 - (iii) No action may be taken at a meeting of the Steering Committee unless a quorum consisting of at least a majority of SC Members is present.
 - (iv) Each SC Member shall be entitled to cast one vote with respect to any decision made by the Steering Committee. Except as otherwise provided herein, any action to be taken by the Steering Committee shall require the vote of at least a majority of the Steering Committee at a meeting at which a quorum is present. Except as otherwise provided herein, approval or action by the Steering Committee shall constitute approval or action by the Company and shall be binding on the Member. Any action to be taken by the Steering Committee or a committee thereof may be taken without a meeting if all members of the Steering Committee or committee, as the case may be, consent thereto in writing.
- (d) Committees. The Steering Committee may designate a subcommittee consisting of at least three SC Members, one individual who shall be the Internet2 Member. Any subcommittee, to the extent provided by the Steering Committee, shall have and may exercise all the power and authority of the Steering Committee. No action may be taken at a meeting of any subcommittee unless a quorum consisting of at least two SC Members is present. All actions of a subcommittee shall require the majority vote of the subcommittee members.
- (e) Advisory Committees. Other committees not having and exercising the authority of the Steering Committee may be constituted and members thereof appointed by a resolution adopted by a majority of the Steering Committee present at a meeting of the Steering Committee at which a quorum is present. No action may be taken at a meeting of any advisory committee unless a quorum consisting of at least a majority of the members is present. All actions of an advisory committee shall require the majority vote of the advisory committee members.
- (f) Telephone Meeting. Members of the Steering Committee or any committee thereof may participate in any meeting by means of conference telephones or similar communications if all members participating in such meeting can hear one another for the entire discussion of the matter(s) to be voted upon.
- (g) Power and Authority of the Steering Committee. Except as otherwise provided for herein, the Steering Committee (acting on behalf of the Company), by its own action, or by action of a subcommittee of the Steering Committee, but not by delegation to

officers or other employees of the Company, shall have the right, power and authority to manage the operations of the Company.

- (h) Third Party Reliance. Third parties dealing with the Company shall be entitled to rely conclusively upon the power and authority of the Steering Committee and the officers of the Company as set forth herein.
- (i) Fiduciary Relationship. No SC Member shall be liable to the Company or its Member for monetary damages for breach of fiduciary duty as an SC Member or otherwise liable, responsible or accountable to the Company or its Member for monetary damages or otherwise for any acts performed, or for any failure to act; *provided, however*, that this provision shall not eliminate or limit the liability of an SC Member
 - (i) for any breach of the SC Member's duty of loyalty to the Company or its Member,
 - (ii) for acts or omissions which involve intentional misconduct or a knowing violation of law, or
 - (iii) for any transaction from which the SC Member received any improper personal benefit.
- (j) Reimbursement. All expenses incurred with respect to the organization, operation, and management of the Company shall be borne by the Company. No salary or fees for services shall be paid to the SC Members for their services as such; *provided, however*, that the Steering Committee may allow a reasonable fixed sum and expenses to be paid for attendance at regular and special meetings of the Steering Committee or committee thereof. The SC Members shall be entitled to reimbursement from the Company for direct expenses allocable to the organization, operation, and management of the Company. Nothing contained herein shall prevent an SC Member from serving the Company in any other capacity and receiving compensation therefore.
- (k) No Individual Authority. Other than through actions taken by the Steering Committee, as set forth herein, no SC Member shall have the authority to bind the Company.
- (l) Member Consent Required for Certain Actions. Notwithstanding any contrary provision in this Agreement, the following decisions and actions shall not be made or taken without the consent of the Member:
 - (i) The sale or other disposition of substantially all of the Company's assets;
 - (ii) An amendment to this Agreement;
 - (iii) The admission of new Members;
 - (iv) The dissolution, merger or combination of the Company;
 - (v) Approving any contract, agreement, or commitment (with the exception of an employment contract) with a value in excess of \$50,000 or a term longer than six (6) months (or a group of related contracts, agreements and commitments with an aggregate value in excess of \$50,000);
 - (vi) Approving the choice of bank depositories and approving arrangements relating to signatories on bank accounts affirmative;

- (vii) Approving the conveyance, sale, transfer, assignment, pledge, encumbrance, or disposal of, or the granting of a security interest in, any assets of the Company the fair market value of which may reasonably be expected to exceed \$25,000;
- (viii) Approving the entry of the Company into any other partnership or joint venture;
- (ix) Incurring indebtedness or loaning any sum or extending credit to any Person in an amount in excess of \$25,000, or for a period in excess of six (6) months;
- (x) Guaranteeing any indebtedness of any other Person in any amount in excess of \$25,000 or for a period in excess of six (6) months, or guaranteeing any contractual obligations of any other Person with a value in excess of \$25,000 or for a period in excess of six (6) months;
- (xi) Conducting litigation to which the Company is a party; or
- (xii) Approving the acquisition approval of any business or a business division from any Person, whether by asset purchase, stock purchase, merger, or other business combination.

6.2 Officers

Operations Manager. The Steering Committee shall appoint an Operations Manager of the Company (the “Operations Manager”) and the appointment shall be approved by the Member. Subject to the supervision and authority of the Steering Committee, the Operations Manager (i) shall be the chief executive officer of the Company, (ii) shall have responsibility and authority for management of the day-to-day operations of the Company, and (iii) may execute agreements and contracts on behalf of the Company. The Operations Manager shall be an employee of Internet2.

6.3 Indemnification of the Member, SC Members, Officers and any Related Party

- (a) Right of Indemnification. To the extent permitted by Section 18-108 of the Act, the Company shall indemnify and hold harmless any Member, SC Member, and officers (individually, in each case, an “Indemnitee”) to the fullest extent permitted by law from and against any and all losses, claims, demands, costs, damages, liabilities joint or several), expenses of any nature (including attorneys’ fees and disbursements), judgments, fines, settlements and other amounts arising from any and all claims, demands, actions, suits or proceedings, whether civil, criminal, administrative or investigative, in which the Indemnitee may be involved or threatened to be involved, as a party or otherwise, arising out of or incidental to the business or activities of or relating to the Company, regardless of whether the Indemnitee continues to be a Member, an SC Member, or an officer thereof at the time any such liability or expense is paid or incurred; provided, however, that this provision shall not eliminate or limit the liability of an Indemnitee (i) for any breach of the Indemnitee’s duty of loyalty to the Company or its Member, (ii) for acts or omissions which involve intentional misconduct or a knowing violation of law, or (iii) for any transaction from which the Indemnitee received any improper personal benefit.

- (b) Advances of Expenses. Expenses incurred by an Indemnitee in defending any claim, demand, action, suit, or proceeding subject to this Section 6.03 may, from time to time, upon request by the Indemnitee, be advanced by the Company prior to the final disposition of such claim, demand, action, suit or proceeding upon receipt by the Company of an undertaking by or on behalf of the Indemnitee to repay such amount if it shall be determined in a judicial proceeding or a binding arbitration that such Indemnitee is not entitled to be indemnified as authorized in this Section 6.03.
- (c) Other Rights. The indemnification provided by this Section 6.03 shall be in addition to any other rights to which an Indemnitee may be entitled under any agreement, vote of the Steering Committee as a matter of law or equity, or otherwise, both as to an action in the Indemnitee's capacity as a Member, an SC Member, an officer or any Related Party thereof, and as to an action in another capacity, and shall continue as to an Indemnitee who has ceased to serve in such capacity and shall inure to the benefit of the heirs, successors, assigns, and administrators of the Indemnitee.
- (d) Insurance. The Company may purchase and maintain insurance on behalf of the Steering Committee and such other Persons as the Steering Committee shall determine against any liability that may be asserted against or expense that may be incurred by such Persons in connection with the offering of interests in the Company or the business or activities of the Company, regardless of whether the Company would have the power to indemnify such Persons against such liability under the provisions of this Agreement.
- (e) Effect of Interest in Transaction. An Indemnitee shall not be denied indemnification in whole or in part under this Section 6.03 or otherwise by reason of the fact that the Indemnitee had an interest in the transaction with respect to which the indemnification applies if the transaction was otherwise permitted or not expressly prohibited by the terms of this Agreement.
- (f) No Third Party Rights. The provisions of this Section 6.03 are for the benefit of the Indemnitees, their heirs, successors, assigns and administrators and shall not be deemed to create any rights for the benefit of any other Persons.

6.4 Conflicts of Interest

The Company shall implement the Conflict of Interest Policy set forth in Exhibit B hereto, which may be amended solely by the Member.

ARTICLE 7 ACCOUNTING

7.1 Bank Accounts

All funds of the Company shall be deposited in Member's name in such checking and savings accounts, time deposits, certificates of deposit or other accounts at such banks as

shall be designated by the Member from time to time, and the Member shall arrange for the appropriate conduct of such account or accounts.

7.2 Books and Records

- (a) The Operations Manager shall keep, or cause to be kept, accurate, full and complete books and accounts showing assets, liabilities, income, operations, transactions and the financial condition of the Company. Such books and accounts shall be prepared on the accrual basis of accounting. Any Member or its designee shall have access thereto at any reasonable time during regular business hours and shall have the right to copy said records at its expense..

7.3 Accounting Decisions

All decisions as to accounting matters, except as specifically provided to the contrary herein, shall be made by the Steering Committee.

7.4 Where Maintained

The books, accounts and records of the Company at all times shall be maintained at the Company's principal office.

7.5 Fiscal Year

The fiscal year of the Company for financial, accounting, Federal, state and local income tax purposes shall be the same fiscal year as its Member.

ARTICLE 8

DISSOLUTION AND LIQUIDATION

8.1 Events Causing Dissolution

- (a) The Company shall be dissolved and its affairs wound up upon the consent in writing to dissolve and wind up the affairs of the Company by its sole Member.

8.2 Cancellation of Certificate

Upon the dissolution of the Company, the Certificate shall be canceled in accordance with the provisions of Section 18-203 of the Act, and the Member (or any other person or entity responsible for winding up the affairs of the Company) shall promptly notify the Steering Committee of such dissolution.

8.3 Distributions Upon Dissolution

- (a) Upon the dissolution of the Company, the Steering Committee (or any other person or entity responsible for winding up the affairs of the Company) shall proceed without any unnecessary delay to sell or otherwise liquidate the Company Assets and pay or make due provision for the payment of all debts, liabilities and obligations of the Company.

(b) The Steering Committee (or any other person or entity responsible for winding up the affairs of the Company) shall distribute the net liquidation proceeds and any other liquid assets of the Company after the payment of all debts, liabilities and obligations of the Company (including, without limitation, all amounts owing to a Member under this Agreement or under any agreement between the Company and a Member entered into by the Member other than in its capacity as a Member in the Company), the payment of expenses of liquidation of the Company, and the establishment of a reasonable reserve in an amount estimated by the Steering Committee to be sufficient to pay any amounts reasonably anticipated to be required to be paid by the Company, to its Member.

8.4 Reasonable Time for Winding Up

A reasonable time shall be allowed for the orderly winding up of the business and affairs of the Company and the liquidation of its assets pursuant to Section 8.03 in order to minimize any losses otherwise attendant upon such a winding up.

ARTICLE 9 AMENDMENTS

9.01 This Agreement may only be amended by the consent of the Member.

ARTICLE 10 PARTICIPANTS

10.01 The Company may permit Persons, who shall be designated as "Participants" or such other name as the Steering Committee may permit to become affiliated with the Company in order to help facilitate and advance the Company's purposes. Such Participants may be designated into one or more classes with such rights and obligations, as provided for by agreement between the Company and such Participant(s). In no event shall such Participant(s) be (i) entitled to vote on any manner involving the affairs of the Company, (ii) entitled to any rights or privileges afforded to the Member, (iii) entitled to any rights or privileges not specifically provided for in the agreement between the Company and the Participant(s), or (iv) entitled to any interest in the Company or its assets.

The foregoing Agreement was adopted by the Company's sole Member, Internet2, on December 10, 2004.

By: _____

Douglas E. Van Houweling, CEO

University Corporation for Advanced Internet Development, Inc.

EXHIBIT A

INCOMMON LLC

Steering Committee

Name	Class	Term Expires
Jerry Campbell, USC	A	12/31/2005
Lev Gonick, CWRU	A	12/31/2005
Susan Perry, Mt Holyoke, Mellon	A	12/31/2005
Clair Goldsmith, UT System	B	12/31/2006
Carrie Regenstein, U Wisconsin-Madison	B	12/31/2006
Mike Teets, OCLC	B	12/31/2006
Mark Luker, EDUCAUSE	C	12/31/2007
Tracy Mitrano, Cornell	C	12/31/2007
David Yakimischak, JSTOR	C	12/31/2007
Ken Klingenstein, Internet2	Internet2 Member	

EXHIBIT B

INCOMMON FEDERATION, LLC

CONFLICT OF INTEREST POLICY

ARTICLE I

PURPOSE

The purpose of the conflict of interest policy is to protect the interest of InCommon, LLC (the “Company”) when it is contemplating entering into a transaction or arrangement that might benefit the private interest of a member of the Steering Committee (each such member, an “SC Member,” and such Committee, the “Steering Committee”), a member of a subcommittee of the Steering Committee (a “subcommittee”), an officer of the Steering Committee, or an employee of the Company (each such member, officer, or employee, a “Company Individual”). This policy is intended to supplement but not replace any applicable federal or state laws governing conflicts of interest applicable to the Company.

ARTICLE II

DEFINITIONS

1. Interested Person

Any Company Individual who has a direct or indirect financial interest, as defined below, is an “Interested Person.”

2. Financial Interest

A Company Individual has a financial interest if he or she has, directly or indirectly, through business, investment or family --

- a. an ownership or investment interest in any entity with which the Company has a transaction or arrangement, or
- b. a compensation arrangement with any entity, except Internet2, or individual with which the Company has a transaction or arrangement, or
- c. a potential ownership or investment interest in, or compensation arrangement with, any entity, except Internet2, or individual with which the Company is negotiating a transaction or arrangement.

Compensation includes direct and indirect remuneration as well as gifts or favors that are substantial in nature.

A financial interest is not necessarily a conflict of interest. Under Article III, Section 2, a person who has a financial interest may have a conflict of interest only if the Steering Committee or appropriate subcommittee decides that a conflict of interest exists.

ARTICLE III PROCEDURES

1. Duty to Disclose

In connection with any actual or possible conflict of interest, an Interested Person must disclose the existence of his or her financial interest and all material facts to the Steering Committee and/or subcommittee considering the proposed transaction or arrangement.

2. Determining Whether a Conflict of Interest Exists

After disclosure of the financial interest and all material facts, and after any discussion with the Interested Person, he or she shall leave the Steering Committee or subcommittee meeting while the determination of a conflict of interest is discussed and voted upon. The remaining Steering Committee or subcommittee members shall decide if a conflict of interest exists.

3. Procedures for Addressing the Conflict of Interest

- a. An Interested Person may make a presentation at the Steering Committee or subcommittee meeting, but after such presentation, he/she shall leave the meeting during the discussion of, and the vote on, the transaction or arrangement that results in the conflict of interest.
- b. The Steering Committee or subcommittee, as the case may be, shall, if appropriate, appoint a disinterested SC Member, officer, or subcommittee to investigate alternatives to the proposed transaction or arrangement.
- c. After exercising due diligence, the Steering Committee or subcommittee shall determine whether the Company can obtain a more advantageous transaction or arrangement with reasonable efforts from a person or entity that would not give rise to a conflict of interest.
- d. If a more advantageous transaction or arrangement is not reasonably attainable under circumstances that would not give rise to a conflict of interest, the Steering Committee or subcommittee shall determine by a majority vote of its disinterested members whether the transaction or arrangement is in the Company's best interest and for its own benefit and whether the transaction is fair and reasonable to the Company and shall make its decision as to whether to enter into the transaction or arrangement in conformity with such determination.

4. Violations of the Conflict of Interest Policy

- a. If the Steering Committee or subcommittee has reasonable cause to believe that a Company Individual has failed to disclose an actual or possible conflict of interest, it shall inform such person of the basis for such belief and afford him or her an opportunity to explain the alleged failure to disclose.
- b. If, after hearing the response of the Company Individual and making such further investigation as may be warranted in the circumstances, the Steering Committee or subcommittee thereof determines that the Company Individual has in fact failed to disclose an actual or possible conflict of interest, it shall take appropriate disciplinary and corrective action.

ARTICLE IV RECORDS OF PROCEEDINGS

The minutes of the Steering Committee and all subcommittees with Steering Committee-delegated powers shall contain --

1. the names of the persons who disclosed or otherwise were found to have a financial interest in connection with an actual or possible conflict of interest, the nature of the financial interest, any action taken to determine whether a conflict of interest was present, and the Steering Committee's or subcommittee's decision as to whether a conflict of interest in fact existed.
2. the names of the persons who were present for discussions and votes relating to the transaction or arrangement, the content of the discussion, including any alternatives to the proposed transaction or arrangement, and a record of any votes taken in connection therewith.

ARTICLE V COMPENSATION COMMITTEES

A voting member of any subcommittee whose jurisdiction includes compensation matters and who receives compensation, directly or indirectly, from the Company for services is precluded from voting on matters pertaining to that member's compensation.

ARTICLE VI ANNUAL STATEMENTS

- Each Company Individual shall annually sign a statement which affirms that such person: -
- a. has received a copy of the conflict of interest policy,
 - b. has read and understands the policy, and
 - c. has agreed to comply with the policy.

**INCOMMON FEDERATION:
FEDERATION OPERATING POLICIES AND PRACTICES
2007 October 15**

Table of Contents

1 ROLE OF THE INCOMMON FEDERATION ORGANIZATION.....	2
2 ORGANIZATIONAL STRUCTURE	2
2.1 MANAGEMENT	2
2.2 COMMITTEES.....	2
2.3 MEETINGS	3
2.4 OFFICES AND RECORDS	3
2.5 PERSONNEL	3
3 POLICIES, REQUIREMENTS, AND STANDARDS.....	3
4 APPLICATION FOR PARTICIPATION IN INCOMMON.....	4
4.1 ELIGIBILITY CRITERIA.....	4
4.2 SUBMITTING AN APPLICATION	5
4.3 APPROVING AN APPLICANT.....	5
5 PARTICIPATION FEES	5
6 REGISTRATION: IDENTIFICATION AND AUTHENTICATION OF TRUSTED OFFICERS.....	5
7 REGISTRATION AND MANAGEMENT OF PARTICIPANT POLICIES, SYSTEMS, AND TECHNICAL COMPONENTS	5
7.1 TYPES OF REGISTERED SYSTEMS: IDENTITY PROVIDERS AND SERVICE PROVIDERS.....	5
7.2 RELATIONSHIP OF SYSTEMS TO PARTICIPANT	6
7.3 REQUIRED INFORMATION COMPONENTS	6
7.3.1 <i>Participant Operating Practices</i>	6
7.3.2 <i>Metadata</i>	6
7.3.3 <i>Digital Certificates for Federation Participant service platforms</i>	7
7.3.3.1 <i>Signing</i>	7
7.3.3.2 <i>Expiration</i>	7
7.3.3.3 <i>Revocation</i>	7
8 DISPUTE RESOLUTION PROCEDURE	7
8.1 DISPUTES AMONG PARTICIPANTS	7
8.2 DISPUTES BETWEEN PARTICIPANT(S) AND THE FEDERATION.....	7
9 OPERATIONS	8
9.1 OPERATIONAL ASSURANCE LEVEL	8
9.2 COMMUNICATIONS AND SUPPORT	8
9.3 FEDERATION TECHNICAL INFRASTRUCTURE	9
9.3.1 <i>Where Are You From (WAYF)</i>	9
9.3.2 <i>Metadata Distribution</i>	9
9.3.3 <i>Participant Administrative Interface</i>	9
9.3.4 <i>Certification Authority (CA)</i>	9
9.3.5 <i>Suspension of Federation Services</i>	9
9.4 DISASTER RECOVERY.....	10
10 PARTICIPATION STATUS: RENEWAL, WITHDRAWAL AND TERMINATION, AND SUSPENSION.....	10
10.1 RENEWAL.....	10
10.2 WITHDRAWAL AND TERMINATION	10
10.3 SUSPENSION OF PARTICIPANTS' SERVICES.....	10
11 FURTHER RISK ASSESSMENT	10

This document describes at a high level how the InCommon support organization is structured and how it operates in accordance with the Limited Liability Company Agreement of InCommon ("Company Agreement") and Bylaws of the InCommon LLC ("Bylaws") to support the entire InCommon Federation ("Federation"). Specific details and logistics are left to the discretion of the InCommon Operations Manager ("OM").

InCommon Federation Participants ("Participants") should review this document to help assess what potential risks, if any, might be incurred by their participation in the Federation. By reviewing the policies and practices of the Federation, Participants and potential participants can evaluate the level of assurance of the Federation's services to ensure trustworthy operations and determine whether they meet a Participant's minimum requirements. Complete evaluation of the entire Federation's infrastructure and level of assurance is out of scope for this document and would need to include evaluation of all relevant Participants' policies and practices. Please contact the InCommon office for clarification or additional information regarding this document or other Federation matters.

1 Role of the InCommon Federation Organization

The InCommon, LLC Bylaws define the mission of InCommon and its Federation and the principles and governance structure under which the Federation operates. This Federation Operating Policies and Practices document (FOPP) outlines the activities undertaken by InCommon on behalf of its Federation Participants.

The administrative and operational functions of InCommon are carried out under direction of the OM in accordance with the Company Agreement. These responsibilities include development of the Federation participant community, processing applications, identifying and authenticating eligible organizations and their trusted officers, processing participant metadata, overseeing the operation of InCommon service platforms, dispute resolution, termination processes, accounting and billing, and other duties as assigned by the InCommon Steering Committee or the officers of the InCommon LLC.

2 Organizational Structure

2.1 Management

Responsibility for management of the business and affairs of the InCommon LLC is vested with the InCommon Steering Committee ("Steering Committee") as described in the Company Agreement. Specific authority may be delegated by the Steering Committee to appointed subcommittees of the Steering Committee or the OM.

The Steering Committee approves this FOPP as an accurate reflection of InCommon Federation operations. Any change to this FOPP will be communicated to each Participant Administrator via email within 15 business days of the change being approved by the Steering Committee.

2.2 Committees

The Steering Committee may designate subordinate or advisory committees to make decisions, develop position papers, and/or provide advice on particular matters of importance to the Federation as outlined in the Bylaws. At least one member of the

Steering Committee will participate in each Advisory Committee to ensure good communication between the committee and the Steering Committee. Additional membership in such committees will be defined by the Steering Committee and typically will be drawn from the Participant community. Other individuals may be asked to participate based on their particular knowledge of the subject matter. Other committees may be formed as detailed in the Bylaws. Current committees are listed on the InCommon website.

2.3 Meetings

The Steering Committee meets no less frequently than once per year, typically by conference call. Minutes are kept of the Steering Committee meetings and, except for confidential personnel or financial matters, are available to Federation Participants upon request.

Advisory and other committees meet as needed, typically by conference call. Minutes need not be kept.

2.4 Offices and Records

The InCommon Federation office's contact information is:

InCommon
c/o Internet2
1000 Oakbrook Dr, Suite 300
Ann Arbor, MI 48104
Email address: incommon-admin@incommonfederation.org
Telephone: 734-913-4250
Website: <http://www.incommonfederation.org>

All records of InCommon are managed by this office.

2.5 Personnel

The InCommon LLC minimally requires at least two officers: the Operations Manager and the Secretary. Other officers may be appointed by the Steering Committee. The OM will provide guidelines and direction for the operational aspects of the Federation's support organization. Operational functions are staffed and performed by Internet2.

Internet2 hires and manages personnel who provide legal, administrative, communications, operational, and other support to the OM.

3 Policies, Requirements, and Standards

The Steering Committee approves all policies, requirements, and standards that apply to the InCommon support organization and its Federation Participants. Current governing documents, available from the InCommon office above and on the website, include:

- Limited Liability Company Agreement of InCommon
- Bylaws of the InCommon LLC
- InCommon Federation: Federation Operating Policies and Practices (this document)

- InCommon Federation: Participation Agreement
- InCommon Federation: Common Identity Attributes
- InCommon Federation: Participant Operational Practices

Additional documents, guidelines, and other papers are also available on the InCommon website.

4 Application for Participation in InCommon

Organizations that wish to participate in the InCommon Federation must be eligible under the requirements defined below.

4.1 Eligibility Criteria

The InCommon Federation currently has two classes of participants: (1) Higher Education (accredited post-secondary institutions and their central offices) and (2) their Sponsored Partners.

To qualify in the first category, an organization must be:

- A two- or four-year degree-granting institution that is accredited by an agency on the U.S. Department of Education's list of recognized Regional Accrediting Agencies as listed on the InCommon website (URL found in section 2.4); or
- A state higher education system office or other central coordinating office which either governs or manages a collection of accredited, degree-granting institutions. The entity must be commissioned, established, or recognized by a local, state, or national government to perform this activity or must be a cooperative venture organized by and for the benefit of higher education institutions for the above purposes. Documentation substantiating these criteria may be required, and determinations will be made on a case by case basis.

A Sponsored Partner is any entity that is sponsored for participation in the Federation by a participating category 1 organization. A Sponsored Partner typically provides online resources, research data, informational, or other services to the sponsoring higher education organization. A sponsorship letter must be received by InCommon from the sponsoring category 1 Participant's designated Executive, either by email or postal mail. For details see the InCommon website.

The InCommon Steering committee may choose to set eligibility criteria for additional types of organizations or may vote on the approval of any applying organization under special circumstances (see 4.3).

Distributed university or corporate systems are expected to require independent universities or businesses to become separate Participants in the InCommon Federation. Examples of such distributed systems include state-wide university systems and large conglomerate corporations where each university or business unit is authorized to commit to and enter into legal agreements on behalf of its own organizational entity. Federations and other complex membership systems will be eligible for InCommon Federation participation on a case by case basis.

4.2 Submitting an Application

Interested organizations may apply for participation by submitting an online application or by submitting a signed Participation Agreement for review. InCommon may request additional information concerning the nature or qualifications of the applying organization.

4.3 Approving an Applicant

Any eligibility questions will be referred to the OM. The OM will determine if the application requires Steering Committee approval.

The Steering Committee may request that additional information be supplied by the applicant. If the Steering Committee deems the applicant eligible, the OM will continue with application processing. In the case that neither the OM nor the Steering Committee approves an applicant, InCommon will notify the applicant of this result in a timely manner.

The applicant will be accepted for participation when two original, signed copies of the Participation Agreement have been received by the InCommon office and have been countersigned by InCommon.

5 Participation Fees

InCommon fees are established by the Steering Committee on a cost-recovery basis and reviewed annually. The Registration fee covers the cost of determining the eligibility of the applicant and the identification and authentication of its trusted officers. Payment by credit card is due upon submission. Annual Participation fees are invoiced, based on a calendar year from January 1 to December 31, and are not prorated. No fees are refundable. The current fee schedule is available on the InCommon website.

6 Registration: Identification and Authentication of Trusted Officers

InCommon verifies the identity of all individuals who fill the Participant's trusted roles of Executive and Administrator (see the InCommon online Glossary for definitions). By constructing an independently verifiable, out-of-band communication path with these officers, the Registration Authority establishes a relatively strong level of assurance that the person is who he or she declares. Details on the registry process are available on the InCommon website.

7 Registration and Management of Participant Policies, Systems, and Technical Components

The Participant's trusted Administrator will be given credentials to manage Federation Participant data and requests in a secure manner.

7.1 Types of Registered Systems: Identity Providers and Service Providers

Within the Federation, both classes of participants may offer services as Identity Provider for its user community, Service Provider to a participant organization's user community, or both. For instance, a Higher Education Institution serving primarily as an Identity Provider might also make online information or services available to

other InCommon participants. Likewise, a Sponsored Partner that is primarily a provider of online services also might act as an Identity Provider.

Participants register identity management systems and/or service provider systems using the InCommon participant administrative interface. Higher Education Institutions and Sponsored Partners receive an initial quota for each system type and can purchase more as needed, subject to certain restrictions, as outlined in the Participation Agreement and Fee Schedule available on the InCommon website.

7.2 Relationship of Systems to Participant

Any identity management system or service provider system registered by a Participant must be under the management hierarchy of the Participant organization. The Participant is responsible for the actions of any system registered with the Federation. Participants may only register third party systems that operate services under contract to Participant and for which Participant will be responsible, in accordance with the provisions of the Participation Agreement. Such third party systems might, for example, include outsourced identity management services.

7.3 Required Information Components

7.3.1 Participant Operating Practices

A fundamental expectation of Federation Participants is that they provide authoritative and accurate attribute assertions to other participants and that participants receiving an attribute assertion protect it and respect any privacy constraints placed on it by the Federation or the source of that information.

To support this goal, each Participant must describe its relevant operations in a Participant Operating Practices (POP) statement and share this POP with Federation Participants. The template POP is available on the InCommon website. In some cases, multiple systems can be described in one POP. A current version of the POP must always be available to the Federation and Participant Administrators. InCommon does not review such Participant Operating Practices against any criteria of performance. The POP is a self-asserted declaration by each Participant of its current practices. More information about POP requirements is available on the InCommon website.

7.3.2 Metadata

A Participant Administrator registers its Identity Provider and Service Provider systems through the participant administrative interface by describing components of its systems. The data are collected and digitally signed by InCommon. Secure, up-to-date, trusted information about all Participants and their systems is a core service of the Federation. InCommon will make reasonable efforts to verify submitted data, and will act in accordance with the practices outlined in the InCommon Operations reference, available on the InCommon website.

Metadata may be removed or modified by Participant Administrators through the participant administrative interface. Changes to metadata are updated within one Internet2 business day following the submission. Under special circumstances, Participant Executives or Administrators may make removal requests via e-mail or telephone as listed on the InCommon website. InCommon will verify these requests using trusted communication channels before processing any removal requests.

Transmission of Federation metadata to Participants is not initiated by InCommon. Instead, Participants are expected to retrieve Federation metadata on a regular basis.

7.3.3 Digital Certificates for Federation Participant service platforms

7.3.3.1 Signing

Certificate Signing Requests are submitted via the participant administrative interface. Certificates are signed in accordance with the InCommon Federation Certification Authority Server Certificate Profile found in the InCommon Certificate Practices Statement.

7.3.3.2 Expiration

Certificates normally are valid for one (1) year. The Participant will be notified by InCommon prior to the expiration of its certificates. The Participant is responsible for submitting certificate requests to update the validity of its certificates.

7.3.3.3 Revocation

The InCommon CA revokes certificates upon request by Participant Executives or Administrators. Certificates are revoked and a new CRL is issued within one Internet2 business day of the verification of the request. Details on the Certificate revocation policy and practices are available on the website.

8 Dispute Resolution procedure

Should disputes regarding Federation services or the use of those services arise among Participants or between a Participant and InCommon, the following procedure is intended to affect a resolution. This procedure will evolve as the Federation gains more experience with the types of disputes that may occur.

Upon resolution, a brief description of the dispute's issues and the resolution of those will be communicated to Federation Participants by email or protected website, unless non-publication is requested by any of the disputing Participants.

8.1 Disputes Among Participants

Participants are expected to make every reasonable effort to settle disputes among themselves, especially if contractual issues among the Participants are involved. If circumstances warrant, (for example, if the dispute centers on the interpretation of Attribute values or the implementation of standards) InCommon may be asked to act as referee in helping the Participants come to resolution.

The OM will serve as the Referee in working with Participants. The Referee will gather as much information as possible from each disputing party and then, if necessary, ask for additional information or advice from other operational staff or advisors. The Referee will then document in writing a proposed solution and submit it to the disputing parties for comment. The Referee then will submit a final draft to the Steering Committee.

8.2 Disputes Between Participant(s) and the Federation

Any Participant may submit a written Notice of Dispute to the OM regarding any aspect of the operation or services supported by the Federation. The OM will make

certain that sufficient information exists to define the dispute and then shall inform the Chair of the Steering Committee. The Chair will appoint one of the Steering Committee Members to serve as Negotiator with the disputing Participant(s).

The Negotiator will gather all the facts and rationales for the dispute and, as necessary, seek advice from any Federation advisors or other relevant parties. The Negotiator will prepare a written report, which shall include a recommended resolution of the dispute. The report shall be submitted to the Chair of the Steering Committee within 30 days of the appointment of the Negotiator unless delayed by the required fact finding.

The Chair shall bring the report to a quorum of the Steering Committee. The Committee, after reviewing the report, may ask for additional information or request the Negotiator to take into account further considerations and prepare a modified recommendation. Resolution of the dispute must be approved by affirmative vote of a quorum of the Steering Committee as defined in the Bylaws. If the Steering Committee is unable to affirm a resolution, the status quo is maintained. The OM shall report the Steering Committee's final action to the disputing Participant(s) in writing as soon thereafter as is practical. If any disputing party believes it cannot accept the outcome of this process, its only recourse would be to discontinue participation in the Federation as stated in the Participation Agreement.

9 Operations

The operation and performance of the Federation infrastructure are paramount to maintaining its trust fabric. InCommon supports certain operational services, including the operation of a certification authority for digital certificate life-cycle management, the secure collection and distribution of participant metadata, a registration authority to identity-proof and credential Participant organizations and officers, communications and outreach, and a Help Desk. As the Federation gains more experience with federated identity and access management and as requirements for higher assurance levels emerge, the InCommon Federation's operations will evolve to meet new functional criteria.

9.1 Operational Assurance Level

Complete procedures were developed detailing InCommon's central operations. Information security industry standards and practices¹ were used to establish the necessary level of assurance. These operations and procedures were approved by a technical advisory group of Internet2 Middleware Architects. A public listing of these procedures can be found on the InCommon website.

9.2 Communications and Support

All InCommon operating documents and Participant Operating Practices statements are made accessible via the InCommon website.

InCommon provides a Help Desk for Participant administrative and technical support. The Help Desk is staffed during normal Internet2 business hours as described on the InCommon website. InCommon also supports a community electronic mailing list for building community involvement and partnerships. Any

¹ RFC 2527, RFC 3647, The American Bar Association PKI Assessment Guidelines, *The Computer Security Handbook 4th edition, Planning for PKI: Best Practices Guide for Deploying Public Key Infrastructure* by Housley and Polk, The Federal Bridge Certification Authority Certification Policy, and others.

end users who inadvertently contact the Federation Help Desk will be referred to their home organization for support in online access to other Participants.

Software guidelines are provided or referenced on the website, along with deployment guides, attribute policies, testing facilities, and other federation-specific information for the operation of Identity Providers and Service Providers in the Federation.

9.3 Federation Technical Infrastructure

InCommon is responsible for the secure operation of a number of technology platforms including: a Shibboleth "Where Are You From" (WAYF) server; a Metadata distribution service; a participant administrative interface; a Certification Authority; and other necessary infrastructure. Operation of the technical infrastructure is described in greater detail in the technical documents available on the InCommon website.

9.3.1 Where Are You From (WAYF)

The WAYF, an optional user interface component, is responsible for allowing users to specify their appropriate Identity Provider for the services they intend to use on-line. Upon selecting an Identity Provider, the user is redirected to the Identity Provider's log in service to authenticate. InCommon operates a redundant WAYF service and Web page on which all Identity Providers are listed.

9.3.2 Metadata Distribution

InCommon digitally signs and makes available to Participants metadata submitted by all Participants for interoperation of Identity Provider and Service Provider systems. The metadata is maintained on redundant servers.

9.3.3 Participant Administrative Interface

Federation Participant Administrators use the Participant Administrative Interface to securely manage the data relevant to their organization's participation in the Federation. The particular tasks include submitting certificate signing requests, Participant Operating Practices, and submitting or modifying Participant metadata.

9.3.4 Certification Authority (CA)

InCommon operates an X.509 CA from which it issues server certificates for use within the Federation. Redundant Certificate Revocation Lists (CRL) are made available and are updated every 30 days or within one Internet2 business day of a verified certificate revocation request, whichever is sooner.

9.3.5 Suspension of Federation Services

If InCommon suspects compromise of any of its service components, it may take immediate action to remedy the situation or verify non-compromise, including taking components out of service for a limited time for diagnosis and repair. The OM always will endeavor to minimize interruption or inconvenience to Participants. Any critical compromise will be communicated to Participants in a timely manner.

9.4 Disaster Recovery

InCommon disaster recovery practices ensure the minimum interruption of availability of Federation services in the event of a disaster. This includes providing redundant hardware and secure data backups. Public versions of disaster recovery practices are available on the InCommon website.

10 Participation Status: Renewal, Withdrawal and Termination, and Suspension

10.1 Renewal

Renewal of Participation is automatic as long as the Participant remains in good standing and pays its fees in a timely manner.

10.2 Withdrawal and Termination

Participant may withdraw from the Federation at any time upon written notice to the InCommon office in accordance with the Participation Agreement.

Termination by InCommon or Participant is governed by the Term provisions of the Participation Agreement.

In all cases of Withdrawal or Termination, the Participant will be removed from the metadata.

10.3 Suspension of Participants' Services

A Participant may request the suspension of any Federation services in the case of Administrator credential compromise, participant key compromise, or other security compromise within the Participant's systems. This request may be made via e-mail or telephone from the Executive or Administrator and will be verified by InCommon using trusted communication channels. Suspension may include processes such as revoking credentials, removing or modifying metadata, or revoking certificates.

If InCommon suspects any compromise or negligence on the part of a Participant, it will make reasonable efforts to contact Participant to verify Participant's status. For example, a non-responsive Administrator's account may be suspended for the security and safety of Participant's metadata if InCommon suspects an Administrator is no longer active and its repeated attempts at contact go unanswered.

11 Further Risk Assessment

For additional information highlighting some of the ways in which operation of the Federation might incur risk to Participants, please read the risk assessment paper found on the InCommon website.

INCOMMON FEDERATION: PARTICIPATION AGREEMENT

v. April 14, 2011

This agreement ("Agreement") for participation in the InCommon Federation services (the "Federation") is made and entered into by InCommon, LLC ("InCommon") and the Participant, _____, (collectively, InCommon and Participant are referred to as "parties"). PARTICIPANT BY EXECUTING THIS AGREEMENT ACKNOWLEDGES AND AGREES THAT PARTICIPANT HAS CAREFULLY READ AND ACCEPTS THE TERMS AND CONDITIONS OF THIS AGREEMENT, AND FURTHER ACKNOWLEDGES THAT PARTICIPANT WILL BE BOUND LEGALLY BY ITS TERMS AND CONDITIONS.

1. The InCommon Federation

Internet2 has created InCommon as a service to higher education and research organizations in the U.S. The InCommon Federation is an activity of InCommon and is generally governed by a Steering Committee representing the interests of Participants. The purpose and role of the Federation is set forth in more detail in the Limited Liability Company Agreement ("LLC Agreement") and Federation Operating Practices and Procedures ("FOPP") of the Federation as amended from time to time by the InCommon Steering Committee. InCommon accepts applications from organizations that are potential Participants in the Federation, as defined in the FOPP, and provides the Federation services to Participants ("InCommon Participants") under the terms and conditions of this Agreement.

2. Legal Form of InCommon

InCommon, LLC is organized and operated as a Delaware limited liability company (LLC). InCommon's sole member is University Corporation for Advanced Internet Development, Inc. d/b/a Internet2 ("Internet2"), a District of Columbia not-for-profit Corporation. The InCommon Federation is operated in accordance with its LLC Agreement and FOPP. By entering into this Agreement, Participant (i) agrees that its participation in the Federation shall not provide Participant with any right or interest in InCommon or its assets and (ii) acknowledges that it has the opportunity to review the LLC Agreement and FOPP, available on the InCommon website.

3. InCommon Participation

With respect to its participation in the InCommon Federation, Participant agrees to abide by policies and standards established by the Federation designed to enable trustworthy shared management of access to on-line resources. Participant may register Identity Management systems and Resource Provider Identifiers as defined in section 7 below.

4. Participant Classes and Fees

- a. *Classes of Participants.* InCommon defines, and may change from time to time, different classes of InCommon Participants. Different classes may receive different services, may have different roles in InCommon activities, and may be liable for different fees and/or dues. Currently defined classes are Higher Education Institutions, Sponsored Partners, and Research Organizations (as defined in the FOPP).

Participant is primarily (check only one):

Higher Education [] Sponsored Partner [] Research Organization []

- b. *Participant Fees.*

Participant fees are assessed on a one-time or annual basis and are not refundable.

- i. Registration Fee. Each InCommon Participant, including Participant, must pay a registration fee ("Registration Fee"), as defined in the attached InCommon Fee Schedule, to cover initial identification and authentication costs and expenses incurred by InCommon.
- ii. Annual Participation Fee. Each InCommon Participant, including Participant, shall be required to pay annual fees ("Annual Participation Fees"), as defined in the attached InCommon Fee Schedule. Participant acknowledges that the Annual Participation Fees may be modified by the InCommon Steering Committee, as necessary, to support the management and operations of InCommon and to respond to the needs of new applications and services. The Annual Participation Fees shall be annually assessed and payable on or before January 1st of each year, unless either the Participant or InCommon has given written notice of termination of this Agreement at least 90 days prior to the renewal date above or within 30 days from the date of notice of Annual Participation Fees, whichever is later.
- iii. Payment of Fees. All Registration fees must be paid by credit card using the secure web interface provided by InCommon. All Annual Participation fees must be paid by any of several methods outlined on the invoice within 60 days of the issuance date of the invoice.

5. Term

- a. *Term.* This Agreement comes into force on the date of acceptance by each party and remains in force through December 31 of the current calendar year (unless terminated sooner) and from year to year thereafter, January 1 through December 31, unless either InCommon or Participant notifies the other to the contrary as provided in Section 4.b.ii, 5.b., or 5.c.

- b. *Participant Withdrawal from InCommon Federation.* Participant shall be permitted to withdraw from participation in the Federation at any time by giving written notice to InCommon of its intent to terminate its participation. If Participant withdraws from the Federation under this Section 5b, Participant shall not be entitled to a refund of its Registration or Annual Participation Fees.
- c. *Termination.* This Agreement may be terminated for cause by either party for failure of the other party to comply with or to perform any term, condition, representation or covenant contained in this Agreement and such failure continues for ten (10) business days after written notice from the other party thereof. Furthermore, Participant's participation in the Federation may be terminated with cause at any time by the majority vote of a quorum of the InCommon Steering Committee. If Participant is terminated from the Federation under this Section 5c, Participant shall not be entitled to a refund of its Registration or Annual Participation Fees.

6. Participant Responsibilities

Participant covenants and agrees to do the following during the term of this Agreement in addition to any other obligations specified herein:

- a. Employ software in conformance with the document, "InCommon Federation Software Guidelines," available on the InCommon website;
- b. Support as defined, and make use of the identity attributes described in the document "InCommon Federation Attribute Overview" available on the InCommon website;
- c. Provide InCommon with accurate metadata: URL trees associated with resources and appropriate corresponding names for user interfaces;
- d. The terms of any agreement for the access of online resources between or among Participants, including terms and conditions related to technical, intellectual property, and other requirements and policies, shall be agreed to by and among such Participants;
- e. Provide technical and administrative contact information as necessary to facilitate contact by other InCommon Participants, and identify to InCommon certain organizational representatives as outlined in section 18 and keep InCommon apprised of any changes to the individuals assigned to these trusted roles;
- f. Bear its own costs and expenses in connection with its participation in InCommon, including without limitation compensation of its employees, and all travel and living expenses associated with the Participant's participation in any meetings and conferences;

- g. Participant agrees not to participate in the Federation in a manner that violates federal, state or local laws and rules, or in a manner that interferes or could interfere with services provided to others;
- h. Participant agrees to make available for distribution to InCommon or any InCommon Participant reliable and trustworthy information about Participant's identity management systems and/or resource management systems by documenting certain specific aspects of its operational and privacy practices in its own Participant Operational Practices ("POP"), a template of which is available on the InCommon website.

7. InCommon Federation Services

a. *System Registrations*

Any participant – Higher Education, Research Organization, or Sponsored Partner – may register with the Federation any number of Identity Provider systems ("IdPs") allowed per Annual Fee Package (see Fee Schedule) that will offer identity assertions to other InCommon Participants. Such an IdP must abide by this Agreement and the rules and policies of InCommon. Participant agrees to be responsible for the actions of all IdPs registered by Participant.

Any participant – Higher Education, Research Organization, or Sponsored Partner – may register with the Federation any number of Service Provider systems ("SPs") allowed per Annual Fee Package that will provide access to on-line resources based at least in part on identity assertions provided by InCommon Participant IdP systems.

All Participant's systems (IdPs and SPs) must be under the management control of Participant. Participant may not register third party systems of any type.

b. *Participant Metadata*

InCommon will use reasonable efforts to provide periodically to Participant composite metadata describing all Higher Education systems and Sponsored Partner systems that have been registered with InCommon. THIS METADATA IS PROVIDED ON A BEST EFFORT BASIS AND IS NOT WARRANTED NOR GUARANTEED TO BE COMPLETE, CORRECT, OR FIT FOR ANY PARTICULAR PURPOSE. PARTICIPANT CONSENTS TO INCOMMON SHARING PARTICIPANT'S METADATA WITH OTHER INCOMMON PARTICIPANTS.

8. Respect for Intellectual Property

Participant agrees, and agrees to advise its end-users as Participant deems appropriate to respect the copyright on any content accessed by virtue of participation in the Federation or through or by other InCommon Participants, in accordance with the terms and conditions established by the InCommon Participant(s) providing access to that

content. Participant also agrees and agrees to advise its end-users as Participant deems appropriate to abide by the terms of any copyrights applicable to the use of InCommon software, documents, or other materials developed by the Federation or Federation Participants.

9. Respect for Privacy of Identity Information

Participant agrees to respect the privacy of and any other constraints placed on identity information that it might receive from other InCommon Participants as agreed upon between Participant and the InCommon Participant(s). In particular, Participant understands that it may not permanently store nor share or disclose or use for any purpose other than its intended purpose any identity information that it receives from another InCommon Participant without express written permission of the other InCommon Participant. Participant understands that the storing and sharing of resources is between the Participant and the InCommon Participant(s) and is not the responsibility of InCommon.

InCommon strongly recommends that Resource provider systems may cache temporarily identity attributes/credentials that are supplied by IdMs for operational efficiency or sequential, repeated authentication purposes within a given session or reasonable length episode. InCommon further recommends that any shared attributes/credentials should not be used for any purpose other than the original purpose or intent, and that such attributes/credentials should be destroyed at the end of the session or episode in which they are needed. This temporary storage of credentials shall not be deemed as permanent storage for the purposes of this Agreement.

10. Dispute Resolution Procedures For Participants

In the event of any dispute or disagreement between two or more InCommon Participants ("Disputing Participants") arising out of or pertaining to their participation in the Federation, the parties agree to make every reasonable attempt to resolve the dispute between or among themselves. In the case that such a dispute cannot be so resolved, the Disputing Participants may choose to submit the dispute to the InCommon Steering Committee. If the dispute is between an InCommon Participant and InCommon and arises out of or pertains to the participation in the Federation, or the dispute is between or among InCommon Participants and affects the Federation, the InCommon Participant(s) shall submit the dispute to the InCommon Steering Committee following procedures defined in the FOPP. The InCommon Steering Committee shall resolve the dispute in the best interests of the Federation. Participant agrees that all decisions by the InCommon Steering Committee concerning disputes between InCommon and Participant shall be final, provided that Participant may terminate its participation in the Federation (per section 5b) if it disagrees with a decision of the Steering Committee and shall not be bound by such decision.

11. Disclaimer and Limitation on Liability

- a. ANY SERVICE PROVIDED FOR HEREIN BY INCOMMON, INCOMMON PARTICIPANTS OR ANY OF INCOMMON'S THIRD

PARTY SERVICE PROVIDERS IS PROVIDED ON AN AS IS, AS AVAILABLE BASIS, WITHOUT WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. INCOMMON EXPRESSLY DISCLAIMS ANY REPRESENTATION OR WARRANTY THAT ANY SERVICE WILL BE ERROR-FREE, SECURE, OR UNINTERRUPTED. NO STATEMENT, ORAL OR WRITTEN, GIVEN BY INCOMMON, ANY OF ITS EMPLOYEES, OR ANY OTHER PERSON WILL CREATE A WARRANTY, NOR MAY ANY PARTICIPANT OR OTHER PERSON RELY ON ANY SUCH STATEMENT FOR ANY PURPOSE. FURTHERMORE, NOTWITHSTANDING ANY CONTRARY PROVISION SET FORTH IN THIS AGREEMENT, PARTICIPANT EXPRESSLY AGREES THAT IN NO EVENT SHALL INCOMMON'S ENTIRE LIABILITY FOR ANY LIABILITIES, LOSSES, CLAIMS, JUDGMENTS, DAMAGES (WHETHER DIRECT, INDIRECT, CONSEQUENTIAL, INCIDENTAL, SPECIAL OR OTHERWISE), EXPENSES OR COSTS (INCLUDING REASONABLE FEES AND EXPENSES OF COUNSEL) ARISING OUT OF THIS AGREEMENT, WHETHER IN CONTRACT, TORT OR OTHERWISE, EXCEPT FOR DIRECT DAMAGES RESULTING SOLELY FROM INCOMMON'S INTENTIONAL AND WILLFUL ACTIONS, EXCEED AN AMOUNT EQUAL TO THE AMOUNT OF THE ANNUAL FEE PAID BY THE PARTICIPANT TO INCOMMON UNDER THIS AGREEMENT DURING ANY CONSECUTIVE TWELVE (12) MONTH PERIOD, MULTIPLIED BY A FRACTION THE NUMERATOR OF WHICH IS THE NUMBER OF MONTHS IMMEDIATELY PRECEDING THE OCCURRENCE OF THE EVENT GIVING RISE TO THE CLAIM IN SUCH CONSECUTIVE TWELVE (12) MONTH PERIOD AND THE DENOMINATOR OF WHICH IS TWELVE (12).

- b. InCommon, its third party services providers, and InCommon Participants reserve the right to interrupt, suspend or reduce the provision of any service to Participant, or any other person, including the Participant's end users, when such action is necessary in InCommon's sole judgment. InCommon will endeavor where reasonably possible, but does not promise, to provide advance notice to Participant of any such interruption, suspension, or reduction. As soon as possible following the interruption, suspension, or reduction InCommon will contact the Participant and any participants in an attempt to resolve any problems and restore service. NOTWITHSTANDING ANY OTHER PROVISION HEREIN, INCOMMON, INCOMMON PARTICIPANTS, AND INCOMMON THIRD PARTY SERVICE PROVIDERS OR THEIR DESIGNEES SHALL NOT BE LIABLE TO PARTICIPANT OR OTHER PERSON FOR ANY ERROR IN TRANSMISSION OR LACK THEREOF OR FOR ANY INTERRUPTION OR TERMINATION OF PARTICIPATION, EITHER PARTIAL OR TOTAL, EITHER INTENTIONAL OR ACCIDENTAL (INCLUDING ANY ERROR, INTERRUPTION OR TERMINATION DUE TO THE

DELIBERATE MISCONDUCT OR NEGLIGENCE OF ANY PERSON), WHETHER OR NOT PRIOR NOTICE OF ANY SUCH INTERRUPTION OR TERMINATION HAS BEEN GIVEN.

- c. InCommon shall not be liable to Participant (or its end-users) for claims or damages caused in whole or part by (i) the fault or negligence of InCommon Participants or by the failure of InCommon Participants to perform their responsibilities; (ii) third party claims against InCommon Participants, except to the extent that such claims arise solely from the intentional and willful actions of InCommon; or (iii) any act or omission of any other party furnishing products or services to InCommon or InCommon Participants. Furthermore, InCommon shall not be liable, either in contract, in tort or otherwise, for unauthorized access to Participant's transmission facilities, its equipment, or unauthorized access to or alteration, delay, theft or destruction of Participant's (or its end users') data files, programs, procedures or other information, except for direct damages arising solely from the intentional and willful actions of InCommon.
- d. Participant is and shall be solely responsible for any or all use of any service or resource obtained as a result of participating in the Federation, including but not limited to audio, video, text, data or other communications originating or transmitted from any site owned or operated by Participant, including any third party content or materials, routed to, passed through and/or stored on or otherwise transmitted or routed to any other InCommon Participant or user ("Participant Content"). InCommon does not intend to review the Participant Content, and Participant assumes all responsibility for use of such Participant Content. Participant shall make no claim against InCommon regarding said Participant Content. The Steering Committee of InCommon or its designees, is responsible for the governing policies of the federation, its purposes and uses, and Participant agrees to be bound by its official, approved policies with regard to federation participation.
- e. Participant acknowledges that InCommon does not conduct its own review or due diligence concerning the qualifications of prospective participants in the Federation, but instead relies on the promises made by InCommon Participants that they will observe and abide by all operating, intellectual property, and other requirements imposed by InCommon or InCommon Participants in connection with their participation in the Federation.

12. Insurance

Participant covenants and agrees to obtain and maintain in force, at its own expense, throughout the term of this Agreement, commercial general liability insurance coverage with a combined single limit of not less than \$3,000,000.00 each occurrence or its equivalent, whether such insurance is maintained through self-insurance or through third party insurance, against claims, regardless of when asserted, that may arise out of, or result from, Participant's participation in the Federation.

13. Severability and Assignment

If any provision of this Agreement or the application thereof in any circumstances, is held to be invalid, illegal or unenforceable in any respect for any reason, the validity, legality and enforceability of any such provision(s) in every other respect and the rest of the provisions of this Agreement shall remain in effect, unless the provisions held invalid, illegal or unenforceable shall substantially impair the benefits of the remaining provisions hereto. This Agreement is not assignable without the express written consent of InCommon.

14. Third Party Beneficiaries

This Agreement is for the sole benefit of the Parties hereto, except as provided for in Sections 2, 5.c, 11.a, and 11.b, nothing herein expressed or implied shall give or be construed to give to any person, other than the Parties hereto, any legal or equitable rights hereunder.

15. Governing Law

This Agreement shall be governed by and interpreted in accordance with the laws of Delaware, and exclusive venue for any and all disputes under law or jurisprudence hereunder shall lie in the state or federal courts located in the State of Delaware.

16. No Joint Venture

Nothing herein shall be construed as creating a partnership, employment or agency relationship between the Parties or as authorizing any party to act as agent for any other party.

17. Modification

This Agreement may be modified only by written consent of the Parties; provided, however, that InCommon retains the right to amend this Agreement unilaterally to conform to any modifications made by InCommon to its policies if so approved by the InCommon Steering Committee. Any such unilateral changes shall be presented to Participant at least ninety (90) days before they are to take effect, and InCommon will work in good faith with Participant to negotiate and resolve any issues raised by such changes that may be of concern to Participant. Each participant's continued participation in InCommon after the change takes effect will constitute its continuing agreement to this Agreement as so modified. Each participant, including Participant, has the right to terminate this Agreement if it is modified in any way that is not acceptable to the Participant.

18. Authorization of Executive

The following person has been designated as the InCommon Executive for Participant regarding InCommon Participation. This Participant Executive represents Participant regarding all decisions and delegations of authority for the responsibilities of InCommon

Participants, including but not limited to payment of invoices, and assigning any person in the trusted Administrator role who submits Certificate Signing Requests, metadata, or Certificate Revocation Requests, and other administrative duties as described herein.

Participant Executive Contact information

Name _____

Title _____

Postal Address _____

Email Address _____

Telephone _____

Fax _____

19. Notices

All notices and other communications hereunder may be delivered to Participant or InCommon by postal mail, email, or facsimile to the following respective addresses, unless or until otherwise notified by the Participant or InCommon in writing to the other party:

Participant Communication Representative Contact information

Name _____

Postal Address _____

Email Address _____

Telephone _____

Fax _____

InCommon contact information
InCommon, LLC
c/o Internet2
1000 Oakbrook Drive, Suite 300
Ann Arbor, MI 48104

Email address: incommon-admin@incommonfederation.org
Facsimile: 734-913-4255
Telephone: 734-913-4250

20. Entire Agreement

This Agreement sets forth the entire understanding of the Parties with regard to the subject matter hereof and merges and supersedes all prior communications or discussions, oral or written, with regard thereto, and no changes, modifications or amendments to this Agreement shall be binding unless agreed by all Parties in writing as defined in Section 17 above. No party to this Agreement may assign or delegate any rights or interests under this Agreement without each other party's prior written consent.

21. Survival of Provisions

This Section 21 and Sections 8, 11, 12, and 15 shall survive the expiration or termination of this Agreement.

22. Execution of this Agreement

This Agreement becomes effective when signed by an officer of each party empowered to enter into legally binding contracts on behalf of their respective organizations.

Agreed to on behalf of Participant by:

Signature

Date

Print Name

Title

Accepted on behalf of InCommon by:

Signature

Date

Print Name

Title

Attachment: InCommon Federation: Service Fee Schedule

Each participant in the InCommon Federation pays a one-time registration fee and also an annual fee. **The one-time registration fee** covers the costs of vetting your organization, and the identity proofing of your executive and administrator. This fee is paid by credit card when you submit your on-line registration form. **Annual fees** support the ongoing operations of the federation and are prorated in the first year, based on the quarter in which a participant joins the federation. After this first year, annual fees for all participants are not prorated and are due on January 1.

Annual fees include the registration of one identity management system and up to fifty (50) service provider entities. A participant may only register a system over which it has management control. Third-party systems are not permitted as outlined in the participation agreement.

The base annual package allows for up to 50 Service Provider IDs, which are registered individually as needed. With the registration of the 51st SP, InCommon will issue an invoice for another package of 50 as part of the next year's annual fee. Higher Education Participants are strongly encouraged to register only one identity management system, though they may register additional systems. InCommon must approve registration of any additional identity systems. Such a case would require an additional fee package as outlined below.

InCommon fees recover the costs of providing services to federation participants and are determined and reviewed by the InCommon Steering Committee.

Fee Schedules

Fee schedules are available on the InCommon website:

Higher Education: www.incommon.org/fees_HE.html

Sponsored Partners: www.incommon.org/fees_SP.html

Research Organizations: www.incommon.org/fees_research.html

INCOMMON FEDERATION: PARTICIPANT OPERATIONAL PRACTICES

Participation in the InCommon Federation ("Federation") enables a federation participating organization ("Participant") to use Shibboleth *identity attribute* sharing technologies to manage access to on-line resources that can be made available to the InCommon community. One goal of the Federation is to develop, over time, community standards for such cooperating organizations to ensure that shared *attribute assertions* are sufficiently robust and trustworthy to manage access to important protected resources. As the community of trust evolves, the Federation expects that participants eventually should be able to trust each other's *identity management systems* and *resource access management systems* as they trust their own.

A fundamental expectation of Participants is that they provide authoritative and accurate attribute assertions to other Participants, and that Participants receiving an attribute assertion protect it and respect privacy constraints placed on it by the Federation or the source of that information. In furtherance of this goal, InCommon requires that each Participant make available to other Participants certain basic information about any identity management system, including the identity attributes that are supported, or resource access management system registered for use within the Federation.

Two criteria for trustworthy attribute assertions by *Identity Providers* are: (1) that the identity management system fall under the purview of the organization's executive or business management, and (2) the system for issuing end-user credentials (e.g., PKI certificates, userids/passwords, Kerberos principals, etc.) specifically have in place appropriate risk management measures (e.g., *authentication* and *authorization* standards, security practices, risk assessment, change management controls, audit trails, etc.).

InCommon expects that *Service Providers*, who receive attribute assertions from another Participant, respect the other Participant's policies, rules, and standards regarding the protection and use of that data. Furthermore, such information should be used only for the purposes for which it was provided. InCommon strongly discourages the sharing of that data with third parties, or aggregation of it for marketing purposes without the explicit permission¹ of the identity information providing Participant.

InCommon requires Participants to make available to all other Participants answers to the questions below.² Additional information to help answer each question is available in the next section of this document. There is also a glossary at the end of this document that defines terms shown in italics.

¹ Such permission already might be implied by existing contractual agreements.

² Your responses to these questions should be posted in a readily accessible place on your web site, and the URL submitted to InCommon. If not posted, you should post contact information for an office that can discuss it privately with other InCommon Participants as needed. If any of the information changes, you must update your on-line statement as soon as possible.

1. Federation Participant Information

1.1 The InCommon Participant Operational Practices information below is for:

InCommon Participant organization name _____

The information below is accurate as of this date _____

1.2 Identity Management and/or Privacy information

Additional information about the Participant's identity management practices and/or privacy policy regarding personal information can be found on-line at the following location(s).

URL(s) _____

1.3 Contact information

The following person or office can answer questions about the Participant's identity management system or resource access management policy or practice.

Name _____

Title or role _____

Email address _____

Phone _____ FAX _____

2. Identity Provider Information

The most critical responsibility that an IdentityProvider Participant has to the Federation is to provide trustworthy and accurate identity assertions.³ It is important for a Service Provider to know how your *electronic identity credentials* are issued and how reliable the information associated with a given credential (or person) is.

Community

2.1 If you are an Identity Provider, how do you define the set of people who are eligible to receive an *electronic identity*? If exceptions to this definition are allowed, who must approve such an exception?

2.2 "Member of Community"⁴ is an assertion that might be offered to enable access to resources made available to individuals who participate in the primary mission of the university or organization. For example, this assertion might apply to

³ A general note regarding attributes and recommendations within the Federation is available here:
<http://www.incommonfederation.org/attributes.html>

⁴ "Member" is one possible value for eduPersonAffiliation as defined in the eduPerson schema. It is intended to include faculty, staff, student, and other persons with a basic set of privileges that go with membership in the university community (e.g., library privileges). "Member of Community" could be derived from other values in eduPersonAffiliation or assigned explicitly as "Member" in the electronic identity database. See <http://www.educause.edu/eduperson/>

anyone whose affiliation is “current student, faculty, or staff.”

What subset of persons registered in your identity management system would you identify as a “Member of Community” in Shibboleth identity assertions to other InCommon Participants?

Electronic Identity Credentials

2.3 Please describe in general terms the administrative process used to establish an electronic identity that results in a record for that person being created in your *electronic identity database*? Please identify the office(s) of record for this purpose. For example, “Registrar’s Office for students; HR for faculty and staff.”

2.4 What technologies are used for your electronic identity credentials (e.g., Kerberos, userID/password, PKI, ...) that are relevant to Federation activities? If more than one type of electronic credential is issued, how is it determined who receives which type? If multiple credentials are linked, how is this managed (e.g., anyone with a Kerberos credential also can acquire a PKI credential) and recorded?

2.5 If your electronic identity credentials require the use of a secret password or PIN, and there are circumstances in which that secret would be transmitted across a network without being protected by encryption (i.e., “clear text passwords” are used when accessing campus services), please identify who in your organization can discuss with any other Participant concerns that this might raise for them:

2.6 If you support a “single sign-on” (SSO) or similar campus-wide system to allow a single user authentication action to serve multiple applications, and you will make use of this to authenticate people for InCommon Service Providers, please describe the key security aspects of your SSO system including whether session timeouts are enforced by the system, whether user-initiated session termination is supported, and how use with “public access sites” is protected.

2.7 Are your primary *electronic identifiers* for people, such as “net ID,” eduPersonPrincipalName, or eduPersonTargetedID considered to be unique for all time to the individual to whom they are assigned? If not, what is your policy for re-assignment and is there a hiatus between such reuse?

Electronic Identity Database

- 2.8 How is information in your electronic identity database acquired and updated?
Are specific offices designated by your administration to perform this function?
Are individuals allowed to update their own information on-line?
-

- 2.9 What information in this database is considered “public information” and would be provided to any interested party?
-

Uses of Your Electronic Identity Credential System

- 2.10 Please identify typical classes of applications for which your electronic identity credentials are used within your own organization.
-

Attribute Assertions

Attributes are the information data elements in an attribute assertion you might make to another Federation participant concerning the identity of a person in your identity management system.

- 2.11 Would you consider your attribute assertions to be reliable enough to:
- [] control access to on-line information databases licensed to your organization?
 - [] be used to purchase goods or services for your organization?
 - [] enable access to personal information such as student loan status?

Privacy Policy

Federation Participants must respect the legal and organizational privacy constraints on attribute information provided by other Participants and use it only for its intended purposes.

- 2.12 What restrictions do you place on the use of attribute information that you might provide to other Federation participants?
-

- 2.13 What policies govern the use of attribute information that you might release to other Federation participants? For example, is some information subject to FERPA or HIPAA restrictions?
-

3. Service Provider Information

Service Providers are trusted to ask for only the information necessary to make an appropriate access control decision, and to not misuse information provided to them by Identity Providers. Service Providers must describe the basis on which access to

resources is managed and their practices with respect to attribute information they receive from other Participants.

3.1 What attribute information about an individual do you require in order to manage access to resources you make available to other Participants? Describe separately for each service ProviderID that you have registered.

3.2 What use do you make of attribute information that you receive in addition to basic access control decisions? For example, do you aggregate session access records or records of specific information accessed based on attribute information, or make attribute information available to partner organizations, etc.?

3.3 What human and technical controls are in place on access to and use of attribute information that might refer to only one specific person (i.e., personally identifiable information)? For example, is this information encrypted?

3.4 Describe the human and technical controls that are in place on the management of super-user and other privileged accounts that might have the authority to grant access to personally identifiable information?

3.5 If personally identifiable information is compromised, what actions do you take to notify potentially affected individuals?

4. Other Information

4.1 Technical Standards, Versions and Interoperability

Identify the version of Internet2 Shibboleth code release that you are using or, if not using the standard Shibboleth code, what version(s) of the SAML and SOAP and any other relevant standards you have implemented for this purpose.

4.2 Other Considerations

Are there any other considerations or information that you wish to make known to other Federation participants with whom you might interoperate? For example, are there concerns about the use of clear text passwords or responsibilities in case of a security breach involving identity information you may have provided?

Additional Notes and Details on the Operational Practices Questions

As a community of organizations willing to manage access to on-line resources cooperatively, and often without formal contracts in the case of non-commercial resources, it is essential that each Participant have a good understanding of the *identity* and resource management practices implemented by other Participants. The purpose of the questions above is to establish a base level of common understanding by making this information available for other Participants to evaluate.

In answering these questions, please consider what you would want to know about your own operations if you were another Participant deciding what level of trust to place in interactions with your on-line systems. For example:

- What would you need to know about an *Identity Provider* in order to make an informed decision whether to accept its *assertions* to manage access to your on-line resources or applications?
- What would you need to know about a *Service Provider* in order to feel confident providing it information that it might not otherwise be able to have?

It also might help to consider how *identity management systems* within a single institution could be used.

- What might your central campus IT organization, as a *Service Provider*, ask of a peer campus *Identity Provider* (e.g., Computer Science Department, central Library, or Medical Center) in order to decide whether to accept its *identity assertions* for access to resources that the IT organization controls?
- What might a campus department ask about the central campus *identity management system* if the department wanted to leverage it for use with its own applications?

The numbered paragraphs below provide additional background to the numbered questions in the main part of this document.

[1.2] InCommon Participants who manage Identity Providers are strongly encouraged to post on their website the privacy and information security policies that govern their *identity management system*. Participants who manage Service Providers are strongly encouraged to post their policies with respect to use of personally identifying information.

[1.3] Other InCommon Participants may wish to contact this person or office with further questions about the information you have provided or if they wish to establish a more formal relationship with your organization regarding resource sharing.

[2] Many organizations have very informal processes for issuing electronic credentials. For example, one campus does this through its student bookstore. A

Service Provider may be more willing to accept your *assertions* to the extent that this process can be seen as authoritative.

- [2.1] It is important for a *Service Provider* to have some idea of the community whose identities you may represent. This is particularly true for *assertions* such as the eduPerson “Member of Community.”. A typical definition might be “Faculty, staff, and active students” but it might also include alumni, prospective students, temporary employees, visiting scholars, etc. In addition, there may be formal or informal mechanisms for making exceptions to this definition, e.g., to accommodate a former student still finishing a thesis or an unpaid volunteer.

This question asks to whom you, as an *Identity Provider*, will provide electronic credentials. This is typically broadly defined so that the organization can accommodate a wide variety of applications locally. The reason this question is important is to distinguish between the set of people who might have a credential that you issue and the subset of those people who fall within your definition of “Member of Community” for the purpose of InCommon *attribute assertions*.

- [2.2] The *assertion* of “Member of Community” is often good enough for deciding whether to grant access to basic on-line resources such as library-like materials or websites. InCommon encourages participants to use this *assertion* only for “Faculty, Staff, and active Students” but some organizations may have the need to define this differently. InCommon *Service Providers* need to know if this has been defined differently.
- [2.3] For example, if there is a campus recognized office of record that issues such electronic credentials and that office makes use of strong, reliable technology and good database management practices, those factors might indicate highly reliable credentials and hence trustworthy *identity assertions*.
- [2.4] Different technologies carry different inherent risks. For example, a userID and password can be shared or “stolen” rather easily. A PKI credential or SecureID card is much harder to share or steal. For practical reasons, some campuses use one technology for student credentials and another for faculty and staff. In some cases, sensitive applications will warrant stronger and/or secondary credentials.
- [2.5] Sending passwords in “clear text” is a significant risk, and all InCommon Participants are strongly encouraged to eliminate any such practice. Unfortunately this may be difficult, particularly with legacy applications. For example, gaining access to a centralized calendar application via a wireless data connection while you are attending a conference might reveal your password to many others at that conference. If this is also your campus credential password, it could be used by another person to impersonate you to InCommon Participants.
- [2.6] “Single sign-on” (SSO) is a method that allows a user to unlock his or her *electronic identity credential* once and then use it for access to a variety of resources and

applications for some period of time. This avoids people having to remember many different identifiers and passwords or to continually log into and out of systems. However, it also may weaken the link between an *electronic identity* and the actual person to whom it refers if someone else might be able to use the same computer and assume the former user's *identity*. If there is no limit on the duration of a SSO session, a Federation *Service Provider* may be concerned about the validity of any *identity assertions* you might make. Therefore it is important to ask about your use of SSO technologies.

- [2.7] In some *identity management systems*, primary identifiers for people might be reused, particularly if they contain common names, e.g. Jim Smith@MYU.edu. This can create ambiguity if a *Service Provider* requires this primary identifier to manage access to resources for that person.
 - [2.8] Security of the database that holds information about a person is at least as critical as the *electronic identity credentials* that provide the links to records in that database. Appropriate security for the database, as well as management and audit trails of changes made to that database, and management of access to that database information are important.
 - [2.9] Many organizations will make available to anyone certain, limited "public information." Other information may be given only to internal organization users or applications, or may require permission from the subject under FERPA or HIPAA rules. A *Service Provider* may need to know what information you are willing to make available as "public information" and what rules might apply to other information that you might release.
 - [2.10] In order to help a *Service Provider* assess how reliable your *identity assertions* may be, it is helpful to know how your organization uses those same assertions. The assumption here is that you are or will use the same *identity management system* for your own applications as you are using for federated purposes.
 - [2.11] Your answer to this question indicates the degree of confidence you have in the accuracy of your *identity assertions*.
 - [2.12] Even "public information" may be constrained in how it can be used. For example, creating a marketing email list by "harvesting" email addresses from a campus directory web site may be considered illicit use of that information. Please indicate what restrictions you place on information you make available to others.
 - [2.13] Please indicate what legal or other external constraints there may be on information you make available to others.
- [3.1] Please identify your access management requirements to help other Participants understand and plan for use of your resource(s). You might also or instead provide contact information for an office or person who could answer inquiries.

- [3.2] As a *Service Provider*, please declare what use(s) you would make of attribute information you receive.
 - [3.3] Personally identifying information can be a wide variety of things, not merely a name or credit card number. All information other than large group identity, e.g., "member of community," should be protected while resident on your systems.
 - [3.4] Certain functional positions can have extraordinary privileges with respect to information on your systems. What oversight means are in place to ensure incumbents do not misuse such privileges?
 - [3.5] Occasionally protections break down and information is compromised. Some states have laws requiring notification of affected individuals. What legal and/or institutional policies govern notification of individuals if information you hold is compromised?
- [4.1] Most InCommon Participants will use Internet2 Shibboleth technology, but this is not required. It may be important for other participants to understand whether you are using other implementations of the technology standards.
 - [4.2] As an *Identity Provider*, you may wish to place constraints on the kinds of applications that may make use of your *assertions*. As a *Service Provider*, you may wish to make a statement about how User credentials must be managed. This question is completely open ended and for your use.

Glossary

access management system	The collection of systems and or services associated with specific on-line resources and/or services that together derive the decision about whether to allow a given individual to gain access to those resources or make use of those services.
assertion	The <i>identity</i> information provided by an <i>Identity Provider</i> to a <i>Service Provider</i> .
attribute	A single piece of information associated with an <i>electronic identity database</i> record. Some <i>attributes</i> are general; others are personal. Some subset of all <i>attributes</i> defines a unique individual.
authentication	The process by which a person verifies or confirms their association with an <i>electronic identifier</i> . For example, entering a password that is associated with an UserID or account name is assumed to verify that the user is the person to whom the UserID was issued.
authorization	The process of determining whether a specific person should be allowed to gain access to an application or function, or to make use of a resource. The resource manager then makes the access control decision, which also may take into account other factors such as time of day, location of the user, and/or load on the resource system.
electronic identifier	A string of characters or structured data that may be used to reference an <i>electronic identity</i> . Examples include an email address, a user account name, a Kerberos principal name, a UC or campus <i>NetID</i> , an employee or student ID, or a PKI certificate.
electronic identity	A set of information that is maintained about an individual, typically in campus <i>electronic identity databases</i> . May include roles and privileges as well as personal information. The information must be authoritative to the applications for which it will be used.
electronic identity credential	An <i>electronic identifier</i> and corresponding <i>personal secret</i> associated with an <i>electronic identity</i> . An <i>electronic identity credential</i> typically is issued to the person who is the subject of the information to enable that person to gain access to applications or other resources that need to control such access.
electronic identity database	A structured collection of information pertaining to a given individual. Sometimes referred to as an "enterprise directory." Typically includes name, address, email address, affiliation, and <i>electronic identifier(s)</i> . Many technologies can be used to create an <i>identity database</i> , for example LDAP or a set of linked relational databases.

identity	<i>Identity</i> is the set of information associated with a specific physical person or other entity. Typically an Identity Provider will be authoritative for only a subset of a person's <i>identity</i> information. What <i>identity attributes</i> might be relevant in any situation depend on the context in which it is being questioned.
identity management system	A set of standards, procedures and technologies that provide electronic credentials to individuals and maintain authoritative information about the holders of those credentials.
Identity Provider	A campus or other organization that manages and operates an <i>identity management system</i> and offers information about members of its community to other InCommon participants.
NetID	An <i>electronic identifier</i> created specifically for use with on-line applications. It is often an integer and typically has no other meaning.
personal secret (also verification token)	Used in the context of this document, is synonymous with password, pass phrase or PIN. It enables the holder of an <i>electronic identifier</i> to confirm that s/he is the person to whom the identifier was issued.
Service Provider	A campus or other organization that makes on-line resources available to users based in part on information about them that it receives from other InCommon participants.



Identity Assurance Assessment Framework

9 May 2011
Version 1.1

EXECUTIVE SUMMARY

The degree to which a Service Provider is willing to accept an Assertion of Identity from an Identity Provider may depend on how the Identity Provider Operator registers Subjects, issues Credentials, and manages the Identity information associated with Credentials. A set of requirements for these and possibly other aspects of Subject Identity that may be needed by Service Providers becomes an Identity Assurance Profile. Identity Provider Operators that meet the requirements of an Identity Assurance Profile can be certified as such by InCommon after passing a thorough assessment by a qualified independent party. Service Providers may choose to accept only Assertions of Identity that are offered by certified Identity Providers and include a particular Identity Assurance Qualifier.

This InCommon Identity Assurance Assessment Framework document describes the Identity assurance trust model that InCommon has adopted including a functional model for Identity Provider Operators and a certification model describing how certification is accomplished. It categorizes different aspects of Identity Credential and Subject information management and the methodology that must be used in performing an assessment of an Identity Provider Operator.

The functional model upon which the assurance framework is based is described and important terms are defined in section 2 of this document.

The structure of an InCommon Identity Assurance Profile is discussed in section 3.

Section 4 of this document describes the process by which Identity Provider Operators become certified by InCommon as compliant with any Identity Assurance Profile. It describes the assessment and audit process and the specific qualifications auditors must have in order to perform such assessments.

The assessment process results in an audit report to the Identity Provider Operator and a summary of findings report delivered to InCommon. InCommon then determines whether one or more Identity Assurance Qualifiers can be used by the Identity Provider Operator. Upon approval by InCommon, the Identity Provider may then include the appropriate Identity Assurance Qualifier(s) as part of its Assertions of Identity.

This document could be used by a Service Provider or any other relying party that wishes to understand the rationale for trustworthiness of the binding between an Identity Subject and his or her authentication Credentials or other information in Assertions of Identity it might receive that are specifically addressed by an Identity Assurance Profile. An InCommon Service Provider may choose to make use of the presence or absence of specific Identity Assurance Qualifier(s) in deciding whether to rely on Assertions of Identity it receives.

It is expected that as the Identity Assurance Assessment Framework is used and the number of assessments undertaken increases, this document will evolve and be extended to reflect experience gained and additional needs of the InCommon community.

TABLE OF CONTENTS

1 INTRODUCTION	1
1.1 RELATED DOCUMENTS	2
2 IDENTITY MANAGEMENT FUNCTIONAL MODEL	4
3 IDENTITY ASSURANCE PROFILES	8
3.1 STRUCTURE OF INCOMMON IDENTITY ASSURANCE PROFILES	8
3.1.1 <i>Business, Policy and Operational Criteria</i>	9
3.1.2 <i>Registration and Identity Proofing</i>	9
3.1.3 <i>Credential Technology</i>	9
3.1.4 <i>Credential Issuance and Management</i>	10
3.1.5 <i>Authentication Process</i>	10
3.1.6 <i>Identity Information Management</i>	11
3.1.7 <i>Assertion Content</i>	11
3.1.8 <i>Technical Environment</i>	11
4 ASSESSMENT AND AUDIT OF IDENTITY PROVIDERS.....	13
4.1 AUDITOR QUALIFICATIONS	13
4.2 AUDIT REPORT	14
4.2.1 <i>Conveyance to InCommon</i>	14
4.3 INCOMMON'S REVIEW AND ACTION	15
4.4 IDENTITY PROVIDER CERTIFICATION	15
4.5 CONTINUING IDPO COMPLIANCE.....	15
4.5.1 <i>Changes to IdPO Operations</i>	15
4.5.2 <i>Security Breach or Other IncidentS</i>	15
4.5.3 <i>Identity Provider Operator Suspension or Decertification</i>	15
APPENDIX A: REFERENCES.....	A-1
APPENDIX B: ACRONYMS	B-1
APPENDIX C: DEFINED TERMS	C-1
APPENDIX D: DOCUMENT HISTORY	D-1

1 INTRODUCTION

The InCommon Federation¹ for shared Identity and access management provides operational and trust enhancement services to both Identity Provider (IdP) Operators and Service Provider (SP) operators. Federation services increase efficiency by reducing redundant functions across Service Providers and by establishing common and consistent approaches to interoperable Identity management. InCommon has established Identity Assurance Profiles (IAPs) in order to further achieve this efficiency through structured requirements for trusted Identity intended to help mitigate risk for relying parties. This document defines the overall model and concepts upon which InCommon's Identity Assurance program is based. Other documents define the specific requirements for particular profiles.

There are at least three parties to any federated Identity transaction: the Identity Subject who uses an Identity Credential, the Identity Provider Operator who issues Credentials and maintains associated Identity information (see section 2 below), and the SP operator that uses Assertions of Identity to manage access to its services. The Identity Subject must trust the IdP Operator to operate in a manner that supports reliable Assertion of Identity on behalf of the Subject while preserving his or her privacy. The IdP Operator mitigates risk for the SP operator and the Subject by minimizing the likelihood that another person would be able to claim a Subject's Identity. The Subject and the IdP Operator trust the SP to use and protect appropriately Identity information it receives.

Assertions of Identity offered by certified InCommon Federation Identity Providers may be relied upon across a wide range of Service Providers because the InCommon Federation verifies adherence to community standards for Identity management and Assertion as described in this Identity Assurance Assessment Framework (IAAF).

The general structure of IAPs is described and processes involved in certifying an InCommon Federation IdP Operator are defined. Assertions of Identity must be supported by defined business and operational practices and Credential technologies. These criteria include requirements for the Identity-proofing of Subjects, digital Credential technologies, and management of Identity information used to make Assertions. Many of the specific criteria are based on technical and policy guidance developed by the National Institute of Standards and Technology (NIST)². They are intended to provide a structured means of defining assurances that should be meaningful to Service Providers that require a defined framework for trustworthiness of a Subject's Identity.

¹ See <http://www.incommon.org/>

² See <http://www.nist.gov/>

The degree to which an IdP Operator meets or exceeds requirements in these areas will determine which of the IAPs that IdP Operator is capable of supporting. Qualified IdP Operators can include the corresponding Identity Assurance Qualifier (IAQ) in Assertions of Identity that their IdP makes to SPs. SP operators that require assurance that an IdP can offer sufficiently trustworthy Assertions should understand this IAAF and accompanying profiles and then determine which InCommon IdP Operators have been certified as eligible to include the required IAQ. The SPs then can check that the Assertions received actually contain the required IAQ.

It is strongly recommended that SP operators use an industry accepted risk assessment methodology to assess potential risks associated with access to their online resources and then confirm that an IdP's certified IAQ(s) indicate conformance with an Identity assurance profile sufficient for the particular application. **The SP is solely responsible for determining whether a given profile is sufficient to mitigate any risks it might face as a result of relying upon Assertions conforming to that profile.**

Nothing in sections 1-3 of this document is normative. **Normative criteria to be used in an assessment process are expressed in separate Identity Assurance Profile documents.**

In order for an IdP Operator to be certified as compliant with an InCommon defined Identity Assurance Profile, the processes described in section 4 are mandatory unless specifically stated otherwise in an IAP.

1.1 RELATED DOCUMENTS

The reader should be familiar with the InCommon Federation Operating Policies and Practices [InC-FOPP] and the InCommon Federation Participation Agreement [InC-FPA]. Identity Assurance Profile documents [InC-IAP] refer to terms defined in this document.

The Federal Office of Management and Budget (OMB) "E-Authentication Guidance" [M-04-04] and NIST Special Publication "Electronic Authentication Guidelines" [SP 800-63] establish terminology and guidance for Identity assurance levels and the technical requirements for Identity Provider Operators that may offer Assertions of Identity to Federal agency applications. The InCommon Federation has adopted compatible terminology, guidance and requirements.

OMB M-04-04 defines the required level of Identity assurance in terms of the likely consequences of an Identity error. As the consequences of an Identity error become more serious, the required level of assurance increases. The OMB guidance provides Service Providers with example criteria for determining the level of authentication assurance required for specific applications and transactions, based on the risks and their likelihood of occurrence with each application or transaction.

NIST Special Publication 800-63-1 provides technical guidance to Federal agencies implementing electronic authentication. The recommendation covers remote authentication of users over open networks. It defines technical requirements for each of four hierarchical levels of assurance in the areas of Identity proofing, registration, Credentials, system

hardware, authentication protocols and related Assertions.

The federal government Identity, Credential, and Access Management (ICAM) program has articulated requirements for IdPs that wish to interoperate with Federal agency applications. These requirements, documented in the Trust Framework Provider Adoption Process (TFPAP), are based on the above documents but also include requirements for privacy and protection of Subject information and for qualification of auditors assessing an IdP Operator. [F-ICAM]

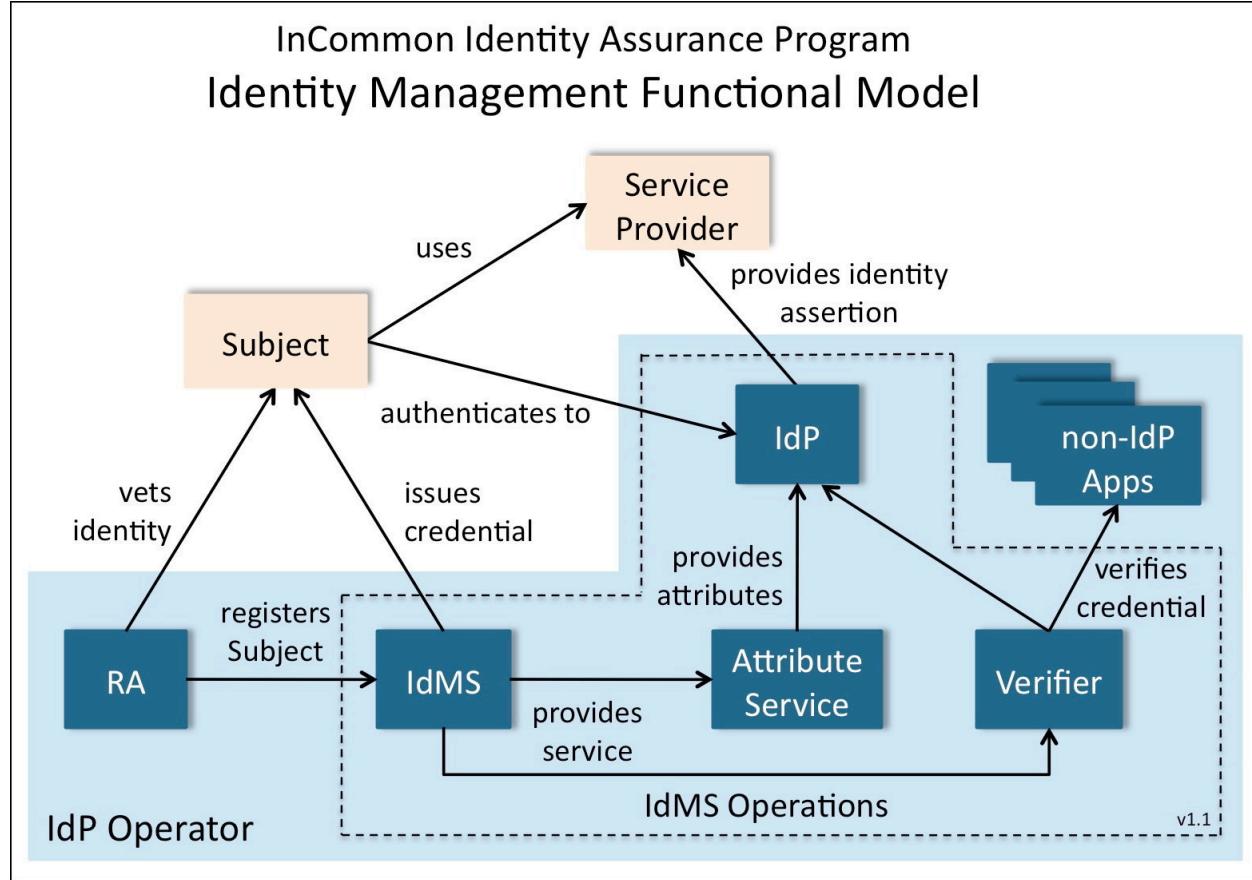
These documents may be considered prerequisite reading for this IAAF document; it is assumed the reader is familiar with the concepts they establish.

The specific criteria used to assess IdP Operators are grouped into Identity Assurance Profiles, the structure of which is described in Section 3.

The InCommon Federation Identity Assurance document suite is available on the InCommon website at <http://www.incommon.org/assurance/>

2 IDENTITY MANAGEMENT FUNCTIONAL MODEL

This section presents a model for the components involved in the Identity management (IdM) practice of an organization operating an Identity Provider (IdP). Identity Assurance Profiles (IAPs) state requirements for the operation of these components. This IdM model is not the only way to organize the functions of an Identity management system, but serves as a reference for the description of assurance requirements, and to identify which components are in scope for such requirements.



Identity, as used in InCommon documents, refers to the set of information that pertains to a Subject. This includes identifiers, memberships, eligibility, roles, names, characteristics, etc. In an Assertion of Identity, these elements are referred to as *Attributes* or *Identity Attributes*.

The organization operating an IdP is an *IdP Operator* (IdPO). The term IdP Operator refers to the legal entity that signs contracts, is a registered participant in InCommon, and is responsible for the overall processes supporting the IdP. Thus, for example, for a university IdP it is the university that is the IdPO, not the internal organization that provides the service. It is the IdPO that is responsible for the service operating in compliance with an IAP regardless of how or where they are implemented, including outsourced or delegated arrangements.

The IdPO is responsible for ensuring IAP conformance by the elements in the shaded area

in the diagram above. The elements within the dashed boundary constitute Identity Management System Operations which includes the IdMS itself and related components.

The *IdP* is the system component that issues Assertions on behalf of Subjects (also known as users) who use them to access the services of *Service Providers* (SPs) (also known as *Relying Parties* or RPs). *Assertions* (sometimes called Identity Assertions) are structured data objects containing information about Subjects and other data useful for authentication and access, and are digitally signed by the issuer (the IdP). These Assertions are validated and consumed by SPs and the information in them is used by SPs for access control, personalization, and other purposes. The IdP also may include an *Attribute Service* that provides Subject Attributes in response to queries from SPs.

To do its job, the IdP relies on a number of other system components, such as Credential verifiers and Subject registration processes. If the IdPO is an organization offering only IdP services, these components are likely to be dedicated solely to supporting the IdMS operation. In an enterprise setting, the IdP is typically only one component in a set of Identity management services that support many enterprise functions. For example, a password verifier used by the IdP may also be used by other enterprise systems that need to verify passwords. Since this enterprise scenario is typical of InCommon participant organizations, and it is more complex than the dedicated-IdP scenario, this model focuses on the enterprise scenario.

A *Subject* is a person who is (or will be) registered with the IdPO, and has obtained (or will obtain) a Credential for use with the IdP. *Registration* is the process of creating a record of the Subject's identifying information. Registration typically includes Identity proofing, which is a process that involves checking the validity of Identity documents and ensuring that they apply to the Subject. In the enterprise setting, registration is sometimes done as part of general business processes such as hiring of employees and enrollment of students, in which case registration records are maintained in business systems, e.g., Human Resources (HR) and Student Information System (SIS), supporting these functions. Registration is performed by a *Registration Authority* (RA). In an enterprise there may be many RAs with many different registration processes.

An *Address of Record* for the Subject provides a means of contacting the Subject. The Address of Record could be a postal mail address, an e-mail address, a telephone number (fixed or mobile) or similar mechanism by which the Subject can receive communications from the IdPO.

Enterprise Identity and access management needs typically are met by a set of functions called an *Identity Management System* (IdMS). An IdMS includes a database of Subjects (an *IdMS database*) with information about people and other entities gathered from other enterprise databases such as HR and SIS. The IdMS database stores identifiers for Subjects, some provided by source systems and others created, managed and provided by the IdMS.

The IdMS database also stores Credentials for Subjects. A *Credential* is a unique identifier and associated authentication material used by the Subject to authenticate to the IdP. A UserID/password pair is the most common form of Credential; a public-key certificate and

associated private key is another form. A Credential also may be issued to a Subject on a hardware device, e.g., a smartcard. A Subject may have more than one Credential bound to his or her record in an IdMS. Each Credential is associated with exactly one Subject record.

The term *Authentication Secret* is used generically for passwords, passphrases, PINs, symmetric keys and other forms of secrets used for authentication. An Authentication Secret may also be generated by a *Token*, which is a physical device (or specialized software on a device such as a mobile phone) used in authentication. Authentication Secrets are vulnerable to guessing attacks, so resistance to guessing is an important IAP requirement. Requirements for protection of Secrets in transit and storage also may be needed.

Credential issuance is a key step in enabling Subjects to authenticate securely. Credential issuance may happen as part of the registration process, or may happen separately. Issuance involves creating the Credential such that it is bound to the Subject's IdMS record, and such that the Authentication Secret (or other authentication material) is available to the Subject and only to the Subject. As with registration, in an enterprise there are likely to be many Credential issuance processes.

As part of the authentication process, the IdP often uses a *Verifier* to validate the correctness of offered authentication material, for example a userID and password. Often this Verifier also serves applications other than the IdP. As such the characteristics of those other systems and their use of the Verifier may also be in scope for IAP requirements. A Verifier generally does its work via access to a *Credential Store* which contains Authentication Secrets for all Subjects. The Credential Store may be part of the IdMS database, or be provisioned from it. Proper protection of this store is particularly important in the overall security of the IdMS. In some enterprise scenarios the Credential Store, or a portion of it, is copied into different systems to support different authentication technologies or vendor platforms. In this case all Credential Store locations are likely to be subject to IAP requirements.

The Subject uses a *User Agent* (typically a web browser) to authenticate to the IdP and convey the Assertion to the SP. The authentication method used between the User Agent and the IdP, including protection of Authentication Secrets in transmission and storage, may be subject to IAP requirements. The protocol used between the IdP and the SP (via the User Agent) is also in scope for IAP requirements, as it should resist various attacks and support SP needs for assured Subject Identity.

Assertions sent by the IdP often contain more than one Identity Attribute relevant to the Subject (Identity Attributes may also be provided to SPs separately via an Attribute Service). The IdP may obtain these Identity Attributes directly from the IdMS database, from an attribute-specific service (such as an LDAP directory) provisioned from the IdMS, or from other sources. Since Identity Attributes may be used by SPs for security purposes the integrity of Attribute sources may be in scope for IAPs. InCommon recommends several defined Attributes for use by its participants.³

³ See <http://www.incommon.org/attributessummary.html>

IdMS Operations refers to the technical environment and operating procedures supporting the IdMS. Since secure operation of the IdMS is critical to the effective assurance of the IdP, IAPs typically place constraints on technical measures and/or personnel used in IdMS Operations that may or may not apply to other enterprise systems.

The security of communications between system components (IdP, IdMS, Verifier, etc.) is important. A *Protected Channel* uses industry-standard cryptographic methods to provide integrity and confidentiality protection, resistance to replay and man-in-the-middle attacks, and mutual authentication. For example, SSL/TLS provides these protections.

A particular IdMS and IdP may support several different IAPs. They also may contain records and include processes that aren't in scope or don't meet the requirements of any IAP. As long as the factors related to a particular Subject (registration, issuance, authentication, etc.) meet the requirements of an IAP, Assertions about that Subject may include the IAQ for that IAP.

3 IDENTITY ASSURANCE PROFILES

An InCommon Identity Assurance Profile (IAP) specifies a set of criteria that, if met or exceeded by an IdPO, provide a useful metric by which an SP might determine whether Assertions of Identity conforming to those criteria can be used to help manage access to its service(s). InCommon defines IAPs in response to the well-articulated requirements of a community of interested SPs and IdPs. It is intended that the number of different profiles be minimized by making each one applicable to the broadest possible number of SPs.

Sufficient assurance of an Identity may involve many factors including registration of a Subject in an IdMS, the type of digital Credential provided to the Subject, the management of Identity information about the Subject, and the security of the processes used to provide an Assertion. Identity Assurance Profiles reflect industry and/or government consensus regarding requirements and best practices in each relevant area and may change or evolve over time.

InCommon IAPs are not necessarily hierarchical in nature. They represent particular sets of Identity management practices and requirements intended to address different use cases. An IdPO might support any number of IAPs and not all Subject records in a given IdMS need meet the requirements of all supported IAPs. In some cases, an IdPO conforming with a given IAP thereby also may conform with another, less stringent IAP and thus could apply for both certifications. An IdPO qualifying for InCommon Silver may be able to qualify readily for InCommon Bronze. An IdP may include in Assertions only those IAQs for which it has been certified and then only if all requirements for that IAQ have been met for the Subject of that Assertion.

InCommon IdP Operators are not required to qualify under any of the defined IAPs. InCommon IdP Operators are required only to self-describe their Identity management practices and make that statement available to InCommon SPs.⁴ There is no InCommon Identity Assurance Qualifier (IAQ) for Assertions provided solely on the basis of this self-described profile.

It is a responsibility of the IdPO, as defined in the Identity Assurance Addendum to the InCommon Participation Agreement, to never knowingly include an IAQ in an Assertion that has not been assigned to it by InCommon and to ensure that any IAQ that is included is appropriate for the particular Subject Assertion being offered.

3.1 STRUCTURE OF INCOMMON IDENTITY ASSURANCE PROFILES

InCommon IAPs aggregate Identity assurance criteria into eight categories, each of which addresses related issues pertaining to an aspect of ensuring that an Assertion of Identity is valid and correctly associated with a given Subject. Criteria to address issues in each category are defined in each IAP if relevant. An IAP also might cover requirements on out-sourced or shared components of an IdPO's operations. If no criteria are needed in a category, the IAP will state that. Additional types of issues may be covered as needed.

⁴ InCommon Participant Operational Practices requirements: <http://www.incommon.org/policies.html>

3.1.1 BUSINESS, POLICY AND OPERATIONAL CRITERIA

An IAP might address the nature of the organization supporting the IdPO and its ability to provide a trustworthy and reliable IdP service. For example, it might be necessary for an IdPO to be a legal entity, or a function of a larger organization that is a legal entity, in order that it can enter into contracts with other legal entities and accept liability for its actions. It might be required to demonstrate adequate resources and infrastructure to support the services it offers.

3.1.2 REGISTRATION AND IDENTITY PROOFING

Identity proofing is the process by which an IdPO or its designated Registration Authority (RA) or Registration Authorities associate a particular physical person with an existing Identity information record in the IdPO's IdMS database, or obtains and verifies the personal information required to create a new record for that physical person. Typically the Subject will be required to provide one or more authoritative documents or references from trusted sources of authority in order to ensure a reliable IdMS database record for that Subject. If the IdPO is a function of a larger organization, then Identity Subjects that are associated with that organization (e.g., employees and/or students) may have undergone some or all of the required Identity proofing during the process of bringing each person into the larger organization. It also might be possible to make a case for the comparability of long-term relationships where, for example, the organization has successful personnel experience with an employee over a number of years, financial information has been submitted successfully to the employee's bank or the IRS, etc.

During Identity proofing, sufficient information may be required to enable the IdPO to contact the Subject or, for some profiles, locate the Subject if necessary. An IAP might require that the Address of Record be verified, e.g., as part of Registration or Credential issuance. If a specific type of address is required in an IAP, e.g., residence or postal mail, this must be distinguished explicitly in the IAP.

Some profiles may require a record of the Identity proofing steps taken and/or authoritative documents presented by the Subject be retained as well, for example to show proof of process or to aid in re-establishing an Identity association at a future time.

3.1.3 CREDENTIAL TECHNOLOGY

A digital electronic Credential is the means by which an Identity Subject authenticates to an IdP Verifier. The "strength" of this Credential – its resistance to third party use, spoofing or discovering the Credential Authentication Secret – is a primary factor in determining the trustworthiness of the binding between a user of the Credential and the IdMS record for its Subject.

For shared secret Credentials, e.g., userID/password, the IAP might address how the Authentication Secret must be sufficiently difficult for a person other than the Subject to determine through trial and error, or other means and must be protected from illicit capture or replay. For physical token-based Credentials, the IAP might address how the Credential must be resistant to misuse if lost or stolen. The NIST document [SP 800-63] provides guidance on the strength of various digital electronic Credential technologies.

In some cases a given Subject may have more than one Credential to accommodate different authentication scenarios or a Subject might have several Credentials of different types. In this case the IAP might require that an IAQ in an Assertion be different depending on which Credential was used. Other factors might be significant such as location of the Subject (e.g., on the campus network or on some remote network). Thus Assertions on behalf of each Subject might fall under different profiles depending on the type of Credential that was used and other factors. Similarly, if the IdPO is aware of a possible compromise of a Subject's Credential, an IAP might require that an Assertion contain a different IAQ or no IAQ, or that the IdPO suspend or invalidate the Credential for the purpose of Assertions until the concern is resolved.

Real-time re-authentication of the Subject by the IdP's Verifier might be required by some SPs if the current authentication event occurred too long in the past.⁵ With some Credentials, e.g., smartcards, the IAP might require a built-in timeout in the Subject's device. If such re-authentication capability is required by an IAP, it may limit the types of Credentials that can be supported by the IdPO.

3.1.4 CREDENTIAL ISSUANCE AND MANAGEMENT

Creating and conveying a Credential to a Subject is a critical process that may be vulnerable in various ways. An IAP might define requirements to ensure that the Subject actually receives the Credential, has control of the Authentication Secret, and that no other person might acquire the Authentication Secret during the process. The IAP also might address Credential reissuance and/or revocation.

It is important to note that registration, Identity proofing, and Credential issuance represent different aspects of the same process. In many cases, however, this process may be broken up into a number of separate physical encounters and electronic transactions. An IAP might require that in these cases methods be used to ensure that the same party acts as Subject throughout the entire process.

3.1.5 AUTHENTICATION PROCESS

An authentication event occurs when a Subject offers his or her Credential to an IdP's Verifier. The Verifier interacts with the Subject to confirm he or she is the rightful physical person associated with the Credential and that the Credential is still valid. An IAP might define requirements to ensure this transaction is secure against interception or exposure of any Authentication Secret to any unauthorized party. The time, date, and nature of the authentication event may need to be recorded and the record retained for a reasonable period of time to aid in problem resolution or forensic analysis. Information about the most recent authentication event for a Subject, for example when it occurred, might be required as part of an Assertion.

Some SPs may wish to request reconfirmation of authentication where, in their judgment, the most recent event occurred too long in the past and they wish to confirm that the identified Subject is still in control of the current session. If this capability is required of

⁵ See also section 3.1.5.

the IdP, the IAP should address what constitutes sufficient reconfirmation.

3.1.6 IDENTITY INFORMATION MANAGEMENT

Assertions offered by the IdP to an SP will be based on information about or pertaining to the Subject, e.g., “name” or “unique identifier,” obtained from reliable sources and held in an IdMS. Management of the IdMS database that stores this information is critical to the degree of assurance that an Assertion might carry. An IAP might include requirements about the sources of Identity information, how it is obtained, and how information is maintained and updated when needed.

Identifiers generated for an IdPO’s Subjects may be used by SPs to manage access. An IAP might address whether a given Subject may have any number of identifiers and whether a given identifier will map only to one specific Subject. IAPs may need to include requirements regarding the uniqueness or persistence of Subject identifiers, e.g., the length of time an assigned identifier is required to be bound to a given Subject or whether an identifier may be reassigned to a different Subject and, if so, whether there must be a period of time before reassignment.

Actions that affect the integrity or contents of the IdMS database may need to be logged securely and in a manner that is resistant to tampering. An IAP might place corresponding requirements on IdMS Operations, e.g., to aid in problem resolution or forensic analysis.

3.1.7 ASSERTION CONTENT

Assertions contain Identity information Attributes in structured, named information objects that refer to or pertain to the Identity Subject. Identity Attributes recommended for use by all InCommon IdPs and SPs are described on the InCommon Federation Attribute Summary [InC-AtSum].

An IAP might address what Attributes IdPs should convey to SPs and whether Subjects should be able to determine what Attributes, if any, will be conveyed to SPs. Real-time Subject consent processes may be used to control the release of personally identifiable information (PII) from the IdP to the SP. Alternatively, an IdPO might be required to obtain prior approval for release of certain PII.

IAPs might include provisions to address the required authoritativeness of some or all information conveyed in Assertions.

3.1.8 TECHNICAL ENVIRONMENT

An IAP may need to address security of the physical, technical and network environment and the adequacy of controls and procedures in place for all critical components of the IdPO’s IdMS(s). All personnel with access to critical systems might be required to have Credentials as least as robust as the strongest Credentials that will be issued by those systems. To the extent possible, the IdPO’s system architecture may need to be resistant to denial of service attacks.

An IAP might address how operating software on all service platforms involved in the IdP

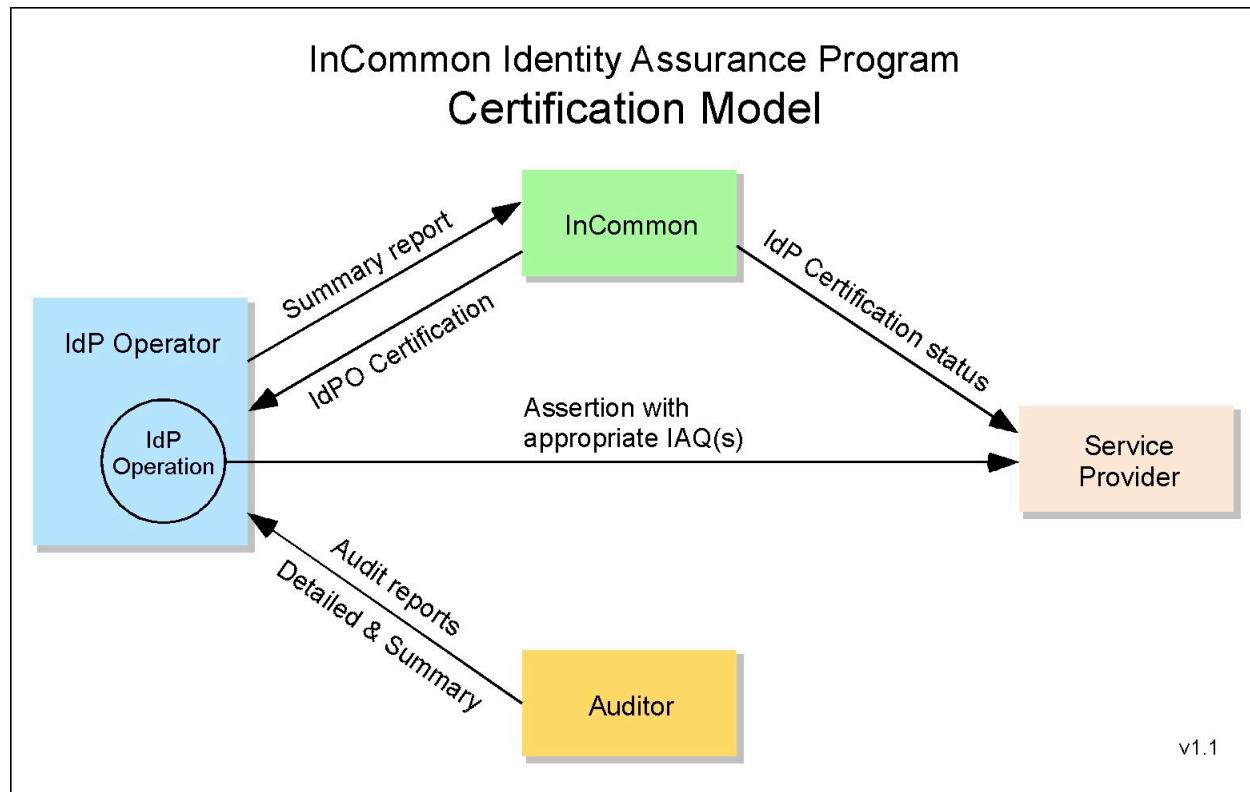
Operations, including registration, IdMS and Attribute Service databases, and Assertion processing, should be kept up to date and security-related software patches installed promptly.

An IAP also might address how IdPOs should participate in problem resolution with SPs. It might be important to define requirements for reporting on and/or participating in response to breach of security or similar incidents.

An IAP might address how IdPOs provide for continuity of Identity verification and Assertion services in case of system failures or natural disasters. For example, by requiring that system designs guard against erroneous Assertions or false positive authentication in cases of partial system failure, minimizing single points of failure, providing backup or stand-by service platforms, or replicating critical data to off-site locations.

4 ASSESSMENT AND AUDIT OF IDENTITY PROVIDERS

InCommon IdP Operators that wish to assert conformance to a specific InCommon IAP are required to undertake initial assessment and then arrange for an independent audit of that assessment, and, for some IAPs, periodic reassessment and audit of the controls for its IdMS Operations. InCommon does not perform such assessments or audits. The IdP Operator initiates the process and engages the Auditor. The Auditor reports to the IdPO and creates the summary report required by InCommon. The IdPO will convey the summary report to InCommon along with any other materials required by InCommon. InCommon makes the final determination regarding conformance.



The IdMS Operation must be fully operational and supported by the organization at the time of assessment. An IdPO may support several IdMS Operations but only those assessed and certified by InCommon may assert InCommon IAQs.

4.1 AUDITOR QUALIFICATIONS

The Auditor may be either an external contractor or may be a member of an internal audit office within the IdPO's organization. The Auditor doing the review must be objective and independent, following guidelines established by professional audit organizations such as The Institute of Internal Auditors "Standards for the Professional Practice of Internal Auditing".⁶

⁶ <http://www.theiia.org/guidance/standards-and-guidance/ippf/standards/>

The Auditor shall possess adequate technical proficiency and industry knowledge for the specific assessment being performed. The Auditor must have demonstrated qualification to make competent determination of the IdPO's compliance with applicable IAP criteria, taking into account technical issues and specific requirements that the criteria might set out (e.g., specific management processes). The Auditor shall have, as a minimum:

- Understanding of the IdPO's industry and services;
- General knowledge of the technologies/techniques being assessed;
- Technical and management audit experience;
- Familiarity with the applicable IAP(s); and
- Familiarity with this IAAF.

To audit an IdP Operator, the Auditor must have current direct experience as an information technology auditor and perform audits regularly in a professional capacity. Demonstrated qualification, such as designation as a Certified Information System Auditor⁷ (CISA) or equivalent knowledge and experience, is required.

4.2 AUDIT REPORT

The Auditor must prepare a written audit report to document the approach, findings, and recommendations regarding compliance of the IdPO with specific IAP(s). The audit report shall identify the Auditor, its basis for independence with respect to the IdPO and the dates during which the audit took place. An audit report must include:

- *Assessment Objective.* The Auditor must identify the IdP Operator and the IAP(s) that the IdPO intends to support;
- *Scope and Methodology.* The scope of the review should be driven by the IdPO management's compliance assertions and include sufficient tests of controls identified in the InCommon IAP to render an appropriate opinion; and
- *Findings.* The Auditor must report the IdPO's compliance with each of the criteria contained in the relevant IAP(s). For each criterion, the Auditor should identify the evidence provided, the rationale for acceptance or rejection, and any identified deficiencies. If significant vulnerabilities are found, e.g., in security or operational controls, these should be discussed with the IdPO.
- *Comparable Alternatives.* Alternatives to procedures or requirements specified in the IAP must be documented in the Auditor's report to the IdPO and be made available to InCommon. Documentation should include the IdPO's rationale for such alternatives.

4.2.1 CONVEYANCE TO INCOMMON

The Auditor must prepare and sign a summary report to be conveyed to InCommon summarizing the final assessment results. The letter must at a minimum:

- Identify the Auditor, including qualifications;

⁷ See Information Systems Audit and Control Association <http://www.isaca.org/>

- Outline the audit methodology;
- Identify any alternatives to specific IAP requirements that the IdPO has chosen; and
- State whether the IdPO conforms with all other requirements of each IAP examined.

All audit summary reports and attachments will be kept in strict confidence by InCommon.

4.3 INCOMMON'S REVIEW AND ACTION

InCommon will review the Auditor's summary report and consider the impact of any alternatives noted in the IdP Operator's assessment. If the nature of the alternatives appear minor and would have little negative impact on the IdPO's Identity assurance, InCommon may choose to accept them. In some cases it may be necessary to work with the IdPO to understand the rationale for an alternative. If significant negative impact on the assurance of Identity in Assertions is found, InCommon will require the IdPO to correct them. When corrected, the IdPO must have the Auditor review the correction and submit an updated summary report to the IdPO to be conveyed to InCommon.

4.4 IDENTITY PROVIDER CERTIFICATION

Once the audit results are accepted by InCommon, the IdP Operator is certified by InCommon to assert one or more IAQs. InCommon will place the IAQ(s) in the IdP metadata describing the IdP. SPs and other relying parties are expected to acquire this information as part of an InCommon participant metadata refresh cycle.

4.5 CONTINUING IDPO COMPLIANCE

Once the IdP Operator is certified by InCommon to be compliant with one or more IAPs, periodic reassessments may be required. If so, this will be specified in the relevant IAP(s). For some IAPs, self-reassessment or a declaration of changes to the IdP Operation may be sufficient. If a complete re-assessment is required, then the auditor qualifications and reporting requirements above apply.

4.5.1 CHANGES TO IDPO OPERATIONS

When changes to an IdPO's operation are reported, InCommon will determine whether the changes are sufficient to require reassessment. Any change-driven reassessment would only need to cover those elements that have changed.

4.5.2 SECURITY BREACH OR OTHER INCIDENTS

When security related breaches or other service related incidents that might impact compliance with an IAP are reported to InCommon, InCommon will work with the IdPO to determine an appropriate remediation of such incidents.

4.5.3 IDENTITY PROVIDER OPERATOR SUSPENSION OR DECERTIFICATION

If deficiencies in the IdP Operations are reported to InCommon by the IdPO, or reported by an affected party and confirmed by InCommon, InCommon will allow the IdPO a reasonable period of time to correct any such deficiencies. Failure of the IdPO to provide

required reports is considered a deficiency in this context. The length of the grace period will depend on the severity of the deficiency with respect to its impact on the assurance of Assertions made by the IdP. If the deficiency is deemed by InCommon to have significant impact, the IdPO may be required to suspend the use of the IAQ in Assertions it makes and this will be reflected in metadata for the affected IdP. This suspension will be lifted upon receipt of a statement from the IdPO and satisfactory to InCommon that the deficiency has been corrected.

If the deficiencies are not corrected during the grace period, the IdPO's certification for use of the relevant IAQ may be revoked. Conditions for re-certification will be defined by InCommon on a case by case basis.

APPENDIX A: REFERENCES

- [M-04-04] “**E-Authentication Guidance for Federal Agencies**”, Federal OMB, Dec 2003,
<http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>
- [SP 800-63] “**Electronic Authentication Guidelines**”, NIST, Special Publication 800-63-1
<http://csrc.nist.gov/publications/PubsSPs.html>
- [InC-AtSum] “**InCommon Federation Attribute Summary**”, InCommon Federation,
<http://www.incommon.org/attributesummary.html>
- [InC-FOPP] “**Federation Operating Policies and Practices**”, InCommon Federation,
<http://www.incommon.org/policies.html>
- [InC-FPA] “**Participation Agreement**”, InCommon Federation,
<http://www.incommon.org/policies.html>
- [InC-IAP] InCommon Federation Identity assurance profiles,
<http://www.incommon.org/assurance/>
- [F-ICAM] **Identity, Credential, and Access Management**, Federal government
<http://www.idmanagement.gov/>

APPENDIX B: ACRONYMS

Acronym	Definition
CISA	Certified Information Systems Auditor
FOPP	Federation Operating Policies and Practices
HR	Human Resources
IAAF	Identity Assurance Assessment Framework
IAP	Identity Assurance Profile
IAQ	Identity Assurance Qualifier
ICAM	Identity, Credential, and Access Management
IdM	Identity Management
IdMS	Identity Management System
IdP	Identity Provider
IdPO	IdP Operator
IT	Information Technology
NIST	National Institute of Standards and Technology
OMB	Office Of Management And Budget (US Federal government)
PIN	Personal Identification Number
RA	Registration Authority
SIS	Student Information System
SP	Service Provider
TFPAP	Trust Framework Provider Adoption Process

APPENDIX C: DEFINED TERMS

Certain terms are defined in this document and must be used consistently in all Identity Assurance Profiles that reference this document. Full definitions are contained in the text of this document on the page indicated. Brief descriptions are listed here for convenience.

Defined Term	Page	Brief summary description
<i>Address of Record</i>	p5	A means of contacting the Subject.
<i>Assertion</i>	p5	Structured data objects containing Identity information and other relevant data. Sometimes called Identity Assertions.
<i>Attributes</i>	p4	Elements of an Identity.
<i>Attribute Service</i>	p5	Provides Subject Attributes in response to queries from SPs.
<i>Authentication Secret</i>	p6	Used generically for passwords, passphrases, PINs, symmetric keys and other forms of secrets used for authentication
<i>Credential</i>	p5	A unique identifier and authentication material.
<i>Credential Store</i>	p6	Contains Authentication Secrets for all Subjects
<i>Identity</i>	p4	Information that is true about a Subject.
<i>Identity Attributes</i>	p4	Information elements relevant to a Subject.
<i>Identity Management System</i>	p5	A set of functions serving the Identity and access management needs of an enterprise.
<i>Identity Provider</i>	p5	The IdMS system component that issues Assertions.
<i>IdMS database</i>	p5	A database of IdMS Subjects.
<i>IdMS Operations</i>	p7	The technical environment supporting the IdMS.
<i>IdP Operator</i>	p4	The organization operating an IdP is an <i>IdP Operator</i> .
<i>Protected Channel</i>	p7	A communication mechanism that provides message integrity and confidentiality protection.
<i>Registration</i>	p5	The process of creating a record of a Subject's Identity information.
<i>Registration Authority</i>	p5	A trusted entity entitled to perform Registrations.
<i>Relying Parties</i>	p5	A synonym for Service Provider.
<i>Service Provider</i>	p5	Uses an Identity Assertion as part of managing access to its services.
<i>Subject</i>	p5	A person who is (or will be) registered with the IdP Operator
<i>Token</i>	p6	A physical device (or specialized software on a device such as a mobile phone) used in authentication.
<i>User Agent</i>	p6	Typically a web browser, used by the Subject to authenticate to the IdP and convey the assertion to the SP.
<i>Verifier</i>	p6	Validates the correctness of offered authentication material.

APPENDIX D: DOCUMENT HISTORY

This document was developed by the InCommon Federation Technical Advisory Committee with significant contributions from other experts and reviewers.

<http://www.incommon.org/about.html>

EDITORS

RL "Bob" Morgan	Tom Barton	John Krienke
Jim Basney	David Walker	Renee Shuey
Steven Carmody	Peter Alterman	Karl Heins
		David Wasley

Status	Release	Date	Comment	Audience
Public	1.0	4 Nov 2008	First full release for implementation	Open
Draft	1.0.2	24 Mar 2010	Revisions to align with ICAM TFPAP	Open
Public	1.0.3	22 Apr 2010	Added to Glossary "FIPS" under "Approved"	Open
Draft	1.0.4	10 Jun 2010	Modified 3.1 to satisfy ICAM	Open
Draft	1.1D1	18 Dec 2010	Greatly modified to remove unnecessary elements and clarify remaining elements	Limited
Draft	1.1D4	21 Jan 2011	Further significant mods based on IdP Functional Model	Limited
Draft	1.1PRD1	9 Mar 2011	Revised from feedback and ready for larger review	Public
Draft	1.1FD1	9 Apr 2011	Revised from wider review; checked for consistency, etc.	Limited
Draft	1.1FD2	15 Apr 2011	Final revisions prior to SC review	Limited
FINAL	1.1	9 May 2011	Approved by InCommon Steering Committee	Public



0100PT

Identity Assurance Profiles Bronze and Silver

9 May 2011
Version 1.1

EXECUTIVE SUMMARY

Identity Assurance Profiles, as described in the InCommon Identity Assurance Assessment Framework, define the specific requirements that Identity Provider Operators must meet in order to be eligible to include InCommon Identity Assurance Qualifier(s) in identity Assertions that they offer to Service Providers. The reader is assumed to be familiar with the InCommon Identity Assurance Assessment Framework.

This document defines requirements for InCommon Silver and Bronze identity assurance certification. These profiles are intended to be compatible with the US federal government ICAM Trust Framework Provider Adoption Process, Levels of Assurance 1 and 2. The requirements are directly applicable to Identity Provider Operators that use Authentication Secret-based Credentials, but equivalent or stronger Credentials could be used instead.

InCommon Bronze certification requires that an Identity Provider Operator support at least basic authentication Credentials with moderately hard to guess Authentication Secrets. Assertions may include a unique identifier for each Subject registered in the Identity Provider Operator's Identity Management System that should be usable in access control lists, but further identity information need not be included or verified. InCommon Silver certification requires Credentials with hard to guess Authentication Secrets and better Credential management, reasonably well verified personal information about each Subject, unique Subject identifiers, and secure business and operational processes.

An Identity Provider Operator that is certified under the Silver profile also may wish to be certified to use the Bronze Identity Assurance Qualifier, for example, for Assertions that do not fully meet Silver requirements but do meet Bronze requirements. Identity Provider Operators that meet or exceed either of these qualifications are identified as certified in the InCommon Identity Provider metadata and may include the appropriate Identity Assertion Qualifier(s) in Assertions they provide.

TABLE OF CONTENTS

1	INTRODUCTION	1
2	SCOPE	1
3	SILVER AND BRONZE PROFILES	2
3.1	INCOMMON BRONZE IDENTITY ASSURANCE PROFILE.....	2
3.2	INCOMMON SILVER IDENTITY ASSURANCE PROFILE	2
4	CRITERIA	3
4.1	SUMMARY OF IDENTITY ASSURANCE CRITERIA.....	3
4.2	SPECIFICATION OF IDENTITY ASSURANCE REQUIREMENTS	5
4.2.1	<i>Business, Policy and Operational Criteria.....</i>	5
4.2.2	<i>Registration and Identity Proofing</i>	5
4.2.3	<i>Credential Technology.....</i>	7
4.2.4	<i>Credential Issuance and Management</i>	9
4.2.5	<i>Authentication Process</i>	10
4.2.6	<i>Identity Information Management.....</i>	11
4.2.7	<i>Assertion Content.....</i>	11
4.2.8	<i>Technical Environment.....</i>	11
	APPENDIX A: REFERENCES.....	A-1
	APPENDIX B: ACRONYMS	B-1
	APPENDIX C: DOCUMENT HISTORY	C-1

1 INTRODUCTION

This document is part of InCommon's Identity Assurance Program. Please refer to the InCommon Identity Assurance Assessment Framework (IAAF) for an overview and for information on how InCommon certifies that an IdP Operator (IdPO) satisfies the requirements of this Identity Assurance Profile (IAP). Additional information can be found at <http://www.incommon.org>

Certain terms used in this document refer to elements of the InCommon identity management functional model as defined in the InCommon IAAF, Section 2. Such terms are capitalized in this document.

2 SCOPE

This IAP document contains requirements that IdPOs must satisfy if they wish to qualify for InCommon Silver or Bronze assurance designation. These requirements apply specifically to IdPOs that authenticate Subjects directly using credentials that the IdPO issues and then provide Assertions of Identity tailored to the needs of cooperating Service Providers (SPs). This IAP applies only for Subjects that are natural persons.¹

The IAP includes issues regarding the process for Subject registration with the IdPO's IdMS, the digital Credentials they are given, the handling of identity information about the Subject, and the Assertion conveyed to SPs. It is not required that all Subject records in a given IdMS meet the criteria in this or any IAP. However, the IdP must be able to determine which Subject records do meet all relevant criteria and include only the appropriate assurance qualifier(s) in Assertions it issues.

An IdPO issues to a Subject one or more digital Credential(s) with which to authenticate to that IdPO's IdP. This IAP addresses primarily Credentials based on an Authentication Secret used for authentication of the Subject to the IdP. Equivalent or stronger² forms of digital Credentials such as one-time Authentication Secret devices, PKI certificates or other secure technologies could satisfy the Credential requirements of these profiles as well.

If other types of digital Credentials are used, the Authentication Secret requirements of this IAP may not apply. In such cases the IdPO and its independent auditor must use professional judgment in determining whether the other type of Credentials meet or exceed the requirements in §4.2.3. Examples include:

- Authentication Secret-based systems that employ specialized client software for the Authentication Secret authentication protocol and access management to the SP;
- Systems that use Authentication Secrets in conjunction with Tokens or specialized software;
- Systems where PINs are used in conjunction with Tokens or specialized software.

The IdPO is responsible for ensuring conformance with the requirements and criteria defined in this IAP regardless of how or where they are implemented, including outsourced or delegated arrangements.

¹ See <http://www.nolo.com/dictionary/natural-person-term.html>

² See NIST [SP 800-63] for a discussion of Credential strength.

3 SILVER AND BRONZE PROFILES

This InCommon IAP document establishes requirements for IdPOs under two assurance profiles: Bronze, which represents a minimal formal set of requirements and Silver, which adds more stringent requirements. InCommon Bronze and Silver are intended to be compatible with US federal government Identity, Credential, and Access Management (ICAM) Trust Framework Provider Adoption Process (TFPAP) Levels of Assurance 1 and 2. They also include requirements regarding support for InCommon-recommended Identity Attributes.

InCommon Bronze requirements are fewer than InCommon Silver requirements. In some places these two IAPs have different requirements for the same criterion where the Bronze criterion is less stringent than that for Silver, for example, in the required Authentication Secret strength. Thus, an IdPO meeting the Silver requirement may be able to satisfy the Bronze requirement as well. InCommon Federation metadata will identify IdPs that are operated by InCommon-certified IdPOs and that meet or exceed the requirements of the Bronze IAP as qualified to assert the Bronze Identity Assurance Qualifier (IAQ) as part of Assertions and IdPs that meet the requirements of the Silver IAP as qualified to assert Silver IAQs, as appropriate, as part of Assertions. A given IdP may be certified to assert either or both IAQs as long as the appropriate IAQ is associated with each Assertion.

3.1 INCOMMON BRONZE IDENTITY ASSURANCE PROFILE

The InCommon Bronze identity assurance profile focuses on sequential identity, that is, reasonable assurance that the same person is authenticating each time with a particular Credential. Assertions under this profile are likely to represent the same Subject each time a Subject identifier is provided.

While no identity proofing requirements are specified, it is expected that IdPOs use reasonable care when issuing Credentials to confirm that a single individual applies for and receives a given Credential and its Authentication Secret.

InCommon Bronze qualified Assertions are typically usable by individuals seeking access to online information resources licensed to an organization and for which the Subject is an eligible user. They also may be usable for access to online services where the SP will invoke other methods for linking of the Subject identifier to information the SP already has regarding individuals who should have access to its services.

3.2 INCOMMON SILVER IDENTITY ASSURANCE PROFILE

The InCommon Silver identity assurance profile builds on the Bronze profile requirements by adding criteria regarding individual Subject identity proofing and identity information records. Stronger Credential technology and Credential management are required as well.

The Silver IAP intends to assure a reasonably strong binding between the physical Subject and that Subject's digital Credential, and reasonably accurate information in Assertions. Credentials must at a minimum make use of Authentication Secrets that are sufficiently difficult to guess or intercept.

4 CRITERIA

The criteria outlined below are organized by functional area, as discussed in the IAAF, and will be applied cumulatively as discussed in Section 2 of this document. These criteria apply to the IdPO and are not dependent on any particular implementation architecture.

4.1 SUMMARY OF IDENTITY ASSURANCE CRITERIA

This table summarizes all of the identity assurance criteria defined for Bronze and Silver IAPs. Cells that are shaded and contain “n/a” do not apply to the indicated profile.

Functional Area	Criteria	Bronze	Silver
4.2.1 Business, Policy and Operational Criteria	1. InCommon Participant.	●	●
	2. Notification to InCommon	●	●
	3. Continuing Compliance	●	●
4.2.2 Registration and Identity Proofing	.1 RA authentication	n/a	●
	.2 Identity verification process	n/a	●
	.3 Registration records	n/a	●
	.4 Identity proofing	n/a	●
	.4.1 Existing relationship	n/a	●
	.4.2 In-person proofing	n/a	●
	.4.3 Remote proofing	n/a	●
	5. Address of Record confirmation	n/a	●
4.2.3 Credential Technology	.1 Credential unique identifier	●	●
	.2 Resistance to guessing Authentication Secret	●	n/a
	.3 Strong resistance to guessing Authentication Secret	n/a	●
	.4 Stored Authentication Secrets	●	●
	.5 Protected Authentication Secrets	●	●
4.2.4 Credential Issuance and Management	.1 Credential issuance process	n/a	●
	.2 Credential revocation or expiration	n/a	●
	.3 Credential renewal or re-issuance	n/a	●
	.4 Retention of Credential issuance records	n/a	●

Functional Area	Criteria	Bronze	Silver
4.2.5 Authentication Process	.1 Resist replay attack	●	●
	.2 Resist eavesdropper attack	●	●
	.3 Secure communication	●	●
	.4 Proof of Possession	●	●
	.5 Session authentication	●	●
	.6 Mitigate risk of sharing Credentials	●	●
4.2.6 Identity Information Management	.1 Identity record qualification	●	●
4.2.7 Assertion Content	.1 Identity Attributes	●	●
	.2 Identity Assertion Qualifier	●	●
	.3 Cryptographic security	●	●
4.2.8 Technical Environment	.1 Software maintenance	n/a	●
	.2 Network security	n/a	●
	.3 Physical security	n/a	●
	.4 Reliable operations	n/a	●

4.2 SPECIFICATION OF IDENTITY ASSURANCE REQUIREMENTS

This section contains all of the normative language for the Bronze and Silver IAPs.

In the requirements that follow, ® indicates that the numbered section applies to the Bronze IAP; ® indicates that the numbered section applies to the Silver IAP.

4.2.1 BUSINESS, POLICY AND OPERATIONAL CRITERIA

IdP Operators must have the organizational structures and processes to come into and remain in compliance with the provisions of this IAP.

4.2.1.1 ®® INCOMMON PARTICIPANT

The IdPO must be an InCommon Participant in good standing in order to be considered for certification under this IAP. In this context, “good standing” means not in arrears with respect to financial obligations to InCommon nor out of compliance with other contractual obligations to InCommon.

4.2.1.2 ®® NOTIFICATION TO INCOMMON

The IdP Operator must notify InCommon of any circumstance that may affect the status of its compliance with this IAP.

1. The IdP Operator must notify InCommon of any significant changes to its operation that may affect the status of its compliance and hence its qualification under this IAP. Notification should occur no less than 30 days before the changes are to be made effective, or as soon as practicable after an unanticipated change is noted.
2. The IdPO must report to InCommon any breach of security or integrity of its IdMS Operations that may affect the status of its compliance and hence its qualification under this IAP. A report must be made as soon as practicable after any such incident is noted.

4.2.1.3 ®® CONTINUING COMPLIANCE

After initial certification by InCommon, IdP Operators must declare to InCommon continued compliance with profiles under this IAP at least every 3 years.

4.2.2 REGISTRATION AND IDENTITY PROOFING

Identity proofing in this IAP is based on government-issued ID or public records. Verified information is used to create a record for the Subject in the IdPO’s IdMS.

4.2.2.1 ® RA AUTHENTICATION

Each RA must authenticate to the IdMS using a credential that meets or exceeds Silver requirements.

Communications between an RA and the IdMS shall be encrypted using an industry standard protocol that also authenticates the IdMS platform.

4.2.2.2 ® IDENTITY VERIFICATION PROCESS

1. The identity proofing and registration process shall be performed according to written policy or practice statements that specify the particular steps taken by IdPO staff or systems to verify identities.
2. The above statement(s) shall address the primary objectives of registration and identity proofing, including:

- Ensuring a person with the claimed identity information does exist, and that the identity information is sufficient to uniquely identify a single person within the IdPO's range of foreseeable potential Subjects;
 - Ensuring that the physical person requesting registration is entitled to the claimed identity.
3. Personally identifiable information collected as part of the registration process must be protected from unauthorized disclosure or modification.

4.2.2.3 ⑤ REGISTRATION RECORDS

1. A record of the facts of registration shall be maintained by the IdPO.
2. The record of the facts of registration shall include:
 - Identity proofing document types and issuers;
 - Full name as shown on the documents;
 - Date of birth;
 - Current Address of Record.
3. Records also must include revocation or termination of registration.

4.2.2.4 ⑤ IDENTITY PROOFING

Prior to this process, the Subject supplies his or her full name, date of birth, and an Address of Record to be used for communication with the Subject, and may, subject to the policy of the IdPO, also supply other identifying information. For each Subject, the full name, date of birth and Address of Record must be verified using one or more of the following methods:

4.2.2.4.1 Existing relationship

If the IdPO is a function of an enterprise, the identity proofing process may be able to leverage a pre-existing relationship, e.g., the Subject is an employee or student. Where some or all of the identity proofing done at the time the existing relationship was established is comparable to that required in §4.2.2.4.2 or §4.2.2.4.3 below, those results may be relied upon for this purpose. The IdPO's Registration Authority (RA) shall confirm that the Subject is a person with a current relationship to the organization, record the nature of that relationship and verify that the relationship is in good standing with the organization.

4.2.2.4.2 In-Person proofing

1. The RA shall establish the Subject's IdMS registration identity based on possession of a valid current government photo ID that contains the Subject's picture (e.g., driver's license or passport), and either an address or nationality.
2. The RA inspects the photo ID and compares the image to the physical Subject. The RA records the document type and issuer, the address given on the ID if there is one, and the date of birth shown on the ID if there is one. If the ID appears valid, the photo matches the physical Subject, and the ID confirms the Subject's date of birth, the RA authorizes issuance of Credentials.
3. If the address given on the ID does not confirm the Address of Record, it must be confirmed as described in §4.2.2.5 below.

4.2.2.4.3 Remote proofing

1. The RA shall establish the Subject's IdMS registration identity based on possession of at least one valid government ID number (e.g., a driver's license or passport) and either a second government ID number or financial account number (e.g., checking account, savings account, loan or credit card) with confirmation via records of either number.
2. The RA verifies other information provided by the Subject using both of the ID numbers above through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, date of birth, and other personal information in records are on balance consistent with the application and sufficient to identify a unique individual. If this appears to be the case, the RA authorizes issuance of Credentials.
3. If the record checks do not confirm the Address of Record, it must be confirmed as described in §4.2.2.5 below.

4.2.2.5 ADDRESS OF RECORD CONFIRMATION

The Address of Record must be confirmed before the Subject's record can be considered to meet the requirements of this IAP. If the Address of Record was not confirmed as part of Identity proofing, then it must be accomplished by one of the following methods:

1. The RA contacts the Subject at the Address of Record and receives a reply from the Subject; or
2. The RA issues Credentials in a manner that confirms the Address of Record supplied by the Subject.
 - a. For a physical Address of Record, the RA requires the Subject to enter online a temporary Secret from a notice mailed to the Subject's Address of Record.
 - b. For an electronic Address of Record, the RA confirms the ability of the Subject to receive telephone communications at a telephone number or e-mail at an e-mail address.

Any Secret not sent over a Protected Channel shall be invalidated upon first use.

4.2.3 CREDENTIAL TECHNOLOGY

These InCommon IAPs are based on use of "shared Authentication Secret" forms of identity Credentials. If other Credentials are used to authenticate the Subject to the IdP, they must meet or exceed the effect of these requirements.

4.2.3.1 ⑧ ⑨ CREDENTIAL UNIQUE IDENTIFIER

1. Each Credential issued by the IdPO shall include a unique identifier (e.g., userID, Distinguished Name, serial number) that distinguishes it from all other Credentials in use by the IdPO.
2. A Subject can have more than one Credential unique identifier, but a given Credential unique identifier must map to at most one Subject.
3. The IdPO shall clearly associate the Credential unique identifier to the Subject's registration record in the IdMS, for use by the Verifier or other parties.

4.2.3.2 ⑧ RESISTANCE TO GUESSING AUTHENTICATION SECRET

The Authentication Secret and the controls used to limit online guessing attacks shall ensure that an attack targeted against a given Subject's Authentication Secret shall have a probability of success of less than 2^{-10} (1 chance in 1,024) over the life of the Authentication Secret. This requires that an Authentication Secret be of sufficient complexity and that the number of invalid attempts to enter an Authentication Secret for a Subject be limited.

Refer to NIST Special Publication 800-63-1 [SP 800-63], Appendix A, for a discussion of Authentication Secret complexity and resistance to online guessing.

4.2.3.3 ⑨ STRONG RESISTANCE TO GUESSING AUTHENTICATION SECRET

1. The Authentication Secret and the controls used to limit online guessing attacks shall ensure that an attack targeted against a given Subject's Authentication Secret shall have a probability of success of less than 2^{-14} (1 chance in 16,384) over the life of the Authentication Secret. This requires that an Authentication Secret be of sufficient complexity and that the number of invalid attempts to enter an Authentication Secret for a Subject be limited.
2. The Authentication Secret shall have at least 10 bits of min-entropy to protect against untargeted attack.

Refer to NIST Special Publication 800-63-1 [SP 800-63], Appendix A, for a discussion of Authentication Secret complexity and resistance to online guessing and how to calculate min-entropy.

4.2.3.4 ⑩ ⑧ STORED AUTHENTICATION SECRETS

Authentication Secrets shall not be stored as plaintext. Access to encrypted stored Secrets and to decrypted copies shall be protected by discretionary access controls that limit access to administrators and applications that require access (see also §4.2.5.6).

Three alternative methods may be used to protect the stored Secret:

1. Authentication Secrets may be concatenated to a variable salt (variable across a group of Authentication Secrets that are stored together) and then hashed with an industry standard algorithm so that the computations used to conduct a dictionary or exhaustion attack on a stolen Authentication Secret file are not useful to attack other similar Authentication Secret files. The hashed Authentication Secrets are then stored in the Authentication Secret file. The variable salt may be composed using a global salt (common to a group of Authentication Secrets) and the userID (unique per Authentication Secret) or some other technique to ensure uniqueness of the salt within the group of Authentication Secrets; or
2. Store Secrets in encrypted form using industry standard algorithms and decrypt the needed Secret only when immediately required for authentication; or
3. Any method protecting stored Secrets at NIST [SP 800-63] Level 3 or 4 may be used.

4.2.3.5 ⑪ ⑧ PROTECTED AUTHENTICATION SECRETS

1. Any Credential Store containing Authentication Secrets used by the IdP (or the IdP's Verifier) is subject to the operational constraints in §4.2.3.4 and §4.2.8 (that is, the same constraints as IdMS Operations). When Authentication Secrets are sent from

one Credential Store to another Credential Store (for example in an account provisioning operation) Protected Channels must be used.

2. Whenever Authentication Secrets used by the IdP (or the IdP's Verifier) are sent between services for verification purposes (for example, an IdP to a Verifier, or some non-IdP application to a Verifier), Protected Channels should be used, but Protected Channels without client authentication may be used.
3. If Authentication Secrets used by the IdP (or the IdP's Verifier) are exposed in a transient fashion to non-IdP applications (for example, when users sign on to those applications using these Credentials), the IdPO must have appropriate policies and procedures in place to minimize risk from this exposure.

4.2.4 CREDENTIAL ISSUANCE AND MANAGEMENT

The authentication Credential must be bound to the physical Subject and to the IdMS record pertaining to that Subject as described in this section.

4.2.4.1 ⑤ CREDENTIAL ISSUANCE

To ensure that the same Subject acts throughout the registration and Credential issuance process, the Subject shall identify himself or herself in any new transaction (beyond the first transaction or encounter) with information known only to the Subject, for example a temporary Secret which was established during a prior transaction or encounter, or sent to the Subject's Address of Record. When identifying himself or herself in person, the Subject shall do so either by using a Secret as described above, or through the use of an equivalent process that was established during a prior encounter.

4.2.4.2 ⑤ CREDENTIAL REVOCATION OR EXPIRATION

1. The IdPO shall revoke Credentials and Tokens within 72 hours after being notified that a Credential is no longer valid or is compromised.
2. If the IdPO issues Credentials that expire automatically within 72 hours or less then the IdPO is not required to provide an explicit mechanism to revoke the Credentials.

4.2.4.3 ⑤ CREDENTIAL RENEWAL OR RE-ISSUANCE

Appropriate policy and process must be in place to ensure that any new Credential and/or new Authentication Secret is provided only to the actual Credential Subject should it be necessary to reissue an Authentication Secret, e.g., due to suspected compromise or the Subject having forgotten the Secret, or to reissue a Credential due to expiration. This process must be at least as trustworthy as the process used for initial issuance of the Credential.

Prior to the IdPO allowing renewal or re-issuance of a Credential, the Subject must prove possession of an unexpired current Authentication Secret or, if the Subject cannot supply the current Authentication Secret, one of the following methods may be used:

1. The Subject must supply answers to pre-registered personalized questions designed to be difficult for any other person to know;
2. A short-lived single use Secret sent to the Address of Record that the Subject must submit in order to establish a new Authentication Secret.

Replacing a forgotten Authentication Secret can be accomplished at any time using the above methodology. Authentication Secrets shall not be recovered; new Secrets shall be issued.

After expiration of the current Credential or Authentication Secret, or if none of the alternative mechanisms specified above are successful, renewal and re-issuance shall not be allowed. The Subject must re-establish her or his identity with the IdPO as defined in Section 4.2 above.

All interactions conducted via a shared network shall occur over a Protected Channel such as SSL/TLS.

4.2.4.4 **⑤ CREDENTIAL ISSUANCE RECORDS RETENTION**

The IdPO shall maintain records of Credential issuance and revocation for a minimum of 180 days beyond the expiration of the Credential. These records must include, for each Credential issuance/revocation event, the Credential unique identifier and the time of issuance/revocation.

4.2.5 AUTHENTICATION PROCESS

The Subject interacts with the IdP to prove that he or she is the holder of a Credential, enabling the subsequent issuance of Assertions.

4.2.5.1 **⑥ ② RESIST REPLAY ATTACK**

The authentication process must ensure that it is impractical to achieve successful authentication by recording and replaying a previous authentication message.

4.2.5.2 **⑥ ② RESIST EAVESDROPPER ATTACK**

The authentication protocol must resist an eavesdropper attack. Any eavesdropper who records all the messages passing between a Subject and a Verifier or relying party must find that it is impractical to learn the Authentication Secret or to otherwise obtain information that would allow the eavesdropper to impersonate the Subject.

4.2.5.3 **⑥ ② SECURE COMMUNICATION**

Industry standard cryptographic operations are required between Subject and IdP in order to ensure use of a Protected Channel to communicate.

4.2.5.4 **⑥ ② PROOF OF POSSESSION**

The authentication process shall prove the Subject has possession of the Authentication Secret or Token.

4.2.5.5 **⑥ ② SESSION AUTHENTICATION**

If the IdP uses session-maintenance methods (such as cookies) so that after an initial authentication act new Assertions can be issued without the Subject having to re-authenticate, such methods shall use industry standard cryptographic techniques to ensure that sessions are at least as resistant to attack as initial authentication.

4.2.5.6 **⑥ ② MITIGATE RISK OF SHARING CREDENTIALS**

Measures shall be taken to reduce the risk of a Subject intentionally compromising his or her Credential to repudiate authentication. These should include one or more of the following, as appropriate:

- Periodic confirmations that Subjects understand and will comply with security policy requirements;
- Confirmations of sensitive online transactions through a separate channel (such as e-mail);
- Educate Subjects about threats of Authentication Secret theft from attacks such as phishing;
- Reminders to Subjects that sharing of Credentials is prohibited.

4.2.6 IDENTITY INFORMATION MANAGEMENT

Subject records in the IdPO's IdMS must be managed appropriately so that Assertions issued by the IdPO's IdP are valid.

4.2.6.1 $\circledS \circledB$ IDENTITY RECORD QUALIFICATION

If Subject records in an IdMS do not all meet the same set(s) of IAP criteria, then the IdP must have a reliable mechanism for determining which IAQ(s), if any, are associated with each record.

4.2.7 ASSERTION CONTENT

The IdPO must have processes in place to ensure that information about a Subject's identity conveyed in an Assertion of identity to an SP is from an authoritative source.

4.2.7.1 $\circledS \circledB$ IDENTITY ATTRIBUTES

The actual meaning of any attribute values identified as attributes recommended for use by InCommon Participants should be consistent with definitions in the InCommon Attribute Summary [InC-AtSum].

4.2.7.2 $\circledS \circledB$ IDENTITY ASSERTION QUALIFIER (IAQ)

An IdPO may be certified by InCommon to be able to include one or more InCommon IAQs as part of Assertions. The IdP **must not** include an InCommon IAQ that it has not been certified by InCommon to assert and **must not** include an IAQ if that Assertion does not meet the criteria for that IAP.

4.2.7.3 $\circledS \circledB$ CRYPTOGRAPHIC SECURITY

Cryptographic operations are required between an IdP and any SP. Cryptographic operations shall use industry standard cryptographic techniques.

The Assertion must be either:

- Digitally signed by the IdP; or
- Obtained by the SP directly from the trusted entity (e.g., the IdP or Attribute Service) using a Protected Channel.

4.2.8 TECHNICAL ENVIRONMENT

IdMS Operations must be managed to resist various potential threats such as unauthorized intrusions and service disruptions that might result in false Assertions of Identity or other erroneous communications.

4.2.8.1 \circledS SOFTWARE MAINTENANCE

IdMS Operations shall use up-to-date supported software.

4.2.8.2 ⑤ NETWORK SECURITY

1. Appropriate measures shall be used to protect the confidentiality and integrity of network communications supporting IdMS operations. Protected Channels should be used for communications between systems.
2. All personnel with login access to IdMS Operations infrastructure elements must use access Credentials at least as strong as the strongest Credential issued by the IdPO.

4.2.8.3 ⑤ PHYSICAL SECURITY

IdMS Operations shall employ physical access control mechanisms to restrict access to sensitive areas, including areas such as leased space in remote data centers, to authorized personnel.

4.2.8.4 ⑤ RELIABLE OPERATIONS

IdMS Operations shall employ techniques to minimize system failures and ensure that any failures are not likely to result in inaccurate Assertions being sent to SPs.

APPENDIX A: REFERENCES

- [IAAF] “**Identity Assurance Assessment Framework**”, InCommon, version 1.1,
9 Apr 2011
<http://www.incommon.org/assurance/>
- [InC-AtSum] “**InCommon Federation Attribute Summary**”, InCommon Federation,
<http://www.incommon.org/attributesummary.html>
- [TFPAP] “**Trust Framework Provider Adoption Process**”, Federal Identity,
Credential, and Access Management, Release candidate 1.0.1, 4-Sep-2009.
<http://www.idmanagement.gov/>
- [SP 800-63] “**Electronic Authentication Guideline**”, NIST, Special Publication 800-63-1
<http://csrc.nist.gov/publications/PubsSPs.html>

APPENDIX B: ACRONYMS

Acronym	Definition
IAAF	Identity Assurance Assessment Framework
IAP	Identity Assurance Profile
IAQ	Identity Assurance Qualifier
ICAM	Identity, Credential, and Access Management
ID	Identity Document
IdM	Identity Management
IdMS	Identity Management System
IdP	Identity Provider
IdPO	Identity Provider Operator
NIST	National Institute of Standards and Technology
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RA	Registration Authority
SP	Service Provider
TFPAP	Trust Framework Provider Adoption Process

APPENDIX C: DOCUMENT HISTORY

This document was developed initially by the InCommon Federation Technical Advisory Committee. The overall concept was derived from the Federal e-Authentication “Password Credential Assessment Profile” Release 2.0.0 and NIST Special Publication 800-63-1.

Version 1.1 is an extensive revision to coordinate better with the [TFPAP].

EDITORS

RL “Bob” Morgan	Tom Barton	David Walker
Jim Basney	Renee Shuey	John Krienke
Steven Carmody	Karl Heins	

Status	Release	Date	Comments	Audience
Public	1.0	4 Nov 2008	First full release for implementation	Open
Public	1.0.1	11 Mar 2009	Minor formatting fixes and clarifications	Open
	1.0.2	24 Mar 2010	Realignment of some criteria in prep for ICAM TFPAP	TAC
Public	1.0.3	22 Apr 2010	Updates for compliance with TFPAP	Open
Draft	1.1 D1	Dec 2010	Extensive revision	Limited
Draft	1.1 D8	24 Jan 2011	Further revision incl. consistent use of terms	Limited
Draft	1.1PRD1	9 Mar 2011	Revised from feedback and ready for larger review	Public
Draft	1.1FD1	9 Apr 2011	Revised from wider review; checked consistency, etc.	Limited
FINAL	1.1	9 May 2011	Approved by InCommon Steering Committee	Public

1 InCommon Federation SAML 2.0 Profiles

2 Working Draft 03 3 February 18, 2010

4 **Document identifier:**
5 draft-incommon-saml2-profiles-03

6 **Location:**
7 TBD

8 **Editors:**
9 Scott Cantor, Internet2 / The Ohio State University

10 **Contributors:**
11 Andreas Åkre Solberg, UNINETT
12 InCommon Federation Technical Advisory Committee

13 **Abstract:**
14 This document contains implementation and deployment profiles for SAML V2.0 recommended
15 for use within the InCommon Federation. It includes a set of requirements for implementers of
16 SAML products intended for use within the federation, and a narrower set of guidelines for
17 deployers intended to foster interoperability.

18 **Table of Contents**

19	1 Introduction.....	3
20	1.1 Notation.....	3
21	1.2 Normative References.....	4
22	2 SAML V2.0 Browser SSO Implementation Profile.....	5
23	2.1 Required Information.....	5
24	2.2 Metadata and Trust Management.....	5
25	2.3 Identity Provider Discovery.....	6
26	2.4 Name Identifiers.....	6
27	2.5 Attributes.....	6
28	2.6 Authentication Requests.....	6
29	2.6.1 Binding and Security Requirements.....	6
30	2.6.2 Message Content.....	7
31	2.7 Responses.....	7
32	2.7.1 Binding and Security Requirements.....	7
33	2.7.2 Message Content.....	7
34	3 SAML V2.0 Browser SSO Deployment Profile.....	8
35	3.1 Required Information.....	8
36	3.2 Metadata and Trust Management.....	8
37	3.3 Attributes.....	8
38	Appendix A. Open Issues.....	9
39		

40 1 Introduction

41 SAML V2.0 is a rich and extensible standard that must be profiled to be used interoperably, and the
42 profiles that typically emerge from the broader standardization process usually remain fairly broad and
43 include a number of options and features that increase the burden for implementers and make
44 deployment-time decisions more difficult. The InCommon Federation, in consultation with its peer
45 federations around the world, has developed a set of requirements and recommendations for both
46 implementers and deployers that are intended to promote a baseline set of features and options required
47 to interoperate securely and effectively.

48 It is the intent of the InCommon Federation to participate in the development and support of profiles more
49 broadly, and this document is a reflection of many such discussions (see [SAML2Int] in particular). The
50 profiles defined here may evolve or be superseded in response to future developments where warranted.

51 1.1 Notation

52 This specification uses normative text to describe the use of SAML capabilities.

53 The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD
54 NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this specification are to be interpreted as
55 described in [RFC 2119]:

56 ...they MUST only be used where it is actually required for interoperation or to limit behavior
57 which has potential for causing harm (e.g., limiting retransmissions)...

58 These keywords are thus capitalized when used to unambiguously specify requirements over protocol and
59 application features and behavior that affect the interoperability and security of implementations. When
60 these words are not capitalized, they are meant in their natural-language sense.

61 Listings of XML schemas appear like this.

62 Example code listings appear like this.

63 Conventional XML namespace prefixes are used throughout the listings in this specification to stand for
64 their respective namespaces as follows, whether or not a namespace declaration is present in the
65 example:

- 66 • The prefix `saml2:` stands for the SAML 2.0 assertion namespace,
 `urn:oasis:names:tc:SAML:2.0:assertion`
- 67 • The prefix `saml2p:` stands for the SAML 2.0 protocol namespace,
 `urn:oasis:names:tc:SAML:2.0:protocol`
- 68 • The prefix `md:` stands for the SAML 2.0 metadata namespace,
 `urn:oasis:names:tc:SAML:2.0:metadata`
- 69 • The prefix `idpdisc:` stands for the Identity Provider Discovery Service Protocol and Profile
 [IdPDisco] namespace, `urn:oasis:names:tc:SAML:profiles:SSO:idp-discovery-
 protocol`
- 70 • The prefix `mdattr:` stands for the Metadata Extension for Entity Attributes Version 1.0 [MetaAttr]
 namespace, `urn:oasis:names:tc:SAML:metadata:attribute`

71 This specification uses the following typographical conventions in text: `<ns:Element>`, `Attribute`,
72 `Datatype`, `OtherCode`.

80 **1.2 Normative References**

- 81 [RFC 2119] IETF RFC 2119, *Key words for use in RFCs to Indicate Requirement Levels*,
82 March 1997. <http://www.ietf.org/rfc/rfc2119.txt>
- 83 [RFC2616] IETF RFC 2616, *Hypertext Transfer Protocol – HTTP/1.1*, June 1999.
84 <http://www.ietf.org/rfc/rfc2616.txt>
- 85 [RFC2818] IETF RFC 2818, *HTTP Over TLS*, May 2000. <http://www.ietf.org/rfc/rfc2818.txt>
- 86 [IdPDisco] OASIS Committee Specification, *Identity Provider Discovery Service Protocol
87 and Profile*, March 2008. [http://docs.oasis-open.org/security/saml/Post2.0/sstc-
 saml-idp-discovery.pdf](http://docs.oasis-open.org/security/saml/Post2.0/sstc-
88 saml-idp-discovery.pdf)
- 89 [MACEAttr] MACE-Dir Working Group Publication, *MACE-Dir SAML Attribute Profiles*, April
90 2008. [http://middleware.internet2.edu/dir/docs/internet2-mace-dir-saml-attributes-
 200804.pdf](http://middleware.internet2.edu/dir/docs/internet2-mace-dir-saml-attributes-
91 200804.pdf)
- 92 [MetaAttr] OASIS Committee Specification, *SAML V2.0 Metadata Extension for Entity
93 Attributes Version 1.0*, August 2009. [http://docs.oasis-
 open.org/security/saml/Post2.0/sstc-metadata-attr.pdf](http://docs.oasis-
94 open.org/security/saml/Post2.0/sstc-metadata-attr.pdf)
- 95 [MetaIOP] OASIS Committee Specification, *SAML V2.0 Metadata Interoperability Profile
96 Version 1.0*, August 2009. [http://docs.oasis-open.org/security/saml/Post2.0/sstc-
 metadata-iop.pdf](http://docs.oasis-open.org/security/saml/Post2.0/sstc-
97 metadata-iop.pdf)
- 98 [SAML2Core] OASIS Standard, *Assertions and Protocols for the OASIS Security Assertion
99 Markup Language (SAML) V2.0*, March 2005. [http://docs.oasis-
 open.org/security/saml/v2.0/saml-core-2.0-os.pdf](http://docs.oasis-
100 open.org/security/saml/v2.0/saml-core-2.0-os.pdf)
- 101 [SAML2Meta] OASIS Standard, *Metadata for the OASIS Security Assertion Markup Language
102 (SAML) V2.0*, March 2005. [http://docs.oasis-open.org/security/saml/v2.0/saml-
 metadata-2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-
103 metadata-2.0-os.pdf)
- 104 [SAML2Bind] OASIS Standard, *Bindings for the OASIS Security Assertion Markup Language
105 (SAML) V2.0*, March 2005. [http://docs.oasis-open.org/security/saml/v2.0/saml-
 bindings-2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-
106 bindings-2.0-os.pdf)
- 107 [SAML2Prof] OASIS Standard, *Profiles for the OASIS Security Assertion Markup Language
108 (SAML) V2.0*, March 2005. [http://docs.oasis-open.org/security/saml/v2.0/saml-
 profiles-2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-
109 profiles-2.0-os.pdf)
- 110 [SAML2Err] OASIS Approved Errata, *SAML V2.0 Errata*. [http://docs.oasis-
 open.org/security/saml/v2.0/sstc-saml-approved-errata-2.0.pdf](http://docs.oasis-
111 open.org/security/saml/v2.0/sstc-saml-approved-errata-2.0.pdf)
- 112 [SAML2Int] A. Solberg et. al., *Interoperable SAML 2.0 Web Browser SSO Deployment Profile*,
113 Draft. <http://saml2int.org/profile/draftic>

114 2 SAML V2.0 Browser SSO Implementation Profile

115 This profile specifies behavior and options that implementations of the SAML V2.0 Web Browser SSO
116 Profile [SAML2Prof] are required to support. The requirements specified are *in addition to* all normative
117 requirements of the original profile, as modified by the Approved Errata [SAML2Err], and readers should
118 be familiar with all relevant reference documents. Any such requirements are not repeated here except
119 where deemed necessary to highlight a point of discussion or draw attention to an issue addressed in
120 errata, but remain implied.

121 SAML leaves substantial latitude to implementations with regard to how software is architected and
122 combined with authentication and application infrastructure. Where the terms "Identity Provider" and
123 "Service Provider" are used, they should be understood to include the total software footprint intended to
124 provided the desired functionality; no specific assumptions are made as to how the required features are
125 exposed to deployers, only that there is some method for doing so.

126 2.1 Required Information

127 **Identification:** urn:mace:incommon:profiles:saml2:browser-sso:implementation

128 **Contact information:** admin@incommonfederation.org

129 **Description:** Given below

130 **Updates:** Nothing

131 2.2 Metadata and Trust Management

132 Identity Provider, Service Provider, and Discovery Service implementations MUST support the use of
133 SAML V2.0 Metadata [SAML2Meta] in conjunction with their support of the SAML V2.0 Web Browser SSO
134 Profile [SAML2Prof]. Additional expectations around the use of particular metadata elements related to
135 profile behavior may be encountered in subsequent sections.

136 Implementations MUST support the SAML V2.0 Metadata Interoperability Profile Version 1.0 [MetalOP]. It
137 is OPTIONAL for implementations to support the generation, publication, or exportation of metadata, but
138 implementations MUST support the following mechanisms for the importation of metadata:

- 139
 - 140 • local file
 - 141 • remote resource at fixed location accessible via HTTP 1.1 [RFC2616] or HTTP 1.1 over TLS/SSL
[RFC2818]

142 In the case of HTTP resolution, implementations MUST support use of the "ETag" header for cache
143 management; other cache control support is OPTIONAL. Implementations SHOULD support the use of
144 more than one fixed location for the importation of metadata, but MAY leave their behavior unspecified if a
145 single entity's metadata is present in more than one source.

146 In accordance with [MetalOP], importation of multiple entities' metadata contained within an
147 <md:EntitiesDescriptor> element MUST be supported.

148 Verification of metadata, if supported, MUST include XML signature verification at least at the root
149 element level, and SHOULD support the following mechanisms for signature key trust establishment:

- 150
 - 151 • direct comparison against known keys
 - 152 • some form of path-based certificate validation against one or more trusted root certificates and
certificate revocation lists

153 The latter mechanism does not impose a particular profile for certificate validation, as no such profile has
154 wide enough adoption across tools and libraries to warrant such a requirement, but should be understood
155 as being consistent with the "usual" practices encountered in the implementation of certificate validation.
156 Where possible, implementations SHOULD document known limitations of the mechanisms they employ.

157 Implementations SHOULD support the SAML V2.0 Metadata Extension for Entity Attributes Version 1.0
158 [MetaAttr] and provide policy controls on the basis of SAML attributes supplied via this extension
159 mechanism.

160 Finally, implementations SHOULD allow for the automated updating/reimportation of metadata without
161 substantial disruption of services.

162 **2.3 Identity Provider Discovery**

163 Service Provider and Discovery Service implementations MUST support the Identity Provider Discovery
164 Service Protocol Profile in conformance with section 2.4.1 of [IdPDisco].

165 **2.4 Name Identifiers**

166 Identity Provider and Service Provider implementations MUST support the following SAML V2.0 name
167 identifier formats, in accordance with the normative obligations associated with them by [SAML2Core]:

- 168 • urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
- 169 • urn:oasis:names:tc:SAML:2.0:nameid-format:transient

170 Support for other formats is OPTIONAL.

171 **2.5 Attributes**

172 Identity Provider and Service Provider implementations MUST support the generation and consumption of
173 <saml2:Attribute> elements that conform to the MACE-Dir Attribute Profile for SAML 2.0 [MACEAttr],
174 with the exception that the ability to support <saml2:AttributeValue> elements whose values are not
175 simple strings (e.g., <saml2:NameID>, or other XML values) is OPTIONAL.

176 As a non-normative summary, this requirement primarily implies the capability to ensure the use of
177 particular Name and NameFormat values when generating and consuming <saml2:Attribute>
178 elements, rather than relying on hard-wired assumptions or proprietary sets of attribute identifiers.

179 **2.6 Authentication Requests**

180 **2.6.1 Binding and Security Requirements**

181 Identity Provider and Service Provider implementations MUST support the use of the HTTP-Redirect
182 binding [SAML2Bind] for the transmission of <saml2p:AuthnRequest> messages, including the
183 generation or verification of signatures in conjunction with this binding.

184 Because verification of signatures by Identity Providers cannot be guaranteed in deployments, Service
185 Provider implementations MUST NOT rely on the integrity of a signed request for the enforcement of
186 requirements derived from options such as the ForceAuthn attribute or the
187 <saml2p:RequestedAuthnContext> element. Rather, Service Providers MUST enforce such
188 requirements based on the content of the <saml2p:Response> messages they receive.

189 Support for other bindings is OPTIONAL.

190 **2.6.2 Message Content**

191 In addition to standard core- and profile-driven requirements, Service Provider implementations MUST
192 support the inclusion of at least the following <saml2p:AuthnRequest> child elements and attributes
193 (when appropriate):

- 194 • AssertionConsumerServiceURL
195 • ProtocolBinding
196 • ForceAuthn
197 • IsPassive
198 • AttributeConsumingServiceIndex
199 • <saml2p:RequestedAuthnContext>
200 • <saml2p:NameIDPolicy>

201 Identity Provider implementations MUST support all <saml2p:AuthnRequest> child elements and
202 attributes defined by [SAML2Core], but MAY provide that support in the form of returning appropriate
203 errors when confronted by particular request options. However, implementations SHOULD fully support
204 the options enumerated above. Implementations MAY limit their support of the
205 <saml2p:RequestedAuthnContext> element to the value "exact" for the Comparison attribute.

206 **2.7 Responses**

207 **2.7.1 Binding and Security Requirements**

208 Identity Provider and Service Provider implementations MUST support the use of the HTTP-POST binding
209 [SAML2Bind] for the transmission of <saml2p:Response> messages.

210 Support for other bindings is OPTIONAL.

211 Identity Provider and Service Provider implementations MUST support the signing of
212 <saml2:Assertion> elements in responses; support for signing of the <saml2p:Response> element
213 is OPTIONAL.

214 Identity Provider and Service Provider implementations MUST support the use of XML Encryption via the
215 <saml2:EncryptedAssertion> element; support for the <saml2:EncryptedID> and
216 <saml2:EncryptedAttribute> elements is OPTIONAL.

217 **2.7.2 Message Content**

218 The Web Browser SSO Profile allows responses to contain any number of assertions and statements.
219 Identity Provider implementations MUST allow the number of <saml2:Assertion>,
220 <saml2:AuthnStatement>, and <saml2:AttributeStatement> elements in the
221 <saml2p:Response> message to be limited to one.

222 In turn, Service Provider implementations MAY limit support to a single instance of those elements when
223 processing <saml2p:Response> messages.

224 It is OPTIONAL for Identity Provider implementations to support the inclusion of a Consent attribute in
225 <saml2p:Response> messages.

226 Service Provider implementations that provide some form of session semantics MUST support the
227 <saml2:AuthnStatement> element's SessionNotOnOrAfter attribute.

228 3 SAML V2.0 Browser SSO Deployment Profile

229 This profile is layered on, and supplements, the Interoperable SAML 2.0 Web Browser SSO Deployment
230 Profile [SAML2Int] and identifies InCommon-specific requirements and recommendations that go beyond
231 that specification.

232 **Note: The current reference to [SAML2Int] is to a draft version. This profile will**
233 **remain in draft form until such time as a stable version of that profile is available**
234 **for reference.**

235 3.1 Required Information

236 **Identification:** urn:mace:incommon:profiles:saml2:browser-sso:deployment

237 **Contact information:** admin@incommonfederation.org

238 **Description:** Given below, in conjunction with [SAML2Int].

239 **Updates:** Nothing

240 3.2 Metadata and Trust Management

241 It is the responsibility of each deployment to incorporate the metadata supplied by InCommon into its trust
242 management infrastructure. It is RECOMMENDED that use of the metadata conform to the SAML V2.0
243 Metadata Interoperability Profile Version 1.0 [MetaIOP] and that metadata be updated at least daily.

244 3.3 Attributes

245 It is RECOMMENDED that any <saml2:Attribute> elements exchanged via any SAML 2.0 messages,
246 assertions, or metadata conform to the MACE-Dir Attribute Profile for SAML 2.0 [MACEAttr].

247 Appendix A. Open Issues

- 248 • Do we care enough about SessionNotOnOrAfter to require support for it?
- 249 • Is making IOP "RECOMMENDED" a sufficient statement for deployers? What would it mean to
250 consume the metadata in a different fashion? Seems like we should make it REQUIRED.
- 251 • Should we make IdP-initiated SSO explicitly OPTIONAL, or just allow that Shibboleth is non-
252 conformant for the time being?

InCommon Certification Practices Statement

for

Client Certificates

14 February 2011
Version 1.0

Latest version:
14 February 2011

This version:
14 February 2011

Table of Contents

1 INTRODUCTION.....	4
1.1 Overview.....	4
1.2 Document Name and Identification.....	4
1.3 PKI Participants.....	5
1.4 Certificate Usage.....	5
1.5 Policy Administration.....	6
1.6 Definitions and Acronyms.....	6
2 PUBLICATION AND REPOSITORY RESPONSIBILITIES.....	8
2.1 Repositories.....	8
2.2 Publication of Certification Information.....	8
2.3 Time or Frequency of Publication.....	8
2.4 Access Controls on Repositories.....	8
3 IDENTIFICATION AND AUTHENTICATION.....	9
3.1 Naming.....	9
3.2 Initial Identity Validation.....	10
3.3 Identification and Authentication for Re-key Requests.....	11
3.4 Identification and Authentication for Revocation Request.....	11
4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS.....	11
4.1 Certificate Application.....	11
4.2 Certificate Application Processing.....	11
4.3 Certificate Issuance.....	12
4.4 Certificate Acceptance.....	12
4.5 Key Pair and Certificate Usage.....	12
4.6 Certificate Renewal.....	13
4.7 Certificate Re-key.....	13
4.8 Certificate Modification.....	13
4.9 Certificate Revocation and Suspension.....	14
4.10 Certificate Status Services.....	15
4.11 End of Subscription.....	16
4.12 Key Escrow and Recovery.....	16
5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS.....	16
5.1 Physical Controls.....	16
5.2 Procedural Controls.....	16
5.3 Personnel Controls.....	17
5.4 Audit Logging Procedures.....	18
5.5 Records archival.....	18
5.6 Key changeover.....	19
5.7 Compromise and disaster recovery.....	19
5.8 CA or RA termination.....	19
6 TECHNICAL SECURITY CONTROLS.....	19
6.1 Key pair generation and installation.....	19
6.2 Private Key Protection and Cryptographic Module Engineering Controls.....	20
6.3 Other aspects of key pair management.....	21

6.4 Activation data.....	21
6.5 Computer security controls.....	21
6.6 Life cycle technical controls.....	22
6.7 Network security controls.....	22
6.8 Time-stamping.....	22
7 CERTIFICATE, CRL, AND OCSP PROFILES.....	22
7.1 Certificate profile.....	22
7.2 CRL profile.....	23
7.3 OCSP profile.....	23
8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS.....	23
8.1 Frequency or Circumstances of Assessment.....	23
8.2 Identity/Qualifications of Assessor.....	23
8.3 Assessor's Relationship to Assessed Entity.....	23
8.4 Topics Covered by Assessment.....	24
8.5 Actions Taken as a Result of Deficiency.....	24
8.6 Communication of Results.....	24
9 OTHER BUSINESS AND LEGAL MATTERS.....	24
9.1 Fees.....	24
9.2 Financial Responsibility.....	24
9.3 Confidentiality of Business Information.....	24
9.4 Privacy of Personal Information.....	25
9.5 Intellectual Property Rights.....	26
9.6 Representations and Warranties.....	26
9.7 Disclaimers of Warranties.....	27
9.8 Limitations of Liability.....	27
9.9 Indemnities.....	27
9.10 Term and Termination.....	27
9.11 Individual notices and Communications with Participants.....	28
9.12 Amendments.....	28
9.13 Dispute Resolution Provisions.....	28
9.14 Governing Law.....	28
9.15 Compliance with Applicable Law.....	28
9.16 Miscellaneous Provisions.....	28
9.17 Other Provisions.....	29
	30

1 INTRODUCTION

InCommon (“InCommon”) is an identity and trust community and services provider that offers optional subscription services for X.509 PKI certificates issued by an InCommon certification authority. Subscribers are institutions as defined in the InCommon Cert Services website (incommon.org/cert). InCommon verifies the identity of each Subscriber and the Internet domains for which they are authoritative. InCommon outsources functions associated with public key operations which include receiving certificate signing requests, requests for revoking and renewing digital certificates, and the maintenance, issuance, and publication of Certificate Revocation Lists (“CRLs”) and the operation of an Online Certificate Status Protocol (“OCSP”) responder.

1.1 Overview

This InCommon Certification Practices Statement (CPS) outlines the legal, commercial, and technical principles and practices InCommon employs in approving, issuing, and managing its certificate services under the Intermediary CA Agreement (“Comodo Agreement”) between Comodo CA Limited (“Comodo”) and University Corporation for Advanced Internet Development (d/b/a Internet2) and its single-member LLC, InCommon. Under this agreement, Comodo provides full operational support, under its own CPS, for a CA that is subordinate to the Comodo “AddTrust External CA.” This CA signs end-user certificates for entities authenticated by subscribing institutions. Subscribing institutions will take appropriate technical and non-technical means to ensure that only properly identified entities are issued certificates.

InCommon’s sole responsibilities are to

- verify the identity of the subscribing institution;
- identify specific individuals at the institution who will be responsible for how certificates will be requested; and
- ensuring that subscribing institutions abide by the terms of their Subscriber Agreement with InCommon.

The CPS is formatted and maintained in accordance with IETF PKIX RFC 3647. To preserve the format of RFC 3647, some section headings do not apply and will contain the text “Not applicable” (“n/a”) or “No stipulation”. The RFC 3647 format is preserved to assist the reader in comparing and contrasting the various CPS documents provided by various CAs.

Sections of this CPS refer to services or practices provided by Comodo under the Comodo Agreement and in accord with provisions with the Comodo AddTrust External CA “Certification Practice Statement” (<http://www.comodo.com/about/comodo-agreements.php>). Such sections will contain the text “Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.” The phrase “issued by InCommon” is to be interpreted as “issued by the Comodo CA under the Comodo Agreement.”

1.2 Document Name and Identification

This document is the InCommon Client Certificate CPS version 1.0, which was approved for publication on 14 February 2011 by InCommon’s certification Policy Authority. There is no separate Certification Policy document; policy is incorporated within this document.

The object identifier (cpOID) for this CPS is identified in Appendix B and will be included in end-entity certificates issued by InCommon. The current version of the CPS is made available to the public through InCommon’s repository as described in Section 2 below.

Revisions not deemed significant by InCommon’s Policy Authority have minimal or no impact on subscribers and relying parties using certificates, the CRLs, or the OCSP responder. Insignificant revisions may be made without changing the version number of the CPS.

Revisions that are deemed significant or may affect the use or trustworthiness of certificates will result in assignment of a new cpOID to this document.

Revisions to this document have been made as follows:

Date	Changes	Version
------	---------	---------

1.3 PKI Participants

1.3.1 Certification Authorities

Certification authorities issue public key certificates to subscribers. A certification authority:

- Conforms its operations to this CPS as amended,
- Revokes certificates upon request by an authorized person,
- Maintains and updates its OCSP on a regular basis,
- Publishes CRLs on a regular basis,
- Distributes issued certificates, and
- Notifies subscribers via email of expiring certificates that it has issued to them.

1.3.2 Registration Authorities

InCommon manages its own Registration Authority (RA). Each Subscriber organization also manages and operates a delegated RA – comprising its Subscriber Registrars and any Delegated Subscriber Registrars – that is responsible for activities under its own management control for its own organization.

1.3.3 Subscribers

Subscribers are research and education institutions, organizations, or other entities that use InCommon's PKI services to acquire certificates that support transactions and communications.

Subjects are identified in an issued certificate. The Requester controls the private key corresponding to the public key listed in an issued certificate.

Regardless of the Subject listed in the Certificate, the Subscriber always has the responsibility of ensuring that the Certificate is only used appropriately.

1.3.4 Relying Parties

Relying parties use InCommon's PKI service certificates to perform transactions, communications, or other functions at their own discretion.

Digital certificates do not guarantee that a certificate holder has good intentions or that the certificate holder will be ethical. It is the Relying Parties' responsibility to independently examine each certificate holder to determine whether the certificate owner is ethical and trustworthy.

1.4 Certificate Usage

A digital certificate is formatted data that cryptographically binds an identified Subject to a public key. A digital certificate allows an entity taking part in an electronic transaction to assert its identity to the other participants in such a transaction. Certificates will only be issued to end users under this CPS.

1.4.1 Appropriate Certificate Uses

Depending on the certificate type, the certificates issued from an InCommon CA may be used for authentication, encryption, access control, and digital signature purposes.

1.4.2 Prohibited Certificate Uses

Certificates may only be used in accordance with their intended purpose and in compliance with all applicable laws and regulations including export laws as described in the Subscriber Addendum.

Certificates may not be used to complete or assist in performing any transaction that is prohibited by law. Digital certificates do not guarantee that a certificate holder has good intentions or that the certificate holder will be ethical.

Certificates may not be used for any application requiring fail-safe performance systems such as the operation of nuclear power facilities, air traffic control systems, weapon control systems, or any other system where a failure of the system could cause loss of life or property.

1.5 Policy Administration

1.5.1 Organization Administering the Document

This CPS is administered by the InCommon Policy Authority (PA). The InCommon PA is described in a document available in the InCommon CA repository as described in Section 2.

1.5.2 Contact Person

InCommon:

Chief Operating Officer, InCommon
c/o Internet2
1000 Oakbrook Dr, Suite 300
Ann Arbor, MI 48103
Email: incommon-admin@incommonfederation.org
Phone: 734.913.4250

1.5.3 Person Determining CPS Suitability for the Policy

There is no separate Certificate Policy document. The CPS combines both policy and practices.

1.5.4 CPS Approval Procedures

InCommon's CPS (and any amendments made to it) are reviewed and approved by InCommon's Policy Authority with concurrence from its legal adviser and from Comodo. Amendments to the CPS may be made by reviewing and updating the entire CPS or by publishing an addendum.

1.6 Definitions and Acronyms

Acronyms:

CA	Certification Authority
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	PKCS#10 Certificate Signing Request
MDC	Multiple Domain Certificate
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
PKCS	Public Key Cryptography Standard
RA	Registration Authority
SGC	Server Gated Cryptography
SSL	Secure Sockets Layer
TLS	Transaction Layer Security
URL	Uniform Resource Locator
X.509	The ITU-T standard for Certificates and their corresponding authentication framework

Definitions:

Applicant	The entity applying to become a Subscriber to the InCommon PKI services. May also be used to refer to an individual submitting a request for a certificate (see Requester below).
Certificate	A message that, at least, states a name or identifies the CA, identifies the Subject, contains the Subject's public key, and contains a serial number.
Delegated Subscriber Registrar	Any other individual to whom the Subscriber Registrar sub-delegates his or her permissions.
Master Registrar	Individuals within InCommon's Registration Authority who can delegate authority for certain Internet domains to up to 3 individuals within a Subscriber organization.
Registration Authority	The InCommon officer(s) who identify Subscriber Registrars and vet the Internet domains for which Subscriber may issue CSRs.
Registrar	The generic term for an individual who may approve submittal of a CSR to the CA and has certain privileges to manage the certificate life cycle. Master Registrar, Subscriber Registrar and Delegated Subscriber Registrar are collectively Registrars and individually a Registrar.
Relying Party	An entity that relies upon the information contained within the Certificate.
Relying Party Agreement	An agreement that must be read and accepted by a Relying Party prior to validating, relying on or using a Certificate and is available for reference in the InCommon PKI repository as described in Section 2.
Requester	An individual who submits a CSR either via the Comodo User Interface (UI) or indirectly via the Comodo Application Programming Interface (API).
Subject	The entity that has been named in a Certificate.
Subscriber	An entity that has entered into an agreement with InCommon to make use of InCommon PKI services.
Subscriber Addendum	A legal addendum to the InCommon Participation Agreement that must be read and accepted by an Applicant before becoming a Subscriber. The Subscriber Addendum binds the Subscriber and all agents of the Subscriber that manage or acquire certificates from InCommon to its terms and conditions.
Subscriber Executive	The management officer at the Subscribing organization responsible for designating the organization's Subscriber Registrars. The Executive is authorized as such in the InCommon participation agreement or by succession and is typically be filled by a CIO, VP of IT, or other senior administrative officer responsible for the organization's information technology assets.
Subscriber Registrar	An individual that the Subscriber's executive contact identifies to InCommon and InCommon registers with Comodo and provides credentials to allow approval of CSRs on behalf of Subscriber. A Subscriber Registrar may delegate his or her permissions to another individual whom the institution wishes to allow to approve certificate requests and manage certificate lifecycle generally.

Credentials may also be installed in an automated system for the issuance of end-entity certificates.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

This CPS is only one of a set of documents relevant to InCommon's certificate services. The list of documents below is a non-exhaustive list of other relevant documents. The document name, location of, and status, whether public or private, are detailed below.

Document Status Location	Status	Location
InCommon Client Certification Practices Statement (This document)	Public	InCommon Repository
InCommon Certificate Service Subscriber Addendum and InCommon Participation Agreement	Public	InCommon Repository
InCommon Certificate Service Relying Party Agreement	Public	InCommon Repository
InCommon Policy Authority	Public	InCommon Repository
Client CA and Certificate Profiles	Public	InCommon Repository

2.1 Repositories

InCommon publishes this CPS, related documents and certificates in its PKI services repository at <https://www.incommon.org/cert/repository/>. The InCommon Operations group maintains the repository. InCommon makes reasonable efforts to ensure that the information in its repository is accurate, updated, and correct. However, in no event shall InCommon be liable for any amounts beyond the limits set forth in this CPS.

Parties accessing the repository agree to the terms posted in the repository in regard to its use of the documents and information on the repository. InCommon may revoke repository privileges for any party failing to comply with the terms on InCommon's website.

2.2 Publication of Certification Information

Certificate information is published in accordance with the provisions of the CPS relevant to such a certificate. Certificate content is published by issuing the certificate. Revoked certificate information is published in CRLs by InCommon's CA service provider and is available also by OCSP. Users and relying parties should consult the CRLs or OCSP server prior to relying on information featured in a certificate.

2.3 Time or Frequency of Publication

Updates to the CPS are published in accordance with Section 9.12. Updates to the Subscriber Agreement, Relying Party Agreements, and other agreements posted in the repository are published as often as necessary. Certificates are published upon issuance.

2.4 Access Controls on Repositories

The information published in the InCommon repository (refer to section 2.1) is public information and may be accessed freely by anyone visiting the site, provided they agree to the site's terms and conditions as posted thereon. Read-only access to the information is unrestricted except as stated in section 2.1 above. InCommon has implemented logical and physical security measures to prevent unauthorized additions, modification, or deletions of repository entries.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

InCommon Certificates are issued with an X.501 compliant non-null Distinguished Name (DN) in the Issuer and Subject Fields. Issuer Distinguished Names will identify Internet2 (InCommon's parent organization) as the primary organization and InCommon as the organizational unit and common name. Certificate Subject Distinguished Names will identify the Subscriber as the primary organizational unit and optionally may contain an organizational subordinate unit. The Subject will be in a name space owned by or under the administrative control of the Subscriber Institution which requested the issuance of the client certificate.¹ Details of certificate profiles for certificates may be found in the InCommon PKI repository as stated in Section 2.

Enhanced naming uses an extended organization field in an X.509v3 certificate to convey information through an organizational unit field. InCommon certificates may include a brief statement describing limitations of liability, limitations in the value of transactions to be accomplished, validation period, and intended purpose of the certificate and any disclaimers of warranty that may apply. The lack of such information does not mean it does not apply to that certificate.

To communicate information InCommon may define:

- An organizational unit attribute.
- An InCommon standard resource qualifier to a certificate policy.
- Proprietary or other vendors' extensions.

3.1.2 Need for Names to be Meaningful

InCommon uses non-ambiguous designations and commonly used semantics to identify both the Issuer of the Certificate and the Subject of the Certificate.

3.1.3 Anonymity or Pseudonymity of Subscribers

Anonymity is not allowed. For pseudonymity, no specification.

3.1.4 Rules for Interpreting Various name Forms

Distinguished Names in Certificates are X.501 compliant. For information on how X.501 Distinguished names are interpreted, please see RFC 2253 and RFC 2616.

3.1.5 Uniqueness of Names

Campuses should use Subject DNs that map uniquely to a single person/entity in perpetuity. However, if this is not possible, a campus must ensure that no two valid certificates containing the same Subject DN map to different persons/entities. While Subject DNs in expired or revoked certificates may map to different persons/entities than currently valid certificates, this practice should be avoided whenever possible. Multiple certificates with different Subject DNs may map to the same person/entity.

The use of the SubjectAlt Email address and/or SubjectAlt/OtherName/PrinipalName is optional in InCommon certificates. However, if these fields are used, InCommon requires that these fields be populated with identifiers such that each field maps uniquely to the same single person/entity.

Campuses must ensure that all SubjectAltName identifiers map to a single person/entity throughout the life of any valid certificate.

InCommon recommends the use of the email field in the Subject DN to guarantee uniqueness but a campus may use any appropriate mechanism to guarantee that the Subject DN uniquely maps to a single person/entity for the period of time that a certificate is valid. If an email address is used in the Subject DN, the email address must also be populated in the appropriate SubjectAltName field.

¹ The Subject Name of a Certificate will at least contain a Country and Organization field, the exact contents for any Subscribing Institution will be determined at registration time.

InCommon's CA assigns certificate serial numbers, which appear in InCommon certificates and which are unique across all certificates issued by that CA.

3.1.6 Recognition, Authentication, and Role of Trademarks

InCommon does not permit the use of a name or symbol that infringes upon the intellectual property rights of another as stated in its subscriber agreements. However, InCommon does not verify or check the name appearing in a certificate for non-infringement. Subscribers are solely responsible for ensuring the legality of any information presented for use in an InCommon CA issued certificate. When submitting or approving a CSR, InCommon subscribers represent that they are not interfering with or infringing upon the rights of any third parties.

InCommon does not arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any intellectual property or a domain's use of any infringing material. InCommon's CA may reject a CSR or revoke a certificate if it believes that any information in the certificate may be subject to infringement claims or ownership disputes.

3.2 Initial Identity Validation

InCommon validates the identity of Institutions that intend to issue end-user certificates. Institutions agree to only issue end-user certificates that indicate affiliation with the identified organization. InCommon or Comodo may refuse to issue an end-user certificate if it appears to be fraudulently issued. However it remains the Institution's responsibility to ensure that end-user certificates are issued to only appropriately identified parties.

3.2.1 Method to Prove Possession of Private Key

Ownership of the private key is demonstrated through the submission of a valid CSR containing the matching public key.

3.2.2 Authentication of Organization Identity

InCommon may accept at its discretion any official organizational documentation supporting an application to become a Subscriber. InCommon may also use the services of a third party to validate and confirm information. Sources include

- official organizational documentation, such as business licenses, articles of incorporation, sales license or other relevant documents.
- Third-party services or records such as bank statements, records of accreditation status, or other relevant documents.

Verification can occur through an automated process or a manual review.

InCommon also verifies the identity of Subscriber's designated officers – an official executive and Subscriber Registrars designated by the executive – using out-of-band means to verify contact information and to make contact with each officer for credentialing and Subscriber Registrar's subsequent authentication to the certificate management UI.

3.2.3 Authentication of Individual Identity

It is the responsibility of subscriber institutions to authenticate and identify individual entities for which it will be issuing client certificates.

Subscriber institutions will issue certificates to its end users using a process that is at least as strong as its existing practice for managing accounts for central services such as electronic mail, calendaring, and access to central file storage.

3.2.4 Non-Verified Subscriber Information

InCommon verifies only the information listed as validated in section 4.2. Any other information provided by Subscriber Registrars is not verified by InCommon.

3.2.5 Validation of Authority

The authority of a Subscriber to be issued a certificate is first confirmed as described in section 3.2.2. Subscribers must notify InCommon if any Subscriber Registrar misrepresents his or her affiliation with or authority regarding Subscriber and Subscriber's affiliated end users.

3.2.6 Criteria for Interoperation

No stipulation.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

It is the responsibility of Subscriber institutions to determine policies related to routine re-keying.

3.3.2 Identification and Authentication for Re-key After Revocation

Subscriber institutions determine the mechanism for authenticating end-users prior to issuing certificates including after the revocation of a certificate.

3.4 Identification and Authentication for Revocation Request

It is the responsibility of Subscriber institutions to authenticate user certificate revocation requests. Authorized staff at subscriber institutions will have access to appropriate software/websites to effect revocation as necessary for client certificates issued to end-entities of their institution. Self-revocation by individual certificate holders will be allowed on a case by case basis, per Subscriber institution's preference.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

Client certificates are issued either via a website operated by Comodo or via a website operated by Subscriber which interacts with an Application Programming Interface (API) provided by Comodo. End-users submit their CSRs to this website and authorized Subscriber Registrars from the Subscriber institution or an automated process approve the request prior to the issuance of the certificate.

Alternatively certificates are issued by a programming API. In this case credentials to access this API are issued to approved contacts at the subscribing institution. The institution then runs a system of its own design to authenticate certificate requests and forward them to Comodo for issuance, using the API and provided credentials.

4.1.1 Who Can Submit a Certificate Application

Any person affiliated with a subscribing institution may apply for a certificate. It is the responsibility of the subscribing institution to determine whether or not issuing a certificate is appropriate.

4.1.2 Enrollment Process and Responsibilities

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

4.2 Certificate Application Processing

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

4.2.1 Performing Identification and Authentication Functions

The Comodo website or API server validates that the "Country", "Domain Name" and "Organization" fields of submitted CSRs are correct as determined at subscription time. It is the responsibility of the Subscriber institution to ensure that other relative distinguished name components are accurate for a given client certificate. Email addresses asserted in certificates will be validated by the Subscribing institution to ensure that the identified party owns, or has direct access to, the email address stated within the certificate.

4.2.2 Approval or Rejection of Certificate Applications

Subscriber Registrars are responsible for the approval of individual CSRs and/or for the correct operation of software that validates CSR submissions on behalf of end-users. Both InCommon and Comodo may reject the issuance of a certificate if there are reasons to believe that appropriate end-user authentication is not being properly performed.

4.2.3 Time to Process Certificate Applications

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

4.3 Certificate Issuance

InCommon may refuse to issue a certificate to any party as InCommon sees fit. InCommon is not obligated to disclose the reasons for such a refusal.

4.3.1 CA Actions During Certificate Issuance

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

4.4 Certificate Acceptance

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

4.4.1 Conduct Constituting Certificate Acceptance

No stipulation.

4.4.2 Publication of the Certificate by the CA

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Certificates and associated private keys may only be used for lawful and appropriate purposes as set forth in this CPS. Subscribers and their end users are responsible for protecting their private keys from unauthorized use.

4.5.2 Relying Party Public Key and Certificate Usage

The final decision concerning whether or not to rely on a verified digital signature is exclusively that of the relying party.

4.6 Certificate Renewal

Renewal request requirements and procedures are treated as new certificate requests.

4.6.1 Circumstance for Certificate Renewal

n/a.

4.6.2 Who May Request Renewal

n/a.

4.6.3 Processing Certificate Renewal Requests

n/a.

4.6.4 Notification of New Certificate Issuance to Subscriber

n/a.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

n/a.

4.6.6 Publication of the Renewal Certificate by the CA

n/a.

4.6.7 Notification of Certificate Issuance by the CA to other Entities

n/a.

4.7 Certificate Re-key

Rekey request requirements and procedures are treated as new certificate requests.

4.7.1 Circumstance for Certificate Re-Key

n/a.

4.7.2 Who May Request Certification of a New Public Key

n/a.

4.7.3 Processing Certificate Re-keying Requests

n/a.

4.7.4 Notification of New Certificate Issuance to Subscriber

n/a.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

n/a.

4.7.6 Publication of the Re-keyed Certificate by the CA

n/a.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

n/a.

4.8 Certificate Modification

Certificate information may change during the life of the certificate. It is the responsibility of subscriber institutions to ensure new certificates are issued as appropriate. Modification request requirements and procedures are treated as new certificate requests

4.8.1 Circumstance for Certificate Modification

n/a.

4.8.2 Who May Request Certificate Modification

n/a.

4.8.3 Processing Certificate Modification Requests

n/a.

4.8.4 Notification of New Certificate Issuance to Subscriber

n/a.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

n/a.

4.8.6 Publication of the Modified Certificate by the CA

n/a.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

n/a.

4.9 Certificate Revocation and Suspension

Upon revocation of a certificate, the operational period of that certificate is immediately considered terminated. The serial number of the revoked certificate will be placed within the CRL and OCSP server and will remain available in those locations until some time after the end of the certificate's validity period.

InCommon does not make use of certificate suspension.

4.9.1 Circumstances for Revocation

Revocation of a certificate is the permanent end of the operational period of the certificate prior to reaching the conclusion of its stated validity period. It is the Subscriber's responsibility to revoke any certificate whose private key becomes compromised or for any of the other conditions described in the Subscriber Addendum. Comodo or InCommon may revoke a digital certificate under any of the conditions described in the Subscriber Addendum.

4.9.2 Who can Request Revocation

The Subscriber, the Requester, or other appropriately authorized parties can request revocation of a certificate.

4.9.3 Procedure for Revocation Request

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

4.9.4 Revocation Request Grace Period

There is no revocation grace period.

4.9.5 Time Within Which CA Must Process the Revocation Request

The processing time is dependent upon the Subscriber Registrar's ability to respond appropriately in his or her role as Subscriber's certificate lifecycle manager. System response time is provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

4.9.6 Revocation Checking Requirement for Relying Parties

Relying Parties must always check the status of the Certificate on which they are relying. Relying Parties may check the OCSP and/or CRL to confirm that the certificate has not been revoked.

4.9.7 CRL Issuance Frequency (if applicable)

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber. Typically an updated CRL is published every 24 hours and remains valid for 5 days. Under special circumstances the CRL may be published more frequently.

4.9.8 Maximum Latency for CRLs (if applicable)

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

4.9.9 On-line Revocation and Status Checking Availability

The InCommon CA manages and makes publicly available information about revoked certificates using Certificate Revocation Lists (CRLs). All CRLs issued by the InCommon CA are X.509v2 CRLs as profiled in RFC4630. Users and relying parties are strongly urged to check the status of certificates at all times

prior to relying on information featured in a certificate. The CRL and OCSP locations are available in the InCommon Server Certificate Profile found in the InCommon Repository.

4.9.10 On-line Revocation Checking Requirements

Relying Parties must confirm the validity of a certificate via the CRL or OCSP mechanisms prior to relying on the Certificate.

4.9.11 Other Forms of Revocation Advertisements available

n/a.

4.9.12 Special Requirements Re-key Compromise

No stipulation.

4.9.13 Circumstances for Suspension

The InCommon CA does not utilize certificate suspension.

4.9.14 Who can Request Suspension

n/a.

4.9.15 Procedure for Suspension Request

n/a.

4.9.16 Limits on Suspension Period

n/a.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Each CRL and the OCSP server contains information for all of InCommon's revoked certificates until they expire.

All expired CRLs are archived as described and Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

Individual entries into the OCSP can be requested using the InCommon OCSP server. Revoked certificates are identified in the OCSP immediately after their revocation.

4.10.2 Service Availability

The OCSP server provides access to certificate status information 24x7. CRLs are open to public inspection 24x7. This is non-inclusive of scheduled maintenance and SLA downtime allowances of 99.9% availability.

4.10.3 Optional Features

n/a.

4.11 End of Subscription

Withdrawal and termination are described in the Subscriber Addendum.

4.12 Key Escrow and Recovery

The InCommon CA escrows Subscriber private keys only upon the Subscriber institution's request. Escrowed keys are kept in encrypted databases provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber. If a Subscriber recovers an escrowed private key, the corresponding certificate is automatically revoked.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical Controls

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

5.1.1 Site Location and Construction

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

5.1.2 Physical Access

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

5.1.3 Power and Air Conditioning

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

5.1.4 Water Exposures

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

5.1.5 Fire Prevention and Protection

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

5.1.6 Media Storage

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

5.1.7 Waste Disposal

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

5.1.8 Off-site Backup

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

5.2 Procedural Controls

5.2.1 Trusted Roles

Trusted roles for InCommon are defined as the RA personnel who verify the Subscriber organization status and the identity proofing of Subscriber Registrars and the assignment of Subscriber Registrar credentials to the management interface. InCommon RA personnel are also responsible for the approval process of all Subscriber information as described in section 4.2 above.

Trusted roles for the physical operation of the CA and certificate request and revocation servers are provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

5.2.2 Number of Persons Required Per Task

InCommon requires one RA for organizational vetting.

For the physical operation of the CA, requirements are provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

5.2.3 Identification and Authentication for Each Role

All InCommon personnel present at least two forms of identification to its human resources department to ensure accurate identification.

For the physical operation of the CA, requirements are provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

5.2.4 Roles Requiring Separation of Duties

RA and physical CA operations roles are separated between InCommon and Comodo.

For the physical operation of the CA, requirements are provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

InCommon follows personnel and management practices that provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties. All InCommon trusted personnel must have the necessary qualifications, experience, or training to fulfill their job descriptions.

Comodo fulfills this requirement for its personnel as stated in the Comodo CPS.

5.3.2 Background Check Procedures

Background checks are performed on all trusted InCommon personnel before access is granted to InCommon's systems. These checks include, but are not limited to, criminal history and employment history (for references).

Comodo fulfills this requirement for its personnel as stated in the Comodo CPS.

5.3.3 Training Requirements

Personnel training occurs via a mentoring process involving senior members of the team to which the employee is attached. The training program is periodically reviewed and enhanced as necessary.

Training programs are tailored toward each individual's job responsibilities and include training on PKI concepts, job responsibilities, operational policies and procedures, incident handling and reporting, and disaster recovery procedures.

Comodo fulfills this requirement for its personnel as stated in the Comodo CPS.

5.3.4 Retraining Frequency and Requirements

Personnel are required to attend refresher training courses to ensure that they can competently and satisfactorily perform their job responsibilities.

Comodo fulfills this requirement for its personnel as stated in the Comodo CPS.

5.3.5 Job Rotation Frequency and Sequence

No Stipulation

5.3.6 Sanctions for Unauthorized Actions

Personnel violating a policy or procedure are subject to disciplinary action. The action taken depends on the circumstances surrounding the action, the severity of the violation, and the personnel's past performance. In some cases, disciplinary action may include the personnel's termination.

Comodo fulfills this requirement for its personnel as stated in the Comodo CPS.

5.3.7 Independent Contractor Requirements

If an independent contractor or consultant is used, InCommon will first ensure that each such contractor or consultant is first obligated to abide by the same functional and security criteria that are set forth herein. Contractors and consultants are subject to the same sanctions as other personnel as set forth in Section 5.3.6

Comodo fulfills this requirement for its personnel as stated in the Comodo CPS.

5.3.8 Documentation Supplied to Personnel

No stipulation.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

5.4.2 Frequency of Processing Log

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

5.4.3 Retention Period for Audit Log

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

5.4.4 Protection of Audit Log

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

5.4.5 Audit Log Backup Procedures

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

5.4.6 Audit Collection System (internal vs. external)

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

5.4.7 Notification to Event-Causing Subject

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

5.4.8 Vulnerability Assessments

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

5.5 Records archival

5.5.1 Types of records archived

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

5.5.2 Retention period for archive

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

5.5.3 Protection of archive

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

5.5.4 Archive backup procedures

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

5.5.5 Requirements for time-stamping of records

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

5.5.6 Archive collection system

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

5.5.7 Procedures to obtain and verify archive information

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

5.6 Key changeover

Towards the end of each private key's lifetime, a new CA signing key pair is commissioned and all subsequently issued certificates are signed with the new private signing key. Both keys may be

concurrently active. The corresponding new CA public key certificate is provided to subscribers and relying parties through the delivery methods detailed in section 6.1 of this CPS.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

5.7.2 Computing resources, software, and/or data are corrupted

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

5.7.3 Entity Private Key Compromise Procedures

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

5.7.4 Business continuity capabilities after a disaster

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

5.8 CA or RA termination

If Internet2 must cease operation, Internet2 will make a commercially reasonable effort to notify all participants in advance of the effective date of the termination as described in the Subscriber Addendum.

6 TECHNICAL SECURITY CONTROLS

The Comodo sites hosting InCommon's PKI CA are under a security policy designed to detect, deter and prevent unauthorized logical or physical access to CA related facilities. This is provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

6.1 Key pair generation and installation

6.1.1 Key pair generation

InCommon CA's private keys are securely generated and protected by Comodo as part of the Comodo Agreement. The InCommon Client CA can generate key pairs for end-user certificates and, when it does, distribute the private keys to individuals through a secure channel provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber. A Subscriber institution can also upload CSRs, creating its own key pairs.

6.1.2 Private key delivery to subscriber

If keys are generated by the Comodo-hosted system (for example, through the web-based self-enrollment system), key delivery specifications are provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber..

6.1.3 Public key delivery to certificate issuer

Certificate requests are generated using Subscriber's software, and the request is submitted to the InCommon CA's approval workflow in the form of a PKCS #10 Certificate Signing Request (CSR).

6.1.4 CA public key delivery to relying parties

InCommon delivers issued certificates to certificate requesters. InCommon PKI root certificates are provided by Comodo, which protects the root CAs that issue the InCommon CA certificates.

The AddTrust External CA Root certificate is present in commonly available web browsers and other device stores and is made available to relying parties through these methods.

6.1.5 Key sizes

Key pairs are of sufficient length to prevent unauthorized determination or reverse engineering of the private key. InCommon's Intermediate CA keys sizes are 2048 bit. For client certificates, InCommon strongly recommends 2048 bit keys.

6.1.6 Public key parameters generation and quality checking

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

The key usage field extension in InCommon Certificates specifies the purpose for which the Certificate and key pair may be used. Enforcement of the limitations of use found in this field is beyond InCommon's control as correct use is highly dependent on having the correct software.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

Protection of InCommon CA key pairs is provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

6.2.1 Cryptographic module standards and controls

Comodo CA Limited protects CA cryptographic key pairs in accordance with its AICPA/CICA WebTrust program compliant infrastructure and CPS. Details of Comodo's WebTrust compliance are available at its official website (www.comodogroup.com).

6.2.2 Private key (n out of m) multi-person control

For InCommon CA key recovery purposes, the InCommon CA signing keys will be encrypted and stored within a secure environment. InCommon's escrowed copy of the private key is split across a number of removable media and requires a subset of the number to reconstruct. Custodians in the form of two or more InCommon authorized officers are required to physically retrieve the removable media from the distributed physically secure locations.

6.2.3 Private key escrow

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

6.2.4 Private key backup

InCommon's CA keys are generated and stored by Comodo as part of the Comodo Agreement.

Subscribers and their end users are solely responsible for protection of their private keys. InCommon maintains no involvement in the protection of such keys.

6.2.5 Private key archival

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

6.2.6 Private key transfer into or from a cryptographic module

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

6.2.7 Private key storage on cryptographic module

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

6.2.8 Method of activating private key

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

6.2.9 Method of deactivating private key

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

6.2.10 Method of destroying private key

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 Other aspects of key pair management

No stipulation.

6.3.1 Public key archival

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

6.3.2 Certificate operational periods and key pair usage periods

The operational period of each Certificate generated ends upon its revocation or expiration. The validity period of InCommon certificates varies dependent on the certificate type, but typically, a certificate will be valid for 1 to 3 years. InCommon reserves the right to, at its discretion, issue certificates that may fall outside of these set periods.

6.4 Activation data

6.4.1 Activation data generation and installation

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

6.4.2 Activation data protection

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

6.4.3 Other aspects of activation data

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

6.5 Computer security controls

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

6.5.1 Specific computer security technical requirements

InCommon computer systems are set up and maintained in a secure manner that prevents unauthorized access. The InCommon CA computers are provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

6.5.2 Computer security rating

No Stipulation.

6.6 Life cycle technical controls

6.6.1 System development controls

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

6.6.2 Security management controls

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

6.6.3 Life cycle security controls

No Stipulation.

6.7 Network security controls

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

6.8 Time-stamping

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

7 CERTIFICATE, CRL, AND OCSP PROFILES

This CPS covers only Client certificates.

InCommon may update or extend its list of products, including the types of certificates it issues, as it sees fit. The publication or updating of the list of InCommon products creates no claims by any third party. If necessary, InCommon will amend this CPS or create a separate CPS upon the inclusion of a new certificate product in the InCommon hierarchy. The CPS will usually be made public on the official InCommon websites at least seven (7) days prior to the offering such new product.

Revoked certificates are appropriately referenced in the CRL and/or OCSP.

7.1 Certificate profile

In order to use and rely on an InCommon certificate, the relying party must use X.509v3 compliant software. Supported certificate profiles are listed in the InCommon Repository.

7.1.1 Version number(s)

See the Client certificate profile in the InCommon Repository.

7.1.2 Certificate extensions

The InCommon CA uses the standard X.509, version 3, to construct digital certificates for use within the InCommon PKI. X.509v3 allows a CA to add certain certificate extensions to the basic certificate structure. InCommon uses a number of certificate extensions for the purposes intended by X.509v3 as per Amendment 1 to ISO/IEC 9594-8, 1995.

7.1.3 Algorithm object identifiers

Refer to the Certificate Profile found in the repository.

7.1.4 Name forms

Refer to the Certificate Profile found in the repository.

7.1.5 Name constraints

No Stipulation.

7.1.6 Certificate policy object identifier

A Certificate Policy (CP) is a statement of the issuer that corresponds to the prescribed usage of a digital certificate within an issuance context. A policy object identifier (OID) is a number unique within a specific domain that allows for the unambiguous identification of a policy, including a certificate policy or a certification practices statement (CPS).

Specific InCommon certificate profiles are found in the InCommon Repository, and any relevant OIDs are provided in Appendix B.

7.1.7 Usage of Policy Constraints extension

No Stipulation

7.1.8 Policy qualifiers syntax and semantics

The InCommon CA includes information in the Policy Qualifier field of the Certificate Policy extension that puts Relying Parties on notice as to the location of its CPS. This field usually includes a URL that points the Relying Party to the Relying Party Agreement, the CPS, and other documents in the repository where they can find out more about the limitations on liability and other terms and conditions governing the use of the Certificate.

7.1.9 Processing semantics for the critical Certificate Policies extension

No Stipulation.

7.2 CRL profile

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

7.2.1 Version number(s)

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

7.2.2 CRL and CRL entry extensions

No Stipulation.

7.3 OCSP profile

OCSP is a way for users to obtain information about the revocation status of an InCommon CA issued Certificate. The InCommon CA uses OCSP to provide information about any of its revoked certificates that are unexpired. OCSP responders conform to RFC 2560.

7.3.1 Version Number(s)

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

7.3.2 OCSP Extensions

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The practices specified in this CPS have been designed to meet or exceed the requirements of generally accepted and developing industry standards, including the AICPA/CICA WebTrust Program for Certification Authorities, ANS X9.79:2001 PKI Practices and Policy Framework, and other industry standards related to the operation of CAs.

8.1 Frequency or Circumstances of Assessment

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

8.2 Identity/Qualifications of Assessor

Provided by Comodo as stated in the Comodo CPS.

8.3 Assessor's Relationship to Assessed Entity

Provided by Comodo as stated in the Comodo CPS.

8.4 Topics Covered by Assessment

Provided by Comodo as stated in the Comodo CPS.

8.5 Actions Taken as a Result of Deficiency

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

8.6 Communication of Results

Provided by Comodo as stated in the Comodo CPS and binding upon the Subscriber.

9 OTHER BUSINESS AND LEGAL MATTERS

While the structure of this CPS has been left intact as a matter of RFC form, the representations, warranties and limitations associated with this service are described in detail and governed by the provisions in the InCommon Participation Agreement and the Certificate Service Addendum.

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

Fees are detailed on the official InCommon website (www.incommon.org/cert). InCommon may change these fees pursuant to its rights under the Subscriber Addendum.

9.1.2 Certificate Access Fees

Currently, InCommon does not charge a fee for Certificate access but may in the future. Charges may be incurred for extensive or time-consuming searches. Fees for such extensive use are negotiated on an individual basis.

9.1.3 Revocation or Status Information Access Fees

InCommon does not charge fees for the revocation of a certificate or for a Relying Party to check the validity status of an InCommon-issued certificate using its CRLs or OCSP.

9.1.4 Fees for Other Services

Fees for other services offered by InCommon are set either within the individual agreements with the parties or are detailed on the official InCommon website, depending on the services required.

9.1.5 Refund Policy

Subscriber refunds are described in the Subscriber Addendum.

9.2 Financial Responsibility

InCommon accepts no financial responsibility.

9.2.1 Insurance Coverage

Refer to the Subscriber Addendum and Relying Party Agreement.

9.2.2 Other Assets

InCommon accepts no financial responsibility

9.2.3 Insurance or Warranty Coverage for End-Entities

InCommon provides no warranty as further described in the Subscriber Addendum and Relying Party Agreement.

9.3 Confidentiality of Business Information

InCommon observes the following rules on the protection of business information:

9.3.1 Scope of Confidential Information

InCommon keeps the following types of information confidential and maintains reasonable controls to prevent the exposure of such records to non-trusted personnel.

- Executed Subscriber agreements when not in violation with applicable state, federal, or other law (for example, state "sunshine" laws).
 - Financial transaction records and financial audit records.
 - External or internal audit trail records and reports.
 - Certain portions of its contingency plans and disaster recovery plans.
 - Internal tracking and records on the operations of the PKI infrastructure, certificate management and enrollment services and data.
 - Subscriber Registrar email address and telephone if requested by Subscriber Registrar
Proof of existence and organizational status of the Organization if marked
- Confidential by Subscriber

9.3.2 Information Not Within the Scope of Confidential Information

Subscribers acknowledge that revocation data of all certificates issued by the InCommon CA is public information. Subscriber data marked as “Public” or submitted as part of a certificate request is not confidential and is published within an issued digital certificate in accordance with this CPS.

9.3.3 Responsibility to Protect Confidential Information

All personnel in trusted positions handle all confidential information in strict confidence. InCommon is not required to and does not release any confidential information, unless otherwise required by law or by obtaining consent from the party to whom the confidential information belongs, without an authenticated, reasonably specific request by an authorized party specifying:

- The consent of the party to whom InCommon owes a duty to keep information confidential.
- The name of the party requesting such information.
- A court order, if any.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

InCommon has implemented a privacy policy, which complies with this CPS. The InCommon privacy policy is published in the InCommon repository described in section 2.

9.4.2 Information Treated as Private

Any information about the designated officers of Subscriber organizations that is not publicly accessible or available through the content of the issued certificate, a CRL, or the OCSP is treated as private information. Subscriber organizations are responsible for the personal information of their delegated officers and constituents.

9.4.3 Information Not Deemed Private

Certificates, CRLs, the OCSP, and the information appearing in them are not considered private. Information about Subscribers available in public directories or databases is also not considered private.

9.4.4 Responsibility to Protect Private Information

All InCommon personnel receiving private information are responsible for protecting such information from compromise and disclosure to third parties. Each party will use the same degree of care that it exercises with respect to its own information of like importance, but in no event will the degree of care be less than a reasonable degree of care.

9.4.5 Notice and Consent to Use Private Information

Unless otherwise stated in this CPS, the applicable privacy policy, or by agreement, InCommon will use private information only for its own business purposes related to the services it provides to Subscriber and will not share that information with external parties except as required for by law or with the permission of the subject.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

InCommon is entitled to disclose any confidential or private information, if InCommon believes, in good faith, that the disclosure is necessary in response to subpoenas and search warrants or if disclosure is necessary in response to a pending legal proceeding or a state's mandated sunshine laws.

9.4.7 Other Information Disclosure Circumstances

No Stipulation.

9.5 Intellectual Property Rights

InCommon or its partners or associates own all intellectual property rights associated with its databases, websites, InCommon digital certificates and any other publication originating from InCommon, including this CPS.

9.5.1 Certificates

Certificates are the property of InCommon. InCommon gives permission to reproduce and distribute certificates on a nonexclusive, royalty-free basis, provided that they are reproduced and distributed in full. InCommon reserves the right to revoke the certificate pursuant to revocation terms in the Subscriber Addendum. Private and public keys are the property of the subscriber's Subjects who rightfully generate and hold them.

Subscribers represent that their use of the certificate does not interfere with or infringe on any rights of third parties. The Subscriber represents that it is not seeking to use the issued certificate's domain and distinguished names for any unlawful purpose, including tortious interference with contract or prospective business advantage, unfair competition, injuring the reputation of another, and confusing or misleading a person, whether natural or incorporated.

9.5.2 Copyright

Copyright © 2010 by Internet2. Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for commercial advantage and that copies bear this notice. Abstracting or creation of derivative works with credit is permitted. To copy otherwise, to republish, to post on servers, or to redistribute to lists, requires prior specific permission.

9.5.3 Trademarks

See Subscriber Addendum.

9.5.4 Infringement

InCommon does not provide infringement resolution services. Subscribers are responsible for their own use of certificates. See the Subscriber Addendum for legal protections, rights and responsibilities.

9.6 Representations and Warranties

Subscribers, Subjects, relying parties and any other parties must not interfere with or reverse engineer the technical implementation of InCommon PKI services, including, but not limited to, the key generation process, the public website, and the InCommon repositories except as explicitly permitted by this CPS or upon prior written approval of InCommon or Comodo as appropriate. Results of failure to comply with this as a subscriber is described in the Subscriber Addendum. Failure to comply with this as a Relying Party will result in the termination of the agreement with the Relying Party, the removal of permission to use or access the InCommon repository and any Digital Certificate or Service provided by InCommon.

All parties – subscribers, certificate subjects, relying parties, and any others – are solely responsible for having exercised independent judgment and employed adequate training in choosing security software, hardware, and encryption/digital signature algorithms, including their respective parameters, procedures, and techniques as well as in using PKI as a solution to their security requirements.

9.6.1 CA Representations and Warranties

Other than the representations and warranties already detailed in this CPS, see Subscriber Addendum and InCommon Participation Agreement.

9.6.2 RA Representations and Warranties

Other than the representations and warranties already detailed in this CPS, see Subscriber Addendum and InCommon Participation Agreement.

9.6.3 Subscriber Representations and Warranties

Other than the representations and warranties already detailed in this CPS, see Subscriber Addendum and InCommon Participation Agreement

9.6.4 Relying Party Representations and Warranties

See the Relying Party Agreement in the InCommon Repository.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

InCommon disclaims all warranties and obligations of any type, including any warranty of fitness for a particular purpose. See the Subscriber Addendum and InCommon Participation Agreement (found in the InCommon Repository) for further information.

9.8 Limitations of Liability

See the Subscriber Addendum and InCommon Participation Agreement (found in the InCommon Repository) for further information.

9.9 Indemnities

9.9.1 Subscriber Indemnity to InCommon

Indemnification by Subscriber to InCommon, if any, is described in the InCommon Subscriber Addendum.

9.9.2 Subscriber Indemnity to Relying Parties

No stipulation.

9.10 Term and Termination

9.10.1 Term

This CPS and any amendments are effective seven days after being published to the Repository and remain effective until replaced with a newer version.

9.10.2 Termination

In case of termination of CA operations for any reason whatsoever except in the case of force majeure, InCommon will provide timely notice and transfer of responsibilities to succeeding entities, maintenance of records, and remedies. Details are provided in the Subscriber Addendum, available in the repository.

9.10.3 Effect of Termination and Survival

Details are provided in the Subscriber Addendum, available in the repository.

9.11 Individual notices and Communications with Participants

InCommon accepts notices related to this CPS by means of email messages or in paper form to the InCommon point of contact listed in section 1.5.2. For communication issues related to the performance of certificates or the designation of Subscriber Executives and Registrars, secure communication will be required, either through out-of-band means such as telephone, through authorized web-based transactions or email secured by digital signature.

9.12 Amendments

The InCommon PA is also responsible for determining the suitability of proposed changes to the CPS prior to the publication of an amended edition. Amendments to this CPS may be made from time to time as approved by the InCommon PA and Comodo. Amendments may be in the form of either an amended form of the CPS or made available as a supplemental document in InCommon's repository.

9.12.1 Procedure for Amendment

Updates supersede any designated or conflicting provisions of the referenced version of the CPS and are indicated through appropriate revision numbers and publication dates. Revisions that are not deemed significant by InCommon (those amendments or additions that have minimal or no impact on Subscribers or Relying Parties), are made without notice and without changing the version number of this CPS.

9.12.2 Notification Mechanism and Period

Upon the PA approving such changes deemed to have significant impact on the users of this CPS, an updated edition of the CPS will be published in the InCommon repository, with seven (7) days notice given to Subscribers via email of upcoming changes. Suitable incremental version numbering will identify new editions.

9.12.3 Circumstances Under Which OID Must be Changed

If InCommon decides that a material change in InCommon's certificate policy warrants a change in the currently specified OID for a particular certificate type, then the revised CPS or amendment thereto will contain a revised OID for that type of certificate.

9.13 Dispute Resolution Provisions

Before resorting to any dispute resolution mechanism including adjudication or any type of alternative dispute resolution, a party must notify InCommon of the dispute with a view to seek a resolution. Parties must work with InCommon in good faith to resolve issues in a reasonable manner prior to third party involvement.

9.14 Governing Law

Details are provided in the InCommon Certificate Service Subscriber Addendum, available in the repository. This choice of law is made to provide uniform interpretation of this CPS, regardless of the place of residence or place of use of InCommon's certificates.

9.15 Compliance with Applicable Law

All parties agree to abide by all applicable laws when validating, issuing, or using certificates.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

This CPS is not the entire agreement between any parties. All parties must accept additional agreements prior to receiving, using, or relying on a digital certificate. Section headings are for reference and convenience only and are not part of the interpretation of the CPS.

9.16.2 Assignment

This CPS is binding upon all successors and representatives of any party. The rights in this CPS are assignable.

9.16.3 Severability

Any provision held invalid or unenforceable will be reformed to the minimum extent necessary to make the provision valid and enforceable. If reformation is not possible, the provision is deemed omitted and the balance of the CPS remains valid and enforceable.

9.16.4 Enforcement

InCommon's failure to enforce any provision of this CPS does not waive its right to enforce the same provision later or right to enforce any other provision of this CPS. To be effective, all waivers must be both in writing and signed by InCommon. Agreements between InCommon and various parties control in the event of a conflict between this CPS and the Subscriber Addendum.

Except where an express time frame is set forth in this CPS, any delay or omission by any party will not impair or be construed as a waiver of such right, remedy or power.

9.16.5 Force Majeure

InCommon is not liable for a delay or failure to perform an obligation to the extent that the delay or failure is caused by an occurrence beyond the party's reasonable control. The operation of the Internet is beyond InCommon's reasonable control, and InCommon is not responsible for a delay or failure caused by an interruption or failure of telecommunication or digital transmission links, Internet slow-downs or failures, or other such transmission failure.

9.17 Other Provisions

No Stipulation

Acknowledgments

The InCommon Policy Authority acknowledges the considerable efforts of the research and education community in the development of this CPS. Specifically a task force under the InCommon Technical Advisory Committee, a PKI advisory committee, edited and contributed to this document: Jim Jokl (Chair), University of Virginia; Jim Basney, National Center for Supercomputing Applications; Paul Caskey, University of Texas System; Michael Gettes, Carnegie Mellon University; Garick Hamlin, University of Pennsylvania; Dan Jones, University of Colorado; John Krienke, InCommon/Internet2; David Walker, University of California, Davis; David Wasley, ret., University of California Office of the President; and Jeffrey I. Schiller, Massachusetts Institute of Technology.

APPENDIX A
PKI HIERARCHY

Comodo The UserTrust Network CA: InCommon Standard Assurance Client CA: Subscriber Client Certificates

APPENDIX B
CERTIFICATE OBJECT IDENTIFIERS

CPS OID **1.3.6.1.4.1.5923.1.4.3.3.0.1**

Appendix H. Federation for Identity and Cross-Credentialing Systems, Inc.®

Attachment 1: FiXs® Bylaws

Attachment 2: FiXs Operating Rules

Attachment 3: FiXs Policy Document

Attachment 4: FiXs Trust Model

Attachment 5: FiXs Implementation Guidelines

Attachment 6: FiXs Security Guidelines

Attachment 7: FiXs Trusted Broker (FTB) Gateway: Operating and Interface Specification and Statement of Objectives

Attachment 8: FiXs Configuration Control Board Procedures

Attachment 9: FiXs Certification and Accreditation Process



The Federation for Identity and
Cross-Credentialing Systems®

FiXS® Bylaws
Version 3.0
September 1, 2010

www.fixs.org

Copyright 2010 by the Federation for Identity and Cross-Credentialing Systems, Inc.®
All Rights Reserved
Printed in the United States of America
10400 Eaton Place, Suite 500A
Fairfax, VA 22030
(703) 591-9255

Bylaws of
**THE FEDERATION FOR IDENTITY
AND CROSS-CREDENTIALING SYSTEMS, INC.®**

Article I: Nature

- 1 **Name.** The name of the corporation is the **Federation for Identity and Cross-Credentialing Systems, Inc. (“Federation”)**, which is a non-profit, non-stock corporation incorporated under the laws of the Commonwealth of Virginia.
- 2 **Location.** The principal office of the Federation is 10400 Eaton Place, Suite 500A, Fairfax, VA 22030-2208. The Federation shall have such statutory registered office and agent as determined by the Board of Directors consistent with applicable Virginia law.
- 3 **Assets.** The Federation’s assets, including any intellectual property, will be owned by and accrue to the benefit of the Federation.
- 4 **Purposes/Objectives.** The purposes and objectives of the Federation are generally set forth in the Articles of Incorporation and include but are not limited to the following specific purposes and objectives:
 - a. Establish, maintain and oversee the Federation for Identity and Cross-Credentialing Systems (“FiXs®”) Network (“FiXs Network”) and standards for the purpose of interconnecting and cooperating for the specific efforts of identity protection, management and authentication for physical and logical access requirements, including compliance with certain common trust models, business rules, policies, and technical specifications standards adopted by the Federation. (The first instantiation of the Network was with the Department of Defense (“DoD”), which established an interface between its Defense Cross-Credentialing Identification System (“DCCIS”) and FiXs. Subsequent instantiations will provide solutions that satisfy Homeland Security Presidential Directive 12 (HSPD-12) and potentially other commercial and government requirements both domestically and internationally.)
 - b. Establish a foundation for the interoperability of identity authentication and verification standards within the FiXs Network to include biometrics.
 - c. Maintain and enforce the provisions of the various governance documents that provide the foundation for the Federation, including the Trust Statement, the FiXs Policy, the Operating Rules (“Rules”), the Technical Interface and Specifications, Implementation Guidelines, Security Guidelines, and any governance documents, Memoranda of

Understanding, and/or other agreements between government, industry, as well as the membership of the Federation.

- d. Establish standards and oversee the operations of the FiXs Network. These responsibilities shall include:
 - (1) Admit and revoke membership into the Federation and the FiXs Network.
 - (2) Developing and executing the operating model for the Federation. This will include a plan for the financing the standards setting activities; certification activities; membership management; ongoing policy and standards updates; and oversight of the FiXs Network in compliance with such standards.
 - (3) Copyrighting of the trust model, policy and “Rules” of the Federation; registering other documents or art (such as a service mark) as may be necessary; and issuing and licensing Federation technical solutions (including software), products and services to issuers and sponsors.
 - (4) Developing and managing Federation service mark(s). This will include any graphics standards for and registering a FiXs service mark, by trademark, that will be owned by the Federation, and overseeing and enforcing the distribution and display of the service mark.
 - (5) Contracting and/or licensing with members in Good Standing for the operations, management and oversight of a federated architecture and interfaces that constitute the FiXs Network. The Federation shall be responsible for the development, maintenance and operation of the core FiXs Network infrastructure requirements, standards, and related activities.
 - (6) Maintaining the configuration and the interoperability of the FiXs architecture.
 - (7) Establishing and maintaining assessment, auditing and certification requirements for sites, personnel, and equipment associated with the FiXs Network for both physical and logical access. This shall include employing the proper and necessary certification and accreditation (C&A) requirements and issuing the necessary authority to operate (ATO) to member firms as set forth in the Operating Rules and other Federation documents as may be amended from time-to-time.
 - (8) Developing or modifying new product and service offerings and standards to keep the architecture relevant and current.

- 5 *Tax Status.* It is intended that the Federation be operated as a tax-exempt organization under Section 501(c)(6) of the Internal Revenue Code of 1986, as amended, or the corresponding provision of any subsequent federal tax law, and that the Federation only engage in activities permitted to be carried out by such an organization.

Article II: Participation

1. *Membership.* Membership is on an organizational or corporate basis determined by size and function of the entity. All members and the organizations or companies they represent agree to comply with the Federation's Bylaws, the Federation's anti-trust and intellectual property policies, and other policies, operating rules and procedures adopted by the Federation or the Board of Directors.
2. *Classes of Membership.* There are six classes of membership:
 - a. *Founding Members.* Founding Members are companies that established FiXs by participating in the initial pilot, proof of concept and transition to full production of the system. Founding Members are entitled to a seat on the Board of Directors, provided that the organization remains in Good Standing with FiXs, as determined by the Membership Committee. All Founding Members are entitled to two votes that may be cast in the resolution of any issue that is before the Board of Directors, the Membership Forum, or any Committee, Subcommittee or Work Group. If a Founding Member is acquired by, merges with, or in some manner assigns its' interest in the Federation to another company, the company making the acquisition or the company resulting from the merger shall retain the Founding Member status. Upon any such acquisition, merger or assignment, the resulting successor in interest shall be subject to any then prevailing membership conditions or criteria, such as background checks, etc. and pay the fee applicable to their membership class or size status. Further, any voting rights shall not be cumulative for any such party. Specifically, no single entity with Founding Member status can have more than two (2) votes and no other Member can have more than one (1)vote in the case of two (2) or more FiXs Members interests being combined in some manner. The following organizations are Founding Members:
 - (1) Founding Large Business Members. Companies with 500 or more employees. The Founding Full Members are: HP, Lockheed Martin Corporation, Northrop Grumman Corporation, and WidePoint.
 - (2) Founding Small Business Members. Companies with fewer than 500 employees. The Founding Small Business Members are: Data Systems Analysts, Inc; and Wave Systems Corp.
 - (3) Founding Association Members. Associations or coalitions. The Founding Association Member is: AFCEA International - The Armed Forces Communications and Electronics Association.

- (4) Founding Sole Proprietor Members. Sole Proprietor Entities that bring special skills or talents. The Sole Proprietor Members are: Unlimited New Dimensions, LLC, 3Factor, and Little River Management Group, LLC (or their assignees).
- b. Full Members. Organizations or corporations, other than the Founding Members, whose employees are enrolled in the FiXs Network, that rely on FiXs identifiers, that provide services or products to the FiXs Network, or that represent the interests of Participants in the FiXs Network. There are two categories of Full Members: Large Businesses and Small Businesses. Small Businesses are organizations or corporations that have fewer than 100 employees. Each Full Member shall be entitled to: privileges as specified in Article IV; be nominated to serve on the Board of Directors; and, if elected, be entitled to one vote on the Board; and cast one vote in the resolution of any issue that is before the Membership Forum, a Committee, Subcommittee or Work Group of the Federation.
- c. Associations and Not-for-Profit Members. Organizations that represent specific industry segments/sectors that have an interest in furthering the goals and objectives of the federated identity management and protection infrastructure for physical and logical access. These organizations may also have an interest in furthering an identity management and protection business model for their industry segment/sector. Certain Associations may also act as “portals” to FiXs, whereby the Association may induce or otherwise encourage members of that separate Association to join FiXs thereby increasing the level of membership in the Federation. Associations acting in this capacity, namely “*Associations acting as Portals*” will be entitled to a reduced dues amount over the dues applicable to other Associations.
- Each Association and Not-for-Profit member shall be entitled to participate in the resolution of issues before the Membership Forum, or a Committee, Subcommittee or Work Group. Each shall also be entitled to one vote as specified in Article IV.
- d. Associate Members. Organizations whose employees are enrolled in the FiXs Network; that rely on FiXs identifiers; that provide services or products to the FiXs Network; or that represent the interests of Participants in the FiXs Network. Network User Associate Members are Associate Members that participate in the FiXs Network by having Participants enrolled in the system and/or by serving as Credential Issuers or Relying Parties. Non-User Associate Members are Associate Members that do not actively participate in the FiXs Network but participate by providing leadership, services or products/technologies to the FiXs Network. Non-User Associate Members do not have Participants enrolled in the FiXs Network, nor do they serve as Credential Issuers or Relying Parties. Each associate shall be entitled to participate in the resolution of any issue before the Membership Forum, a Committee, Subcommittee or Work Group of the Federation, but shall not be entitled to vote.
- e. Sole Proprietor Members. Organizations of ten or fewer employees who have a special interest or talent in support of the Federations' goals and objectives. Each member shall

be entitled to participate in the resolution of any issue before the Membership Forum, a Committee, Subcommittee, or Work Group of the Federation, but shall not be entitled to vote. However, on a case-by-case basis, the Executive Committee may vote to make a Sole Proprietor Member eligible to: (1) be elected to the Board of Directors; (2) vote on members of the Board of Directors; (3) vote on any issue before the Membership Forum, or a Committee, Subcommittee or Work Group of the Membership Forum; (4) chair a Committee or Work Group; and (5) participate in other activities not reserved for the Board of Directors under the Federation's Bylaws.

- f. **Subscribers**. Organizations that exclusively sponsor their employees and/or their agents to obtain and use FiXs-certified credentials. Subscribers do not participate in the proposing, drafting, or setting of standards, operating rules or other governance activities of the Federation. Subscribers do not participate on any committees, work groups or other member forums or hold any positions in the Federation. The only fees or obligations of being a Subscriber to the Federation entail paying a nominal fee associated with conducting any required background check(s) of the organization to determine the legitimacy of the organization and an affirmative acknowledgement of the obligations to comply with the rules and standards of the Federation; to include those associated with any Terms of Use License Agreement(s). Any organization or legal entity of any size, type or structure is eligible to become a Subscriber to the Federation, abiding by its operating rules, guidelines and policies, and thus use its certified services and products.
3. **Government Advisors**. While not being formal Federation members, government employees from certain federal, state, or other governmental agencies or departments approved by the Federation may participate in all Federation meetings, conference calls and other functions and provide input into the development of Federation projects and documents without paying dues. Each Government Advisor shall be entitled to participate in the resolution of any issue before the Membership Forum, a Committee, Subcommittee, or Work Group of the Federation. However, Government Advisors will not be entitled to a vote and do not have fiduciary duties as officers, directors, or committee members as part of the Federation.
4. **Categories of Membership**. The Federation may establish additional categories of membership or dissolve certain categories of membership, as determined to be in the best interests of the Federation, at its sole discretion. It is anticipated that membership categories will be based on an organization's role in the Federation, credential issuance and Network usage.
5. **Membership Application**. Application for membership shall be in accordance with the FiXs Operating Rules.
6. **Membership Determination**. Determination of membership is based upon whether the applicant meets the criteria for a category of membership and the requirements of the Federation. Any question with regard to membership determination shall be resolved by the Board of Directors.

7. *Resignation.* Any member may resign by filing a written resignation with the President of the Federation; however, resignation does not relieve a member from liability for any unpaid dues or fees, or any other obligation arising prior to the date of resignation. If a member has made payment on any invoice prior to resigning, then no refunds will be given.
8. *Termination.* Any member may be terminated for failure to maintain Good Standing eligibility for membership, for failure to pay required dues or fees, or for good cause in accordance with “due process” policies and procedures recommended by the Membership Committee and adopted by the Board of Directors.
9. *Membership Transfer and Allocation of Votes.* Founding Members each have two votes and Full Members and Associations/Not-for-Profit members shall each have one vote on issues before the Membership Forum and Committees, Subcommittees and Work Groups of the Membership Forum. In the case of the acquisition, merger or assignment of any FiXs membership, the resulting successor in interest shall be subject to any then prevailing membership conditions or criteria, such as background checks, etc. and pay the dues applicable to their membership class or size status. Further, any voting rights shall not be cumulative for any such party. Specifically, no single entity with Founding Member status can have more than two (2) votes and no other Member can have more than one (1) vote in the case of two (2) or more FiXs Members merging in some manner.

Article III: Dues, Fees, Vesting and Termination

Membership dues will be assessed on a sliding scale, based on an organization’s revenue and/or size. The Federation Strategy, Business, and Finance Subcommittee of the Executive Committee shall develop a business model for fees and other funding for: (1) the operation of the Federation and (2) the operation of the FiXs Network.

A member in Good Standing is a member who is current with dues payment or other such fees as prescribed by the Federation and that upholds its explicit and implicit responsibilities related to membership in the Federation. Payment is expected within 60 days of invoice date and by the date of membership expiration. The Federation may from time-to-time waive initiation fees for full members and/or allow for installment payment of dues as deemed necessary by the Board in order to increase participation in the Federation.

A new member shall obtain Good Standing in the Federation upon the acceptance of its membership application by the Federation as specified in Article II, Sections 5-6 and its’ payment of any applicable dues or fees.

Should a member’s dues not be paid by their renewal date, their membership shall be immediately suspended and the member shall be precluded from voting on any issue. Further, any person from the member who holds an officer position or other position of leadership in the organization shall forfeit their leadership position for the remainder of their term. Should the member’s dues be received within 30 days after the renewal due date, the membership shall be re-instated and their voting privileges restored without having to re-apply for membership.

The Chief Executive Officer of the Federation may grant extensions to the payment due date, or a grace period, on an exceptional basis and under extenuating circumstances of up to 14 days. No member shall be granted more than 1 grace period extension.

Article IV: Membership Forum and Meetings

1. ***Membership Forum Meetings.*** The Membership Forum shall be comprised of Federation members and Government Advisors, as specified in Article II, Section 2. The Federation shall conduct at least three general Membership Forum meetings a calendar year and may meet more often as is necessary. The time and place of these meetings will be determined by the President of the Federation.
 - a. **Attendance at meetings.** Attendance at Membership Forum meetings shall be limited to:
 - (1) Founding Members of the Federation, who may each invite two guests.
 - (2) Full Members of the Federation, who may each invite two guests.
 - (3) Associate Members of the Federation.
 - (4) Sole Proprietor Members of the Federation.
 - (5) Association and Not-For-Profit Members of the Federation.
 - (6) Government advisors.
 - (7) Federation staff.
 - (8) Guests invited by the Federation President.
 - (9) Legal counsel designated by the President.
 - b. **Means of Meeting.** Any member of the Federation or of any Committee, Subcommittee or Work Group thereof, may participate in a meeting by means of conference telephone or similar communication equipment by means of which all persons participating in the meeting hear each other, and participation in a meeting by such means shall constitute presence in person at such meeting.
2. **Membership Forum Members and Rights.**
 - a. **Founding Members.** Founding Members in Good Standing are members in perpetuity and shall be entitled to appoint a representative to a seat on the Board of Directors. Founding Members shall be eligible to: (1) vote on issues before the Board of Directors; (2) vote on members of the Board of Directors that are subject to election; (3) vote on any

issue before the Membership Forum, or a Committee, Subcommittee or Work Group of the Membership Forum; (4) chair a Committee or Work Group; and (5) approve amendments to the Bylaws.

- b. *Full Members.* Full Members shall be eligible to: (1) be elected to the Board of Directors; (2) vote on members of the Board of Directors; (3) vote on any issue before the Membership Forum, or a Committee, Subcommittee or Work Group of the Membership Forum; (4) chair a Committee or Work Group; and (5) participate in other activities not reserved for the Board of Directors under the Federation's Bylaws.
 - c. *Association and Not-for Profit Members.* Association and Not-For Profit Members are entitled to: (1) vote on members of the Board of Directors; (2) vote on any issue before the Membership Forum, or a Committee, Subcommittee or Work Group of the Membership Forum; and (3) participate in other activities not reserved for the Board of Directors under the Federation's Bylaws.
 - d. *Associate Members.* An Associate Member is not entitled to vote, but may participate in the Membership Forum and a Committee, Subcommittee or Work Group of the Membership Forum.
 - e. *Sole Proprietor Members.* A Sole Proprietor Member is not entitled to vote, but may participate in the Membership Forum and a Committee or Work Group of the Membership Forum. However, on a case-by-case basis, the Executive Committee may vote to make a Sole Proprietor Member eligible to: (1) be elected to the Board of Directors; (2) vote on members of the Board of Directors; (3) vote on any issue before the Membership Forum, or a Committee, Subcommittee or Work Group of the Membership Forum; (4) chair a Committee or Work Group; and (5) participate in other activities not reserved for the Board of Directors under the Federation's Bylaws. If a sole proprietorship experiences a change of control, the Executive Committee reserves the right to reevaluate the membership status of such sole proprietorship and to re-determine membership status and any positions then held.
 - f. *Government Advisors.* A Government Advisor is not entitled to vote, but may participate in the Membership Forum and a Committee or Work Group of the Membership Forum.
3. *Quorum of Members.* The presence in person or by proxy of fifty percent of the voting members shall constitute a quorum for the purpose of transacting Federation business at Membership Forum meetings, or at Committee, Subcommittee or Work Group meetings. A simple majority of votes cast by members' present carries any action except where provided otherwise by law or by these Bylaws.
 4. *Voting Procedures.* Voting may take place in person or by proxy provided by advance written notice. Votes may also be cast orally via conference call or via email either during or after a conference call. The Board of Directors may modify procedures for voting

within the Federation based upon unusual or unique circumstances should they be in the best interests of the Federation.

Article V: Board of Directors

The Board of Directors shall manage the activities of the Federation.

1. *Duties.* The Board of Directors shall:

- a. Vote on and approve the foundational documents, including the Bylaws (as specified in Article IX), the Trust Statement, the FiXs Policy, the Rules and the Technical Architecture and Specifications, and any amendments thereto.
- b. Develop, approve and maintain an annual business plan and budget for the Federation.
- c. Define and oversee the strategic direction of: the FiXs Network and Network Service Provider(s); Member Services Providers; Credential Issuers; and the Certification and Accreditation (C&A) and Authorization to Operate (ATO) processes, and the organization(s) responsible for these processes.
- d. Assign responsibility for the day-to-day operations of the Network to the Officers of the Federation with oversight and advice from the Executive Committee as provided for in Articles VI and VII.
- e. Remove members of the Board of Directors (Directors).

2. *Composition.* The Board of Directors shall be comprised of one representative designated by each of the Founding Member organizations and additional members elected from among the Full Members by all voting members, for a total not to exceed twenty-five voting members. Up to five Government Advisors selected by the Board of Directors may participate in meetings of the Board of Directors, but shall not have fiduciary duties or a vote on Board issues. Membership on the Board of Directors is on an organizational or corporate basis, not on an individual basis. The nominating subcommittee of the Membership Committee shall prepare a slate of: 1) members subject to election and 2) up to five Government Advisors. A nomination does not have to be made for each open seat, as the Board may have fewer than 25 members. The slate shall seek to achieve a balance of companies or organizations based on size and type of business or affiliation. The slate shall be prepared on behalf of the Board of Directors, which may modify the slate before approving it. The organization or company that a Director represents may appoint an alternate (the "Alternate Director") to serve in the capacity of Director in the event of the absence of the Director. When serving in the capacity of Director, the Alternate Director shall have all the rights, privileges and fiduciary duties and responsibilities of the Director. The words "Director" or "Directors" shall also include "Alternate Director or Directors" as applicable.

The President may, at his discretion, appoint a new member/applicant to fill any vacancy on the Board of Directors for a one-year term, without requiring voting by the Full Membership.

3. *Voting, Remote Participation, Informal Action.*

- a. Each Founding Member Representative on the Board of Directors shall have two (2) votes, and each Full Member Representative shall have one (1) vote, with respect to any matter that comes before the Board of Directors.
 - b. Members of the Board of Directors may participate in meetings of the Board of Directors by means of a telephonic conference call or by similar means of communication, provided that all persons participating in any such meeting can simultaneously hear and speak to each other. A director's participation in a meeting of the Board of Directors by the foregoing means shall constitute such director's presence in person at such meeting. The Board of Directors may take action by a majority of the votes cast at a meeting at which a quorum is present.
 - c. Any action required or permitted to be taken at any meeting of the Board of Directors may be taken without a meeting, if consent in writing to such action is signed by each director and such written consent is filed with the minutes of the proceedings of the Board of Directors. A director may submit his or her signature to a written consent executed in accordance with this Section by facsimile transmission or similar means of communication (e.g., a pdf file), provided that such director retains a copy of the original signature page for future reference. A consent executed in accordance with this Section has the effect of a meeting vote and may be described as such in any document.
4. *Term of Office.* Each member of the Board of Directors, other than the Founding members in Good Standing, shall serve two-year terms, except that half of the initial Board members taking office after January 1, 2006, shall serve one-year-terms to achieve staggered terms. The Board of Directors shall determine how those with one-year terms shall be selected.
5. *Vacancies.* If any vacancy occurs on the Board of Directors before the expiration of a term, the member organization holding the seat shall appoint a replacement subject to confirmation by the Board of Directors. If this appointment does not occur within 30 days of the vacancy occurring, the Board of Directors may determine the manner in which this vacancy shall be filled.
6. *Meetings.* The Board of Directors shall meet at least three times per year and may meet more often as is necessary. Meetings of the Board of Directors shall be called by the President. Meetings shall be limited to Board of Directors members, FiXs or secretariat staff, legal counsel designated by the Board of Directors, and guests invited by the President.
7. *Quorum and Vote of the Board of Directors.* The presence in person of fifty percent of the Board of Directors members shall constitute a quorum for the purpose of transacting Federation business at meetings of the Board of Directors. A simple majority of votes cast by "members present" carries any action.

8. *Removal*. Other than Directors representing Founding Members, a Director may be removed for cause by a majority of votes cast by the standing Board of Directors. Directors shall be automatically removed for missing three (3) or more meetings in a twelve (12) month period or because the director is no longer a member in Good Standing as defined by the Membership Committee.
9. *Compensation*. Members of the Board of Directors do not receive compensation from the Federation for their services on the Board.

Article VI: Officers and Staff of the Federation

1. *Officers*. Officers shall be elected from among the members of the Board of Directors. The following officers shall perform those duties that are usual to their positions. These offices are held by the individuals rather than the organization they represent. The offices of Secretary and Treasurer may be combined.
 - a. President. The President shall serve as the Chief Executive Officer of the Federation and shall be Chair of the Board of Directors. The President presides at meetings of the Board of Directors and the membership. The President has responsibilities for the activities and programs of the Federation and has the authority to make expenditures and execute contracts on behalf of the Federation.
 - b. Vice President. The Vice President shall also serve as Vice Chair of the Board of Directors.
 - c. Secretary. The Secretary shall also serve as the Secretary of the Board of Directors.
 - d. Treasurer. The Treasurer shall also serve as Treasurer of the Board of Directors.
2. *Election of Officers*. Upon the expiration of initial terms, officers shall be elected by voting members of the Federation. The nominating subcommittee of the Membership Committee shall develop a slate of officers for President, Vice President, Secretary and Treasurer.
3. *Terms*. Unless otherwise stated herein, officers shall be selected for a term of two years. The Officers commitment may extend a Board of Directors member's term into a third year.
4. *Staff Positions*. Subject to approval by the Board of Directors, the President may hire the following staff:
 - a. *Chief Operating Officer*. The Chief Operating Officer shall have responsibility for overseeing the operation of the FiXs Network.

- b. *Chief Technology Officer.* The chief technology officer shall have responsibility for the development of new FiXs service offerings.
 - c. *Chief Financial Officer.* The Chief Financial Officer shall oversee all accounting and payment functions for the Federation and shall prepare monthly financial statements. This position shall oversee adherence to the long range financial plan prepared by the Strategy, Business, and Finance Committee and approved by the Board of Directors.
 - d. Other staff as necessary.
5. Compensation. The Board of Directors shall determine appropriate compensation, if any, for officers.
 6. Vacancies. If any vacancy occurs in an office before expiration of a term, an election shall be conducted to fill the officer's unexpired term.

Article VII: Committees, Sub-Committees, Boards and Working Groups of the Federation

The overriding objective of all committees is to maintain the viability of the Federation and interoperability of the FiXs Network and its certified products and services. Each standing committee must be chaired by a member of the Board of Directors, who shall be appointed by the FiXs President. The FiXs President may also appoint a vice chairperson for each committee. The organization or company that a committee member is employed by, or represents, may designate in writing an alternate member, with the same duties and responsibilities, to vote on matters before the Committee at any meeting that the regular committee member cannot attend. There are two types of committees: 1) Committee of the Board of Directors and 2) Committees of the Membership Forum.

1. Committees of the Board of Directors. The following standing committees are limited to members of the Board of Directors. Any member of the Board of Directors may volunteer to serve on these committees. Board members may co-chair the sub-committees of the Board along with the assigned co-chair FiXs Officers.
 - a. Executive Committee. This Committee is responsible for day-to-day operations of the Federation and the Network; for advising the President; and for making recommendations on decisions requiring action by the Board of Directors. This committee shall also prepare and facilitate resolution of and recommendation for agenda items going to the full Board of Directors. The Committee will oversee the implementation of actions voted on by the Board of Directors. This committee is comprised of: the officers; a representative of each Member Service Provider or Credential Issuer; a representative of each Network Service Provider; a representative of each certified independent third party assessor; and others appointed by the President. The President may invite guests to participate on this committee. This committee is chaired by the President and shall meet

at the discretion of the President. The following subcommittees shall report to the Executive Committee:

(1) Legal and Policy Subcommittee. This sub-committee has jurisdiction over the FiXs By-Laws; FiXs Trust Model; FiXs Policy Document, and legal, contractual and privacy matters. This committee shall develop a plan to register, protect, and manage the FiXs service mark(s) and intellectual property of the Federation.

The Legal and Policy Sub-Committee shall coordinate with all other sub-committees, boards or working groups on matters of mutual interest. The Board of Directors must approve modifications to the FiXs By-Laws; FiXs Trust Model, and FiXs Policy Document. This sub-committee will have a co-chair that is the FiXs Corporate Secretary.

(2) The Change Control Board (CCB). The CCB shall be responsible for maintaining the technical specifications and interface configurations that constitute the make-up of the FiXs Network. The CCB will also maintain the FiXs Technical Architecture and Specifications document and shall be responsible for the technical development and modification of FiXs certified products and services, to include the oversight of development efforts and maintenance of software; site, product, service and security certification requirements thru the FiXs test and lab environment. The CCB will also maintain the Certification and Assessment (C&A) processes and the C&A matrices approved by the Executive Committee. The CCB shall develop policies and practices for the security of the FiXs Network in keeping with government requirements and industry best practices. It shall maintain the FiXs Security Policy.

The CCB reports directly to the Executive Committee for recommendations on necessary implementation of changes that affect day to day operations of the Network; C&A and Security matters; approved products or services; and test and lab matters. The CCB will coordinate with all other sub-committees that have impact on matters under its jurisdiction. The CCB will have a co-chair that is the FiXs Vice President.

(3) Federation Strategy, Business, and Finance Subcommittee. This subcommittee shall develop and oversee the execution of a business plan to finance the long-term operation of the Federation (and any operating entity (ies) if established). This subcommittee shall also recommend appropriate compensation for officers and staff. For the operational FiXs Network, this sub-committee shall also develop and maintain the criteria for use and display of the service mark and evaluate alternative revenue models.. This sub-committee will have a co-chair that is the FiXs Treasurer.

(4) Operating Rules and Guidelines Subcommittee. This subcommittee has responsibility for the FiXs Operating Rules and FiXs Implementation Guidelines for both the physical and logical use of “FiXs-Certified Credentials”. These documents cover all matters affecting organizational and individual vetting procedures; enrollment processes; documentation; issuance; maintenance; and revocation of “FiXs-Certified Credentials” issued by an MSP or Credential Issuer for use on the FiXs Network and other interoperable Networks to which

FiXs has established interface protocols. This subcommittee must continually coordinate with the Legal and Policy subcommittee, and the CCB, to ensure consistency with other processes, procedures and legal requirements of the Federation.

(5) *Elections and Membership Subcommittee*. The committee shall have responsibility for nominating, vetting and preparing the recommended slate of nominees for the annual election of members to the Board of Directors from eligible full members. This election shall take place by January 31st of each year. The newly elected Board will be seated as of the succeeding May 1st after the election. This subcommittee shall also recommend any Government Advisors to the Board from Federal, State and Local agencies and jurisdictions. This subcommittee will also vet and prepare a slate of nominees for election of Officers of the Federation, per the cycle as prescribed by these By-Laws.

This committee shall also develop and execute a plan for membership recruitment and management and shall develop policies and practices for the acceptance of new Federation members. It shall deal with member benefits; parameters for a member in Good Standing and termination criteria for Full Members and other member classifications. This committee shall report to the Executive Committee.

Committees of the Membership Forum. The following standing committees are open to members of the Membership Forum, as described in Article IV, Section 3 of these Bylaws. Recommendations of these committees will be subject to review by the Membership Forum and will then be considered for adoption by the Board of Directors:

(1) *Governance and Standards Committee.* This committee shall have the responsibility for soliciting and collating the collective views, priorities, and issues of the general membership and user population and presenting them in a prioritized and concise manner to the Executive Committee for consideration and possible adoption. The Executive Committee will assign the recommendations to the appropriate Board Subcommittee for further vetting and preparation prior to presentation to the full Board for review and possible vote.--

(2) *Education and Public Affairs Committee.* This committee shall develop educational and promotional materials about FiXs. Inputs on topics and areas of focus will be accepted from the general membership as well as the full and associate members of the Federation.

Additional Committees. The Board of Directors may create additional committees to deal with issues of ongoing concern to the Federation or to the FiXs Network. As an example, the Certification and Accreditation Subcommittee will be established from time to time to address merging requirements.

Article VIII: Work Groups

1. *Creation and Purpose.* Work Groups are ad hoc groups created by any standing committee, the Membership Forum, or the Board of Directors. The purpose of a Work Group is to address a particular issue that is of concern to the Committee, the Membership Forum or the Board of Directors.
2. *Work Group Chairperson.* A Work Group shall have a chairperson, who shall be a founding or full member appointed by the President or chairperson of the body that created it.
3. *Composition.* Work Groups are composed of members of the Membership Forum, as described in Article IV, Section 3 of these Bylaws. The Work Group Chairperson may invite non-Federation members to participate in a work group if their participation will contribute to resolution of the issue at hand. The organization or company that a Work Group member is employed by or represents may designate an alternate member, with the same duties and responsibilities, to vote on matters before the Work Group at any meeting that the regular member cannot attend.

Article IX: Amendments to the Bylaws and Limitation of Liability

1. *Amendments.* Amendments to these Bylaws may be made at any meeting of the Board of Directors by a majority of the members present and voting. Notice of the proposed amendments shall be provided to all Board of Directors members at least fifteen calendar days in advance of the vote.
2. *Release.* In consideration for the opportunity to join and participate in the Federation, each member organization, company, and representative waives and discharges any and all rights that the member or any of its affiliates may now or in the future have to pursue any right, claim or cause of action, enforcement of any obligation or liability to it, recovery of any loss or other damage, or any other form of relief, by litigation, arbitration or any other means, resulting from any action or inaction of such person(s) in connection with activities of the Federation. In the event a member resigns from or otherwise terminates its membership on the Federation, this waiver shall continue indefinitely in full force and effect with respect to any such action or inaction occurring while such former member was a member of the Federation.
3. *Severability of Provisions.* Each provision of these Bylaws shall be incorporated in such a manner as to be effective and valid under applicable law. In the event that any one or more of the provisions of these Bylaws shall be held to be invalid, illegal or unenforceable, the remaining provisions of these Bylaws shall not be affected or impaired thereby.

4. *Housekeeping.* The Bylaws may be edited from time-to-time to provide consistency and accuracy with other approved governance documents and actions, and to address grammatical errors, without formal action of the Board of Directors through an amendment to the Bylaws. Any such editorial changes or revisions must be thoroughly documented as to the nature and necessity of the change and be reviewed and formally approved by all Officers of the Federation. The Bylaws will be annotated by sequential revision numbers (i.e. 2.2, 2.3 etc.) each time any such edit or revision is made. A summary of all such edits and revisions previously performed will be provided to each current member of the Board of Directors prior to each routinely scheduled Board Meeting.
-

Revision History

Version	Date	Comments
1.0	April 13, 2004	First Charter unanimously approved.
1.1	May 10, 2004	Changes primarily reflect DoD's interest in being a Federal advisor, rather than a member of the Council
1.2	February 11, 2005	Changes reflect changes made by the Board of Directors with regard to: the Initial Phase (adopted on October 4, 2004); the name change adopted in November 2004 for filing the Articles of Incorporation; and the addition of the Security Committee on February 11, 2005.
1.3	April 25, 2005	Modified to include individual members, to begin dues assessment on July 1, 2005, and to provide for terms of initial co-chairs.
1.4	July 28, 2005	Modified to address intellectual property; appointment of officers; ownership of the Federation; create Association members; and to make additional changes.
1.5	October 27, 2005	Housekeeping changes made for internal consistency.
1.6	December 15, 2005	Major rewrite to remove the initial phase from the Bylaws and clarify of membership and committees for the operational phase.
1.7	February 3, 2006	Revisions made to incorporate Counsel's recommended changes to ensure compliance with Virginia law.
1.9	October 16, 2006	Revisions made to clarify that all members understand and follow FiXs' intellectual property and anti-trust policies. Revisions made to amend the definition of sole proprietorship from fewer than three employees to fewer than ten and to become full members.
2.0	November 7, 2006	Revisions made to clarify tax status, ownership, participation based on general counsel's recommendations.
2.1	July 30, 2007	Revisions made to change correct address; clarify and revise Article I: Nature - Purposes/Objectives consistent with FiXs standards setting and network oversight roles, tax and regulatory guidance; incorporate four Bylaws amendments passed by the Board dealing with Article III: Dues Payments; Article IV - Membership Transfer; Article II – Membership Transfer; and Article IX - Housekeeping
2.2	November 26, 2007	Revisions made to replace original Article III: Dues Payments with Board-approved language regarding payment due dates and penalties for late payment. Additional minor revisions of a housekeeping nature intended to clarify or correct original text.
2.3	May 8, 2008	Revised Proviso at end of the Bylaws dealing with Board of

		Directors Composition reflecting unanimous vote of the Board granting the President the authority to appoint new Directors to the Board should there be any vacancy up until April, 30 2009.
2.4	July 10, 2008	Revised Article VII to update FiXs committees structure
2.5	January 28, 2010	Revised Article II. based on BoD voted changes to add a membership sub-category of “Association acting as Portal”, membership and membership dues payment; Article III. Based on Board vote to allow waiver of initiation fees and allow dues payments based on installment payments; Article V. to make permanent the FiXs President’s ability to appoint new members to fill vacant Board seats; and, Article VI. to remove language dealing with “Interim Officers” as this period has passed and the language now irrelevant.
3.0	September 1, 2010	Editorial changes. Synch with DoD/DMDC baseline versions 3.0



The Federation for Identity and
Cross-Credentialing Systems®

FIXs® OPERATING RULES

Version 3.3

September 15, 2010

www.fixs.org

Copyright 2010 by the Federation for Identity and Cross-Credentialing Systems, Inc.

All Rights Reserved

Printed in the United States of America

10400 Eaton Place, Suite 500A

Fairfax, VA 22030

(703) 591-9255

Table of Contents

1 GENERAL REQUIREMENTS AND DEFINITIONS.....	12
1.1 Personnel Definitions and Requirements	14
1.1.1 Program Manager	15
1.1.2 Enrollment Personnel Requirements.....	16
1.1.3 Authentication Personnel Requirements	17
1.2 Systems Facility Definitions and Requirements	18
1.2.1 FiXs®-Certified Trust Broker (FTB) Interface Requirements	18
1.2.2 System Assessment.....	18
1.2.3 Credential Issuer Operational Requirements	19
1.2.4 FiXs® Domain System Requirements	21
1.2.5 Relying Party Operational Requirements	22
1.2.6 Member Service Provider Requirements.....	24
1.2.7 Records/Files Maintenance Requirements.....	25
1.3 Logical Authentication.....	26
1.4 Level 1 (FiXs® equivalent “Low”)	26
1.5 Level 2 (FiXs® equivalent “Medium”)	26
1.6 Levels 3 (FiXs® equivalent “Medium High”)	26
1.7 Level 4, (FiXs® equivalent “High”)	27
1.8 Framework	27
1.9 Certificate Validation.....	27
1.10 FiXs® Logical Trust Model	27
1.10.1 DoD PKI	28
1.10.2 Federal PKI common Policy Framework (FPCPF).....	29
1.10.3 Federal Bridge Certification Authority (FBCA)	29
1.11 Certificate Profile	30

1.11.1	FiXs® Person Designator Identifier (PDI).....	30
1.11.2	FiXs® Assurance Level	31
2	FIXS®-CERTIFIED CREDENTIAL ISSUANCE.....	32
2.1	Credential Issuance	32
2.1.1	Validate Applicant’s need for FiXs® Credentials	32
2.1.2	Verify Applicant Identification (Vetting/Identity Proofing)	32
2.1.3	Verification Process Requirements.....	33
2.1.4	Enroll Applicant Into FiXs®-Certified System	34
2.1.5	Issue Participant Valid FiXs® Identifier.....	35
2.1.6	Appeals Process	36
2.2	Transaction Request Processing.....	36
2.2.1	Processing Authentication Inquiries	37
2.2.2	Initiating Authentication Responses	37
2.3	CERTIFICATE ISSUANCE.....	37
2.4	Certificate Practice Statement	38
2.5	Registration Practice Statement	38
2.6	Life Cycle Technical Controls.....	39
2.6.1	Physical Safeguards.....	40
2.6.2	Access Controls	40
2.6.3	Equipment.....	40
2.6.4	Upgrades.....	40
2.6.5	Development Environment Security.....	40
2.6.6	Configuration Management Security.....	40
2.6.7	Network Security Controls.....	40
2.7	Uniqueness Across the FiXs®-Certified Network	40
3	SPONSORING ORGANIZATIONS INTO THE FIXS®-CERTIFIED NETWORK	42
3.1	Vetting.....	42

3.2 Sponsorship of Employees.....	42
3.3 Adhere to FiXs® Foundational Documents.....	42
4 RELYING PARTY RESPONSIBILITIES.....	45
4.1 Visitor Transaction Processing	45
4.1.1 Credential Validation and Transaction Routing.....	45
4.1.2 Processing Authentication Responses	47
4.2 Exception Processing.....	47
4.2.1 Badge/Token-Not-Present	47
4.2.2 Other Exceptions.....	48
4.3 Application Provisioning.....	48
4.3.1 TRUST DETERMINATION TECHNIQUES AND PARAMETERS	48
4.3.2 ENABLE APPLICATION AUTHENTICATION	49
4.3.3 User Repository/ Privilege Management.....	49
4.3.4 Digital Signatures and Storage Considerations.....	52
4.4 Documenting Compliance.....	52
4.4.1 Identity/Qualifications of Compliance Auditor.....	52
4.4.2 Compliance Auditor’s Relationship to Audited Party	52
4.4.3 LIFE CYCLE MANAGEMENT STRATEGY	53
5 FIXS®-CERTIFIED TRUST BROKER (FTB) RESPONSIBILITIES	54
5.1 System Administration Requirements.....	54
5.1.1 Designate FTB System Administrator	54
5.1.2 Member Interface Management	54
5.1.3 Maintenance of Control Data	54
5.1.4 Activation and De-Activation of FiXs®-Certified Domains	54
5.1.5 System Performance Requirements	56
5.2 Transaction Processing and Routing.....	56
5.2.1 Authentication Inquiries	56
5.2.2 Authentication Responses	56

5.2.3	Audit Control Data Transactions.....	56
5.3	FIXS®-CERTIFIED CERTIFICATE VALIDATION	56
5.4	TRUST DETERMINATION.....	57
5.4.1	Path-Based Trust.....	58
5.4.2	Validation Protocols.....	58
5.4.3	Other Trust Determination Techniques.....	58
5.4.4	Checking Certificate Revocation List.....	58
5.4.5	Online Certificate Status Check	59
5.4.6	Standard Certificate Validation Protocol (SCVP)	59
5.4.7	Fully PD-Val Capable Web Servers.....	60
5.4.8	Other Techniques and Protocols	60
5.5	OCSP Responder Self-Signed Certificate	60
5.6	OCSP Responder Certificate.....	61
5.7	OCSP Request Format.....	61
5.8	OCSP Response Format	61
6	SECURITY REQUIREMENTS	63
6.1	General Security Requirements	63
6.2	Infrastructure Requirements	63
6.3	Audit Requirements	63
6.4	Security Authorizations	63
6.4.1	General.....	63
6.4.2	Domain Technical Administrator	63
6.4.3	Domain Functional Administrator	64
6.4.4	Facility Domain Administrators.....	64
6.4.5	Facility Administrative Enroller.....	64
7	LIABILITIES AND INDEMNIFICATION	65

7.1	Liability under these Rules.....	65
7.2	Liability to Members and Participants.....	65
8	PRIVACY	66
8.1	Privacy.....	66
8.1.1	Badge/Token-Not-Present	66
8.1.2	Other Exceptions.....	66
9	FIXS® GOVERNANCE.....	67
9.1	FiXs® Business Requirements.....	67
9.1.1	Establish FiXs® Member Partnership Agreement(s)	67
9.1.2	Effect of Rules	67
9.2	Public Statements	67
10	MEMBERSHIP APPROVAL, AUTHORIZATION TO OPERATE AND COMPLIANCE MONITORING	68
10.1	Summary	68
10.2	Vetting Requirements for Member Organizations	72
10.2.1	Application for membership	72
10.2.2	Membership Review and Approval Process	72
10.2.3	Certification of Authorization to Operate.....	72
11	MISCELLANEOUS.....	75
11.1	Voluntary Termination of Members	75
11.2	Amendment to These Rules	75
12	DEFINITIONS.....	76
13	REFERENCES	85
14	REVISION HISTORY.....	97

FIXS® OPERATING RULES

Background

The Federation for Identity and Cross-Credentialing Systems® (FiXs®) is a not-for-profit 501c(6) trade association comprised of a coalition of industry and public sector organizations whose objective is to support efforts to develop standards supporting the creation and deployment of a secure interoperable identity cross-credentialing network. These Operating Rules define the rights, responsibilities and liabilities of FiXs® Member Organizations and those parties using FiXs®-Certified Credentials or supporting components of the FiXs®-Certified Network. The Rules are a part of a larger package of documents that lay the foundation for “trust” in the FiXs® Network. The other documents, known as the FiXs® Foundational Documents, include:

- The Trust Model;
- FiXs® Policy;
- Implementation Guidelines;
- The Technical Architecture and Specifications; and
- Security Guidelines.

The FiXs®-Certified Network provides a highly-scalable, secure, auditable solution set, whereby FiXs® Member Organizations and relying parties can authenticate and validate FiXs®-Certified Credentials issued to users from other participating organizations, or “Subscribers”, as well as authenticate the credentials issued by other related organizations (i.e. cross-credential). FiXs® relies on a Federated Model of Trust, which is discussed more fully in the FiXs® Trust Model. The federated identity model establishes trust between member organizations through the use of agreements, standards and technologies that make identity credential” portable across the organizations.

Initially, FiXs® established a trusted relationship between certain FiXs® Member Organizations and the Department of Defense (DoD), Defense Cross-Credentialing Identification System (DCCIS). The federation enabled participating DoD and industry facilities to achieve strong, and interoperable, identity verification and authentication of participating contractor/private sector personnel who present a company-issued trusted credential (i.e. FiXs®-Certified Credential). Similarly, participating industry locations also recognize a DoD-issued Common Access Card (CAC) and the Defense Biometric Identity System (DBIDS) credential, which required no modifications in order to operate with the FiXs® and DCCIS networks.

FiXs®, which is the only organization currently authorized to inter-operate a cross-credentialing system with DoD and can use its federated system to enable other government agencies, first responders, and industry partners to verify the identity of individuals who seek access to their physical or logical assets in either the government or commercial environment.

In a federated system each subscribing or participating organization maintains or controls its own data store of enrolled member data (“participants”) that the organization has sponsored. Privacy and security are maintained because minimal identity information is held centrally or maintained in the infrastructure except in the employee’s host organization domain server.

At the present time the Federal Government has defined four recognized levels of credentials

and/or trust. It is generally accepted that each level is defined by two distinct processes; one that defines the vetting process that is accomplished prior to a credential being issued; and the second defines the standards for the data, and its placement on the credential, and the standards and specifications for the credential/card itself. *FiXs® has chosen to use a FIPS 201 compliant smart card specifications for all Levels of Trust. Thus, the main differentiation between the levels is primarily with the vetting process, documentation/verification, and biometric data collected, verified and maintained in the federated data model. This version of the FiXs® Operating Rules extend that paradigm into Logical Access functionality.*

These FiXs® Operating Rules match logical access certified credentials will also contain the appropriate data designating under which Level of Trust the credential was issued and classified.

The current Government sanctioned nomenclature for “Levels” is numerical (i.e. 4, 3, 2, 1) and described below. FiXs® attempts to define these levels with a verbal designation of Trust Levels which offers its customers a descriptive context associated by level. Therefore, the remainder of this document and the accompanying guidelines, as specified by the Federal Government. For the highest levels of assurance, the FiXs®-Certified Credential shall hold and protect digital certificates that have been established and are certified to inter-operate with the Federal Government. Thereby, combining its federated system to enable other government agencies, first responders, and industry partners to reliably authenticate the identity of individuals who seek access to both physical and logical assets in either the government or commercial environment. In all cases however, the privileges or authorities actually granted is a decision of the cognizant system owner/manager.

At the present time the Federal Government has defined four recognized levels of credentials and/or trust. It is generally accepted that each level is defined by three distinct processes; one that defines the vetting process that is accomplished prior to a credential being issued; the second defines the standards for the data, and its placement on the credential, and the standards and specifications for the credential/card itself; and the third defines the chain of trust and accountability of these process (the subject of this document).

FiXs® standards entail the use the FIPS 201 compliant smart card specifications for all Levels of Trust. Thus, the differentiation between the levels is primarily with the vetting process, documentation/ verification, and biometric data collected, verified and maintained in the federated data model; as well as the life cycle management of the digital certificate and private keys issued to and protected by the credential. FiXs®-Certified Credentials also contain the appropriate data designating under which Level of Trust the credential was issued and classified.

The current Government sanctioned nomenclature for “Levels” is numerical (i.e. 1, 2, 3, & 4) and described below. FiXs® correlates these document will offer a corollary verbal description of levels to equate to the numerical levels with a textual designation of Trust Level that provides a descriptive context associated by each level. Therefore, the remainder of this document and the accompanying Guideline documents will provide a corollary textual description of levels to equate to the standard government numerical designation:

“High Trust” = 4; “Medium High Trust” = 3; “Medium Trust” = 2”; and “Low Trust”= 1”

Level 1 (FiXs® equivalent “Low”). This level (if required) is currently considered an

unacceptable level of trust for official Federal Government use purposes. FiXs® assigns the Low Level Trust (Level 1) the working definition of: a level of assurance that requires minimal proof of identity but no background check, and no document verification, therefore, it provides little or no level of trust assurance.

FiXs®-Certified Credential Issuers are not permitted to enroll Users at a Low Trust Level (1); load any data into a FiXs®-Certified Domain Server; nor attempt to authenticate such credentials across the FiXs®-Certified Network.

Examples of a Low Level (1) credentials are shopper discount cards and public email accounts. Because these “credentials” may be granted by non-FiXs® Members or Subscribers without any kind of identity verification, FiXs® Members or Subscribers are cautioned against granting rights to a bearer.

At a future date FiXs® may assess the validity, requirements, and resources required for this level of credential. The Level I – “Low” is not used currently.

The FiXs® Medium Trust Level (Level 2) applies to a level of assurance required by a specific implementation. This will require a background check, using commercially available sources of data, and fingerprints will be collected digitally at time of enrollment, solely for the purpose of linking to the issued credential. At this level the fingerprints **will not** be sent to the FBI for a National Criminal History Fingerprint Check.

The Medium Level may suit those commercial vendors who may require frequent access to facilities in order to provide deliveries; or stock shelves/vending machines; or provides maintenance services. This Medium Level may provide adequate acceptable risk for granting local privileges at lower threat levels, but may not be acceptable as threat levels rise. This level may also be used to accommodate persons who may temporarily work in positions of public trust, such as certain categories of first responders, health care workers or volunteers who help out at a disaster scene (i.e., Red Cross and other volunteers; public works employees; emergency technicians, etc.). The Medium Level credential can also be used for Commercial applications.

This level is intended for applications handling sensitive medium value information based on the relying party’s assessment, with the exception of transactions involving issuance or acceptance of contracts and contract modifications. Examples of medium assurance applications include:

- Non-repudiation for small and medium value financial transactions other than transactions involving issuance or acceptance of contracts and contract modifications
- Authorization of payment for small and medium value financial transactions
- Authorization of payment for small and medium value travel claims
- Authorization of payment for small and medium value payroll
- Acceptance of payment for small and medium value financial transactions

Level 3, (FiXs® equivalent “Medium High”) has not been defined by a Federal Directive or Policy at this point in time. FiXs® members and industry at-large, however, have a requirement for this level of credential and accordingly, FiXs® has developed standards to comply with this requirement and proposes these Guidelines to the Federal Government for consideration and adoption. FiXs®-Certified Credentials certified at Level 3 are aligned with PIV II (as defined in the FiXs® Operating Rules), but differ from PIV I provisions relating to the enrollment process.

The vetting and issuance process mirror the process performed by the Federal Government for a Level 4 credential with the exception of the use of commercial sources instead of having the involvement of the Office of Personnel Management (OPM). Accordingly, this assurance level of credential is considered as the “commercial equivalent” of the Level 4 credential. For logical access control purposes, the digital credential created and protected in this environment shall carry a medium hardware assertion. The DoD has defined this as “Medium Hardware Assurance” and General Services Administration (GSA) has designated this as “Common Hardware”.

Level 4, (FiXs® equivalent “High”) is aligned with Homeland Security Presidential Directive 12 (HSPD 12). HSPD 12, dated August 27, 2004, entitled “Policy for a Common Identification Standard for Federal Employees and Contractors” which directed promulgation of a federal standard for secure and reliable forms of identification for federal employees and contractors. In March 2006, the National Institutes of Standards and Technology (NIST) issued Federal Information Processing Standards 201 (FIPS 201) for Personal Identity Verification (PIV) of federal employees and contractors. The PIV standard consists of two parts – PIV-I and PIV-II. PIV-I satisfies control objectives, including enrollment requirements, of HSPD 12. PIV-II specifies implementation standards, including physical card characteristics, and use of identity credentials on integrated circuit cards for a federal personal identity verification systems. For logical access authentication purposes, a digital credential created and protected in this environment shall carry a hardware assertion. The DoD has defined this as “Medium Hardware Assurance” and GSA as “Common Hardware”.

Since Level 3 and 4, of “high” and “medium high assurance” credentials carry a hardware assertion, these logical credentials are available for all applications operating in environments appropriate for medium assurance but which require a higher degree of assurance and technical non-repudiation based on the relying party’s assessment. Examples include:

- All applications appropriate for medium assurance certificates
- Mobile code signing
- Applications performing contracting and contract modifications

The FiXs® Implementation Guidelines provides the specific requirements for the vetting of sponsored individuals requesting credentials in specific market/ functional venues. The accompanying Card Holder Unique Identifier (CHUID) section of the Guidelines deals with the specifics of the data and specifications of the card. Accordingly, these FiXs® Logical Operating Rules, the FiXs® Operating Rules and the FiXs® Implementation Guidelines are all complementary must be incorporated concurrently to implement FiXs® cross-credentialing physical and logical authentication services.

Historically, FiXs® has emulated many of its concepts and standards from the electronic payments industry. In the electronic payments industry, specific operating rules provide a uniform business and legal framework, as well as standard formats, for the exchange of financial payments among and between a diverse group of institutions and individuals. To rely on the principles already established for the payments industry, NACHA – The Electronic Payments Association, or formally known as the National Automated Clearing House Association, assisted with its knowledge and experience in development of the FiXs® Operating Rules. FiXs® also adopts standards-based certificate validation protocols that provide a flexible, cost effective, and robust validation solution ideally suited to a wide range of client applications

in diverse operating environments. At the core of this validation solution is a sophisticated digital certificate status responder capable of servicing Online Certificate Status Protocol (OCSP), Server-based Certificate Validation Protocol (SCVP), or CRL requests for full or delta CRL downloads; providing mechanisms to obtain and manage CA Certificates, Certificate Revocation Lists (CRL), and CA issued listings of non-sequential certificate serial numbers to service requests.

It is recognized that processing, or authenticating, an individual's identity credential is largely analogous to processing a payment. FiXs® encourages maximum participation among industry at-large to adopt this common set of standards to create a consistent, seamless, and secure operational framework and avoid the disruption and risks of implementing differing internal practices and platforms. The overall objective is to establish a secure and interoperable "Chain of Trust" for all members (including contractors, delivery and repair personnel, transport workers, law enforcement, first responders and others, needing access to facilities).

The FiXs® Implementation Guidelines document provides the specific requirements for the vetting of sponsored individuals requesting credentials at levels 1-3, and in specific market/functional venues. The accompanying CHUID section of the Guidelines deals with the specifics of the data and specifications of the card. Thus, these Operating Rules and the Guidelines must be read in tandem to execute FiXs® cross-credentialing services.

Historically, FiXs® has borrowed many of its concepts from the electronic payments industry. In the electronic payments industry, specific operating rules provide a uniform business and legal framework, as well as standard formats, for the exchange of financial payments. To rely on the principles already established for the payments industry, NACHA – The Electronic Payments Association assisted with its knowledge and experience in development of the FiXs® and DCCIS Operating Rules.

Since processing an employee's credentials is analogous to processing a payment, the FiXs® Operating Rules for cross-credentialing, encourage maximum participation among participating members that would otherwise use differing internal practices and platforms. The objective is to establish a secure and interoperable "Chain of Trust" for all members (including contractors, delivery and repair personnel, transport workers, law enforcement, first responders and others, needing access to facilities).

1 GENERAL REQUIREMENTS AND DEFINITIONS

This Section defines the requirements that need to be met for performing FiXs® operations. It describes the general requirements associated with FiXs® Member Organizations as well as administrative and system requirements in their roles as FiXs®-Certified Credential Issuers, Primary Trusted Organizations (PTOs) and Relying Parties. A **FiXs® Member** or **Member Organization** is a company, agency, or organization that has submitted a Membership Application with the Federation for Identity and Cross-Credentialing Systems, Inc. to join FiXs® in a membership category, and has been approved by the FiXs® Board of Directors, in accordance with Section 9. **The Federation for Identity and Cross-Credentialing Systems, Inc. (FiXs®)** is the legal entity that manages membership and maintains the FiXs® Foundational Documents. (See Definitions for the precise meaning of all capitalized terms.)

The role of major governed by these Rules is described below. There are two processes that are fundamental to the issuance of FiXs®-Certified Credentials. The first process requires that an organization sponsor an individual Participant into the FiXs®-Certified Network and the second process involves issuing the Participant a FiXs®-Certified Credential and processing Authentication Inquiries from Relying Parties. In the case of an Issuer Sponsor, described below, both of these roles are performed by the same FiXs® Member Organization.

- A **Participant** refers to the individual employee or subcontractor of a Member Organization that qualifies to participate in the FiXs®-Certified System.
- A **Credential Issuer** is a FiXs® Member that issues a FiXs®-Certified Credential to FiXs® Participants and processes and responds to Authentication Inquiries. A Credential Issuer is not responsible for the acts and omissions of the Participants to whom it issues Credentials.
- A **Sponsor** is an organization that uses the services of an Issuer Sponsor to host its FiXs® operations and that sponsors Participants into the FiXs®-Certified Network. A sponsor is responsible for the acts and omission of the Participants that it sponsors. There are two kinds of Sponsors – Member Organizations and Non-Member Organizations. In this case, the Issuer Sponsor hosts the Sponsor's FDS and processes its FiXs® authentication transactions.
- An **Issuer Sponsor** is a FiXs®-Certified Credential Issuer that also sponsors Participants to whom it issues FiXs®-Certified Credentials. This means that an Issuer Sponsor is a Member Organization that is both a Credential Issuer and a Primary Trusted Organization.
- A **Relying Party** relies on the FiXs®-Certified to authenticate the identity of a Participant and/or initiates authentication inquiries to the FiXs®-Certified Credential Issuer and processes the responses in accordance with FiXs® Operating Rules.
- A **Primary Trusted Organization (PTO) or Subscriber** is a member organization that sponsors individual employees or contractual agents of the PTO/Subscriber who are to be issued a FiXs®-Certified Credential in accordance with all FiXs®-Certified Processes, and policies and that agrees to be responsible for the acts and omissions of employees or Contractual Agents. These organizations must agree to and execute the current FiXs® Terms of Use Agreement for use of such credentials.
- *The FiXs® Trust Broker* is the operational intermediary between FiXs®-Certified

Credential Issuers and Relying Parties that serves as the “switch” by processing Authentication Inquiries from Relying Parties to Credential Issuers and Authentication Responses from Credential Issuers to Relying Parties via the FiXs®-Certified Trust Broker.

Under the Federated Model of Trust XML messages and a system of servers are designed so that the Trust Brokers see *only* the data that they need. To ensure that is the case, the payload data of all XML transaction messages are encrypted, using the PKI certificates of the trusted end-point destination and the source domain servers. A trust broker serves as a single, centralized, and authoritative holder for the list of sites that are considered to be “trusted” FiXs® members.

Organizations are likely to join FiXs® for various reasons. Some organizations will join with the sole intent of using the FiXs®-Certified Infrastructure for *internal* purposes. For example, a company may have a large number of employees scattered in field offices around a large geographic area, and it may have a well-established internal networking infrastructure already in place. However, this particular company may not have a need to authenticate employees from other FiXs® member company sites. In this situation, this particular company would not be listed in the FiXs®-Certified Trust Broker, because they have no need to interact with other FiXs® Members.

A Member only becomes a “trusted” organization when its unique identifying number, known as its Organizational Code, appears in the FiXs®-Certified Trust Broker. If a Member uses the FiXs®-Certified Network strictly for internal purposes, its Organizational Code will not appear in the Broker server’s trust list, and all transactions for the member will be rejected by that Trust Broker. Member companies become “trusted” by joining FiXs® and expressing their desire to interact with other FiXs® “trusted” members. A Member Organization is de-activated by removing its Organization code from the FiXs®-Certified Trust Broker (FTB) registry.

Let’s now consider the second case, where FiXs® Member Organizations *are* interested in interacting with other FiXs® Member Organizations. This illustrates a scenario where employees have frequent interactions with other FiXs® member organizations, and there is a requirement for a high level of trust and assurance in the credentials and identities that are being presented. In this situation, these companies *would* be listed in the FTB.

Finally, the third scenario is a complete and full trust by both FiXs® and an entity, such as the Department of Defense (DoD), which has a separate ‘Trust Broker’. In this scenario companies require a high level of trust, assurance, confidence and interaction with other FiXs® Member Organizations as well as with the DoD. Conversely, since this is a two-way trust, this scenario also implies that members of the DoD (CAC holders) will be able interact with these trusted FiXs® member companies in a highly trustworthy manner. In this case, these member company sites will be listed in *both* trust lists of the FTB *and* the DoD TGB. Again, it is important to note that DoD (and FiXs®, for that matter) still retains the ability to individually single out a particular member for exclusion from its trust list. It is the sole decision and discretion of DoD to allow or deny electronic interchange of FiXs®-Certified or DoD credentials with specific FiXs® member companies.

The agreements process that binds FiXs® Member Organizations to one another is depicted in Figure 1.1, while the transaction flow process is depicted in Figure 1.2.

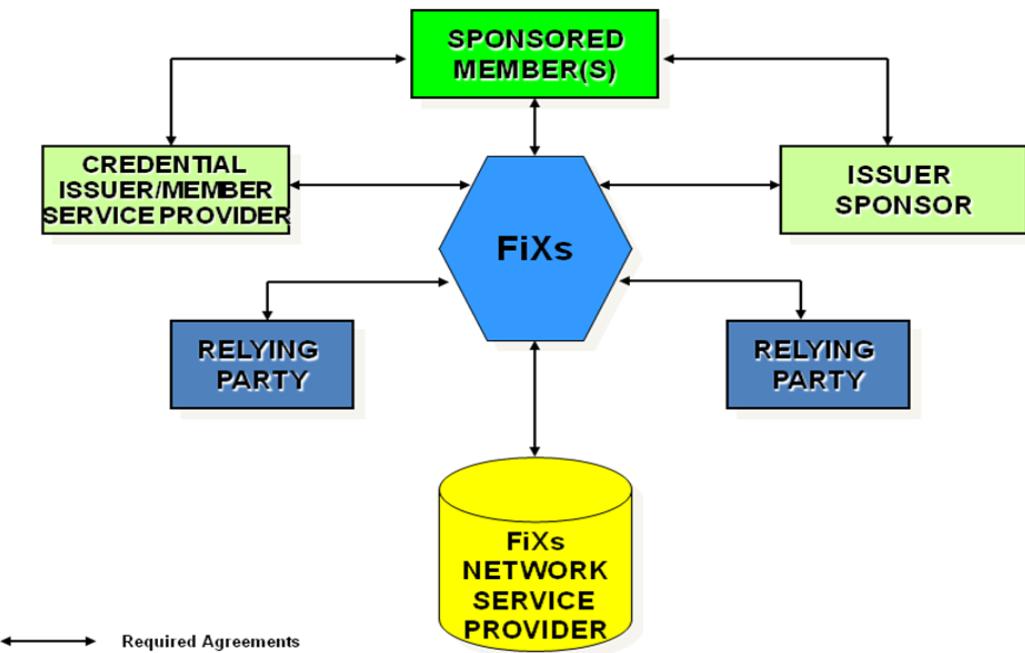


Figure 1.1 FiXs® Agreement Process

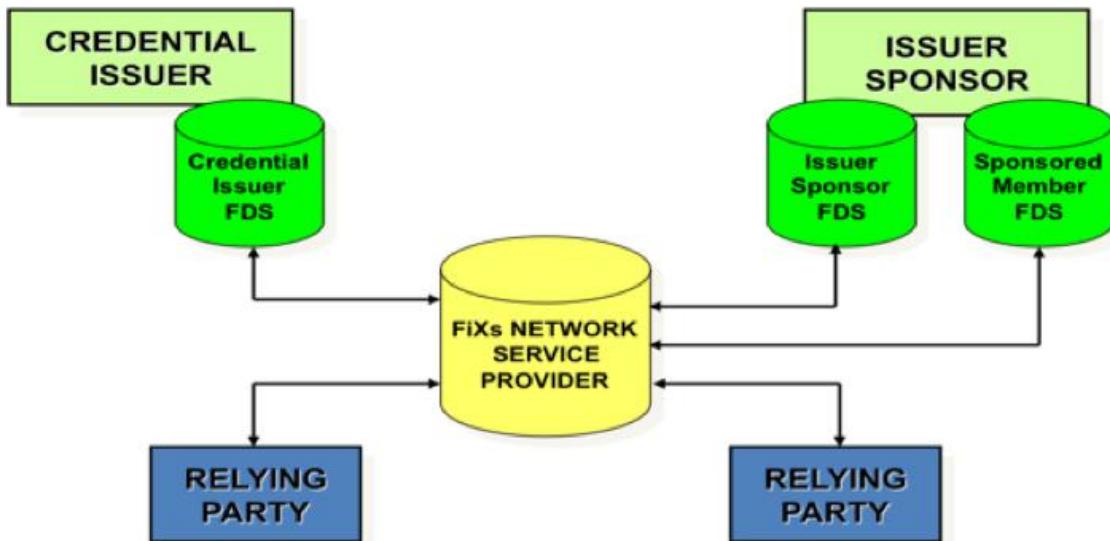


Figure 1.2 FiXs® Transaction Flow

1.1 Personnel Definitions and Requirements

This section defines and describes the requirements associated with personnel that will

perform FiXs® functions for FiXs®-Certified Credential Issuers and Relying Parties. Note: these are the functions that need to be discharged in the FiXs® program. However, it is up to the Member Organization as to how these positions will be filled within the Organization (for example, a Member may opt to appoint an existing employee to take on a FiXs® function as an additional role). These Rules must be posted so as to be easily accessible to all personnel whose responsibilities are addressed by these Rules. The only exceptions are that 1) the Domain Program Manager cannot serve as either a Facility Enroller or Facility Verifier, and 2) Facility Enrollers and Facility Verifiers must always be separate personnel. See Figure 1, Sample Organization Chart, for an illustration of how FiXs® functions/positions can be organized.

1.1.1 PROGRAM MANAGER

The **Program Manager** (PM) manages and administers the FiXs® program within a Member company or organizational domain. The PM has technical oversight of the program and is responsible for appointing the Domain Technical Administrator and Domain Functional Administrator for the Program.

1.1.1.1 Domain Technical Administrator

The PM must designate at least one **Technical Administrator** who has the authority to perform maintenance on the Enrollment System and/or the Authentication System for the Member Organization. The FiXs® Domain Administrator works with the Security Official of the Organization responsible for Physical Security to ensure a coordinated approach, particularly at the Authentication Station sites.

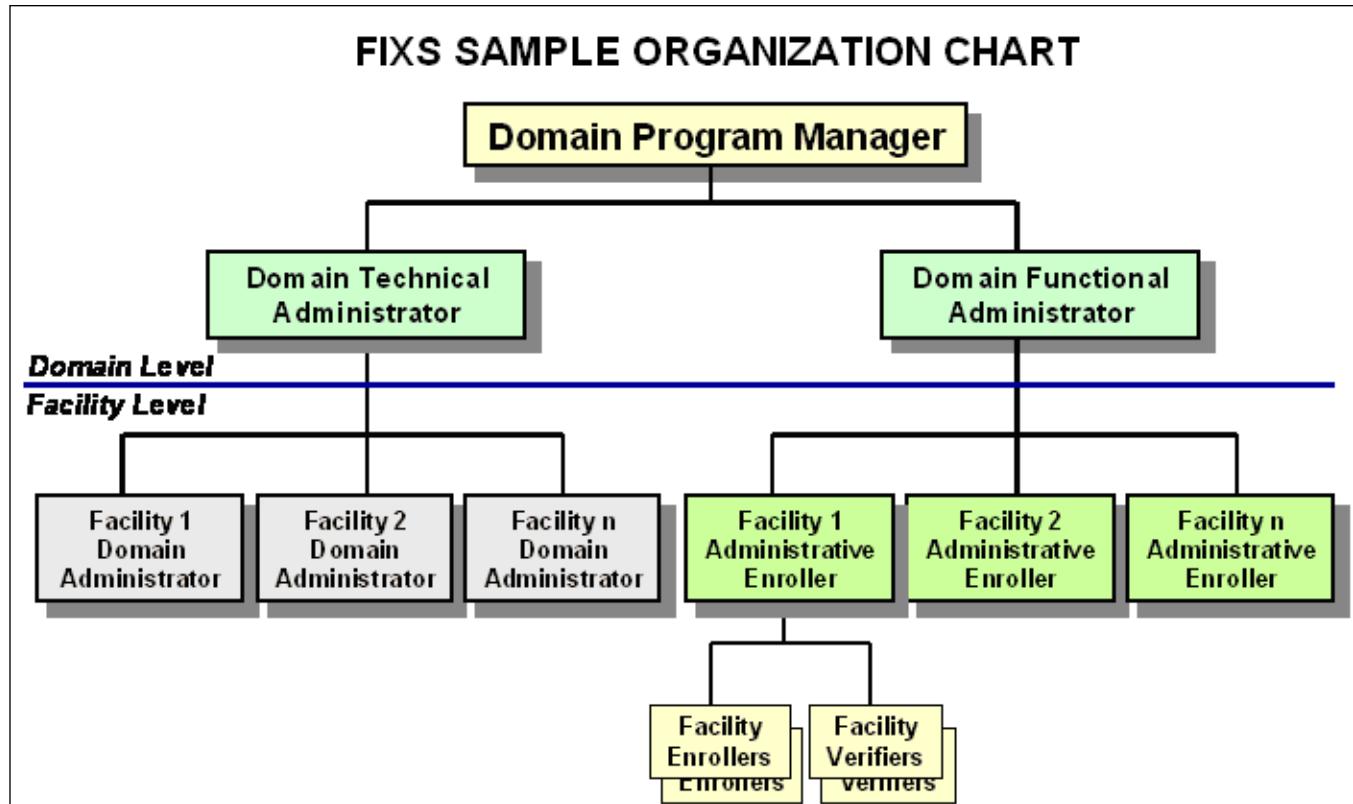


Figure 1.3: FiXs® Sample Organization Chart

1.1.1.2 Domain Functional Administrator

The PM must designate a Domain Functional Administrator if the organization is participating in FiXs® as a FiXs®-Certified Credential Issuer. The **Domain Functional Administrator** is responsible for the enrollment functions and management of the enrollment personnel within the Member organization. The Domain Functional Administrator is authorized to enroll and train Facility Administrative Enrollers. In addition, the Functional Administrator must designate individuals within the organization who have the authority to attest to the applicant's need for a FiXs®-Certified Credential.

1.1.2 ENROLLMENT PERSONNEL REQUIREMENTS

The FiXs®-Certified Credential Issuer is responsible for designating, training, and certifying Enrollment Personnel on the FiXs®-Certified System. Enrollment Personnel must be vetted in accordance with 2.1.2, Verify Applicant Identification (Vetting/Identity Proofing). Enrollment Personnel are under the management and supervision of the Domain Functional Administrator. FiXs® Member Organizations are responsible for maintaining an up-to-date list of certified Enrollment Personnel, periodically reviewing their lists, ensuring current training is provided to all personnel and maintaining up-to-date certifications for all Enrollment

Personnel. It is recommended that each FiXs® Member Organization review its list of Enrollment Personnel at least on a yearly basis. These personnel categories are described below.

1.1.2.1 Facility Administrative Enrollers

A FiXs®-Certified Credential Issuer must designate at least one Facility Administrator Enroller per Member facility. **Facility Administrative Enrollers** are responsible for enrolling and terminating new local Facility Enrollers using the Enrollment Operator Maintenance Web Application.

1.1.2.2 Facility Enrollers

Facility Enrollers are employees of a FiXs®-Certified Credential Issuer who operate the Enrollment Client and are responsible for capturing the required FiXs® ID data from FiXs® Applicants. Facility Enrollers may be designated by the Facility Administrative Enroller, and once appointed must be trained and certified by Facility Administrative Enrollers to perform the functions described below on the Enrollment Client.

1.1.2.2.1 Session Authentication

The Facility Enroller must authenticate himself/herself to the Enrollment Web Application at the beginning of each session using their FiXs®-Certified Credential/ identification number and a biometric.

1.1.2.2.2 Capture Participant Enrollment Data

In a single session, the Facility Enroller must completely and successfully capture and store an applicant's digitized photograph, fingerprint biometrics, and name identification and demographic data. All data must be correctly entered during the single session.

1.1.2.3 Facility Verifiers

A FiXs®-Certified Credential Issuer must designate at least one Facility Verifier per Member facility. A **Facility Verifier** is an employee within the organization who has the authority to perform the identity proofing tasks outlined in Section 2.1.2. In addition, the Facility Verifier is responsible for safeguarding background check documents and results in accordance with the policies and procedures outlined in the *National Industrial Security Program Operating Manual (NISPOM)*. *Facility Verifiers shall not dis-enroll participants.*

1.1.3 AUTHENTICATION PERSONNEL REQUIREMENTS

The Relying Party is responsible for designating, training, and certifying Authentication Personnel described in the sections that follow. The Relying Party is also responsible for maintaining an up-to-date list of certified Authentication Personnel, periodically reviewing their lists, ensuring current training is provided to all personnel and maintaining up-to-date certifications for all Authentication Personnel. It is recommended that each Relying Party review its list of Authentication Personnel at least on a yearly basis.

1.1.3.1 Facility Domain Administrators

A FiXs® Member organization must designate at least one Facility Domain Administrator per Member Facility. **Facility Domain Administrators** have the technical and operational responsibilities for individual FiXs®-Certified Facilities within a domain.

1.1.3.2 Authentication Station Operators

Authentication Station Operators operate the Authentication Client at Relying Party facilities. They must be trained and certified by the Facility Domain Administrator to perform Authentication Inquiries and routine administrative functions. These functions include:

1.1.3.2.1 Session Authentication/Log-On

Prior to processing FiXs® Participants, the Authentication Station Operator must log in and authenticate to the system using their FiXs®-Certified Credential/ identification number and biometric.

1.1.3.2.2 Authenticate Participant Credentials

The Authentication Station Operator must validate a FiXs® Participant's credentials in accordance with the instructions provided on the Authentication Station after correctly entering the initial ID data.

1.1.3.2.3 Explicitly Accept or Reject the Credentials

Based on local operating procedures, the FiXs®-Certified Authentication Station Operator decides whether to grant the Participant access. In accordance with Section 3.1.2.2, the Authentication Station Operator must explicitly record his or her decision about whether to grant the Participant access and the decision shall be recorded in the system Audit Log.

1.2 Systems Facility Definitions and Requirements

The Sections that follow describe the systems requirements at FiXs®-Certified Credential Issuer facilities and Relying Party facilities that must be in place prior to starting FiXs® operations. For a standard FiXs® Member configuration and list of standard components as well as the standards and formats associated with data and messages, please refer to the *FiXs® Technical Architecture and Specifications*.

1.2.1 FIXS®-CERTIFIED TRUST BROKER (FTB) INTERFACE REQUIREMENTS

FiXs®-Certified Credential Issuers and Relying Parties (including the DoD) acting in each of these roles must maintain an interface to the FTB system in compliance with the *FiXs® Technical Architecture and Specifications*.

1.2.2 SYSTEM ASSESSMENT

The organization shall issue credentials only through systems and providers whose reliability has been established by the agency and so documented and approved in writing (i.e., certified) in accordance with the *FiXs® Security*

Guidelines.

1.2.3 CREDENTIAL ISSUER OPERATIONAL REQUIREMENTS

The Credential Issuer system supports enrollment of the FiXs® Participant; maintenance of reliable connectivity for data access, storage of the participant data, log and audit trails; and, credential authentication. The hardware and software requirements association with these functions are described in the sections that follow. See Figure 2: Credential Issuing System.

1.2.3.1 Enrollment Site Certification Requirements

Enrollment Sites must be certified according to the procedures established by FiXs® Guidelines. The DoD. The Domain Technical Administrator is responsible for ensuring that these procedures are followed and that all relevant documentation and checklists are signed.

1.2.3.2 Enrollment System Requirements

This section describes the system requirements for enrolling new FiXs® members.

1.2.3.2.1 Enrollment Client (and Browser)

The **Enrollment Client** is a PC with a Web browser for network access to the FDS. It also contains a set of drivers for a web camera and a fingerprint reader.

1.2.3.2.2 Enrollment Web Server

The **Enrollment Web Server** is a standard web server (which resides on the FDS) that processes enrollments from the Authentication Client and stores the records in the Sponsor's FiXs®-Certified Data Repository.

1.2.3.2.3 Enrollment Web Application Software

The **Enrollment Web Application Software** enables entry of new FiXs® Participants into the Sponsor's FiXs®-Certified Data Repository.

1.2.3.2.4 Operator Maintenance Web Application

The **Operator Maintenance Web Application Software** enables new local site Enrollment Operators to be created and terminated on the Sponsor's FiXs®-Certified Data Repository. This operation can only be conducted by a designated Facility Domain Administrator at each local site and must be conducted in accordance with the *FiXs® Security Guidelines*.

1.2.3.2.5 Smart Card Writer (Optional)

The Enrollment System may include a Smart Card Writer. The **Smart Card Writer** can be used to write ID data to the card and record images for comparison to a scanned image on the Authentication Client. Captured data must conform to the

specifications found in the *FiXs® Technical Architecture and Specifications*.

1.2.3.2.6 Biometric Capturing Device

The Enrollment System must include a **Fingerprint Capturing Device** and software for capturing, reading, storing and comparing fingerprints or other devices as may be consistent with these operating rules for capturing biometrics. Captured data must conform to the specifications found in the *FiXs® Technical Architecture and Specifications*. (Devices compliant with the software are listed in the *FiXs® Technical Architecture and Specifications*.)

1.2.3.2.7 Digital Camera

The Enrollment System must include a **Digital Camera** capable of capturing digital photos and storing them in file formats as per the *FiXs® Technical Architecture and Specifications*. (Devices compliant with the software are listed in the *FiXs® Technical Architecture and Specifications*.)

1.2.3.2.8 Bar Code Reader/Printer

The Enrollment System must include a **Bar Code Reader/Printer** for storing and accepting current token barcodes or printing new barcodes for existing tokens as per the *FiXs® Technical Architecture and Specifications*. (Devices compliant with the software are listed in the *FiXs® Technical Architecture and Specifications*.)

1.2.3.2.9 Driver's License/Passport Reader

The Enrollment System must capture and validate information for enrollment in compliance with the *FiXs® Technical Architecture and Specifications*.

1.2.3.2.10 Scanning Device

The Enrollment System must include a device that is capable of scanning physical documents into electronic form so that the documents may be electronically stored.

1.2.3.2.11 Enrollment System Performance Requirements

The Enrollment System must be available for use 24 hours a day 7 days a week.

1.2.3.2.12 Trusted Computing

In order to achieve higher levels of trust, assurance and security, interested FiXs® members may (optionally) employ enrollment and/or authentication client machines with a hardware-based Trusted Platform Module (TPM) device. Such TPM devices are implemented in accordance with open specifications, as defined

by the Trusted Computing Group™.

For peripheral devices, such as trusted smart card readers/writers, fingerprint readers, keyboards, and secure PIN entry devices, there are even more secure, high assurance, trusted path devices that may be implemented, which offer an additional layer of trust, especially in sensitive or classified environments. Such devices are offered by a number of vendors and manufacturers, some of which are existing FiXs® member companies.

1.2.4 FIXS® DOMAIN SYSTEM REQUIREMENTS

This section describes system requirements for FiXs®-Certified Domain Server (FDS) and authentication system.

1.2.4.1 FiXs®-Certified Domain Server

The ***FiXs®-Certified Domain Server (FDS)*** platform contains the enrollment and authentication server software and it interfaces to the FiXs®-Certified Data Repository, the FTB, the Enrollment Client, and the Authentication Client.

1.2.4.2 FiXs®-Certified Data Repository

The ***FiXs®-Certified Data Repository*** stores the identification credentials and audit files associated with the FiXs® Participants of the Member Organization and interfaces to the Member's FDS. Data and formats are described in the *FiXs® Technical Architecture and Specifications*.

1.2.4.3 Hardware Security Modules

A ***Hardware Security Module (HSM)*** must be attached to the FDS. The HSM device is used to encrypt messages that are being sent to the FTB and to verify signatures of messages received from the FTB. The HSM contains: a) the private key for the new FDS; and, b) the public key of the Trust Server. These HSMs are loaded by the FTB and delivered securely to each FDS environment.

1.2.4.4 System Performance Requirements Authentication Processing

The Verification System must be operational 24 hours a day, 7 days a week, with an up-time availability of 99.99%. The FDS must process an Authentication Inquiry and return an Authentication Response in no more than 5 seconds.

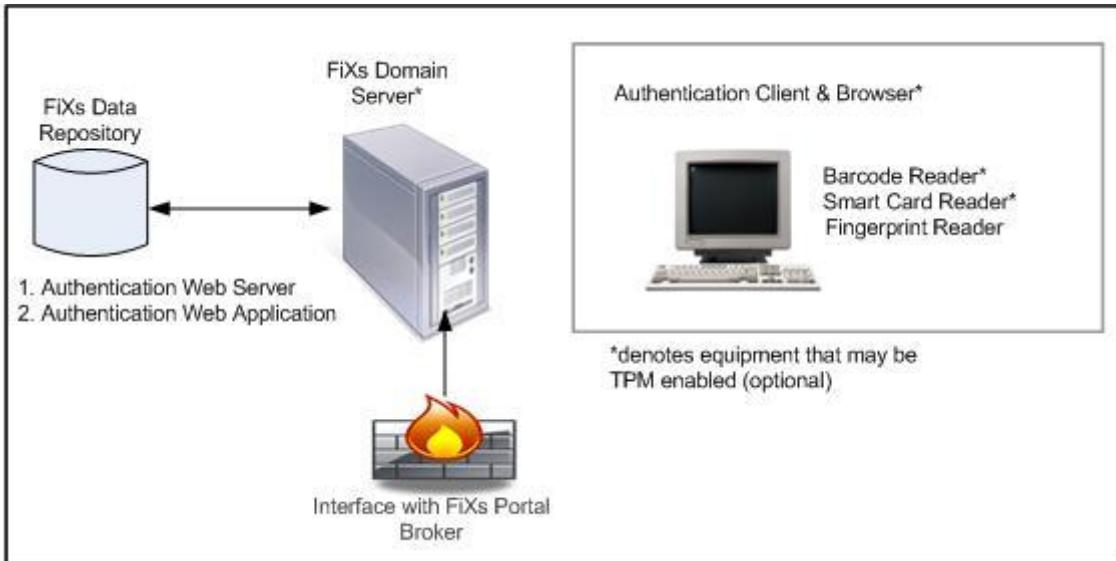


Figure 2: FiXs®-Certified Credential Issuing System

1.2.5 RELYING PARTY OPERATIONAL REQUIREMENTS

The Relying Party system serves to originate Authentication Inquiries for FiXs® Participants visiting the Relying Party's sites. The hardware and software requirements associated with this function are described in the sections that follow. See Figure 3: Relying Party System Requirements.

1.2.5.1 Relying Party Authentication Site Certification Requirements

Authentication Sites must be certified according to the procedures established by the FiXs® Implementation Guidelines. The Facility Domain Administrator is responsible for ensuring that these procedures are followed and that all relevant documentation and checklists are signed certified and remitted to DoD. (For the POC, certification is not required.)

1.2.5.2 Relying Party Authentication System Requirements

This section describes the system requirements for Relying Parties.

1.2.5.2.1 *Authentication Client*

The **Authentication Client** is a PC with a standard Web browser for access to the FDS. Each client will contain an embedded site ID file and a set of drivers for a bar code reader, a smart card reader, and a fingerprint reader.

1.2.5.2.2 *Authentication Web Server*

The **Authentication Web Server** is a standard web server (which resides on the FDS) that processes Authentication Inquiries and Responses between the Authentication Client and the FTB and the Relying Party's FDS.

1.2.5.2.3 *Authentication Web Server Application*

The **Authentication Web Server Application** receives the ID credential information from the Client and returns identity information and fingerprint data for matching on the Client.

1.2.5.2.4 Fingerprint Reader for Authentication

The Authentication system must include a **Fingerprint Reader** in accordance with the *FiXs® Technical Architecture and Specifications*. (Devices compliant with the software and drivers are listed in the *FiXs® Technical Architecture and Specifications*.)

1.2.5.2.5 Smart Card Reader for Authentication

The Authentication system must include a **Smart Card Reader** in accordance with the *FiXs® Technical Architecture and Specifications*. (Devices compliant with the software and drivers are listed in the *FiXs® Technical Architecture and Specifications*.)

In order to support full interoperability with existing DoD CAC cards, FiXs®-Certified Smart Card Readers and Writers should be compliant with current DoD CAC card standards; as of this writing, the current standard is Government Smart Card (GSC) Interoperability Specification (IS) version 2.0.

1.2.5.2.6 Bar Code Reader

The Authentication system may include a **Bar Code Reader** in accordance with the *FiXs® Technical Architecture and Specifications*. (Devices compliant with the software and drivers are listed in the *FiXs® Technical Architecture and Specifications*.)

1.2.5.2.7 Pin Pad

The Authentication System must include a device that enables a Participant to enter his or her Personal Identification Number (PIN) as part of the authentication process for a CAC or similar card.

1.2.5.2.8 Driver's License/Passport Reader

The Authentication System must include a device that is capable of validating the authenticity of a Participant's driver's license or passport.

1.2.5.2.9 Authentication System Performance Requirements

The Authentication System must be operational 24 hours a day, 7 days a week, with an up-time availability of 99%.

1.2.5.2.10 Trusted Computing

In order to achieve higher levels of trust, assurance and security, interested FiXs® members may (optionally) employ enrollment and/or authentication client machines with a hardware-based TPM device. Such TPM devices are implemented in accordance with open specifications, as defined by the Trusted Computing

Group™.

For peripheral devices, such as trusted smart card readers/writers, fingerprint readers, keyboards, and secure PIN entry devices, there are even more secure, high assurance, trusted path devices that may be implemented, which offer an additional layer of trust, especially in sensitive or classified environments. Such devices are offered by a number of vendors and manufacturers, some of which are existing FiXs® member companies.

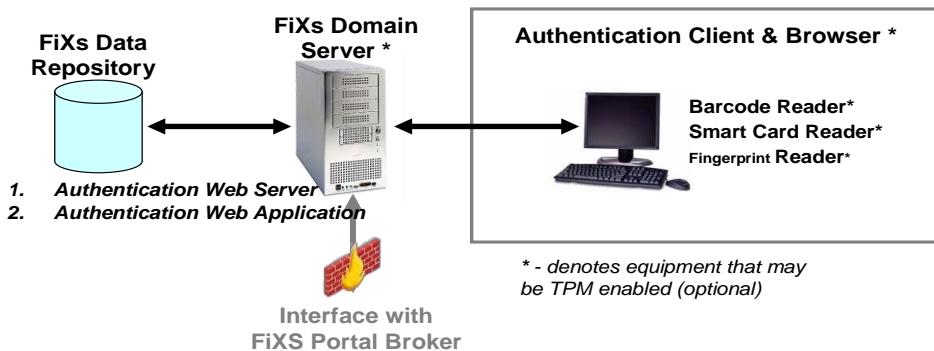


Figure 3: Relying Party System Requirements

1.2.6 MEMBER SERVICE PROVIDER REQUIREMENTS

A FiXs®-Certified Member Service Provider (MSP) is a FiXs® Founding Member that has agreed to provide equipment procurement and management services to FiXs®-Certified Credential Issuers and/or FiXs® Relying Parties. In its role as MSP, designated Founding Members will supply domain servers, enrollment equipment and authentication equipment (including required peripherals) to FiXs®-Certified Credential Issuers and Relying Parties that request these services. MSP services include equipment procurement, delivery and deployment; inventory management; equipment certification; equipment configuration; and documentation. Optionally, MSPs may also provide local application development and integration as well as consultative services to FiXs®-Certified Credential

Issuers and Relying Parties.

1.2.7 RECORDS/FILES MAINTENANCE REQUIREMENTS

This section describes FiXs® requirements for records and file maintenance.

1.2.7.1 FiXs® File Updates

FiXs®-Certified Credential Issuers are responsible for maintaining updated FiXs® files including Enrollment Files, Control Files, Administrative Files, Revocation and Audit Files. These files must be updated and maintained by the FiXs® Member Organization in a timely manner.

In some cases, such as the Control Files and certain Administrative Files, updates may be electronically communicated by the FTB to the FiXs®-Certified Credential Issuer's FDS server/s. It is the responsibility of the FiXs®-Certified Credential Issuer to ensure proper firewall connectivity, in order to receive, accept, process, and internally disseminate (if necessary) these updates.

1.2.7.2 Notification of Revocation of FiXs® Status/Dis-Enrollment

A FiXs®-Certified Credential Issuer must maintain a near-real-time list of participants that it has enrolled into the FiXs®-Certified System. When an employee leaves a Sponsor or when a Sponsor's Program Manager revokes a Participant's authorization for FiXs® participation, the Sponsor must notify the FiXs®-Certified Credential Issuer in sufficient time to ensure that the participant is dis-enrolled and the FDS updated within three (3) hours.

For changes in employee status, such as change of name, termination, ineligibility, or other changes as noted in The Privacy Act of 1974, the FiXs®-Certified Credential Issuer must complete the updates (including any revocation of credentials, if necessary) within three (3) hours.

Dis-enrolling a FiXs® participant means that his or her identifier is no longer valid, and that all subsequent authentication attempts should result in a failure. The Relying Party shall be responsible for the actions of any participant who is granted access after the participant was successfully dis-enrolled in accordance with these Rules and the Relying Party received the appropriate message in response to an authentication request.

While the reason for any dis-enrollment may be provided to the FiXs® Domain Administrator, such reason shall not be transmitted to the Authentication Station. All dis-enrollments shall be accomplished at the participant's FDS and shall be performed by the Facility Administrative Enroller or a Facility Enroller. A Facility Verifier is not allowed to perform a dis-enrollment operation.

1.2.7.3 Audit Requirements

This section describes the auditing requirements for a FDS.

1.2.7.3.1 System Audits

Auditing of the FDS must be at a sufficient level to recreate any transaction successfully or unsuccessfully performed within the FiXs®-Certified System. The software provided by the FiXs® program will record the data to a level that is sufficient to satisfy these requirements.

1.3 Logical Authentication

This Section defines the requirements for starting FiXs® logical authentication operations. In the case of the requirements necessary to effect the proper life cycle management of the digital certificate protected on the FiXs®-Certified Credential, Certificate Policies (CPs), referenced herein, and the associated Certification Practice Statements (CPSs) shall be relied upon to describe the establishment and operation of the Public Key Infrastructure (PKI) and the policies and procedures relating to holding or using certificates issued onto a FiXs®-Certified Credential. Each CP is applicable to all individuals that will be interacting with the Federation; DoD activities; other government agencies; and associated individuals and contractors. The purpose of each CPS is to inform individuals relying (Relying Parties) on certificates issued and credential holders (holders of certificates) of their duties and obligations. It is also to advise those parties of the policies, practices and procedures that are used for issuing, validating and revoking these certificates.

FiXs® recognizes the need to interoperate within various domains and has a requirement to establish trust relationships with Certification Authorities (CAs) that achieve a satisfactory assurance level. The CPs referenced herein shall be enforced in full, in accordance with the policies asserted by each:

- Department of Defense PKI Certificate Policy (DoD PKI CP)
- United States (US) Government Certificate Policy (CP) for External Certification Authorities (ECA) [ECA CP]
- Federal PKI Common Policy Framework [FPCPF]
- Federal Bridge Certificate Authority [FBCA]

1.4 Level 1 (FiXs® equivalent “Low”)

The digital certificates at this level shall assert basic assurance as stipulated by the FBCA, at a minimum.

1.5 Level 2 (FiXs® equivalent “Medium”)

The digital certificates at this level shall assert medium assurance as stipulated by the DoD PKI CP, the ECA CP and the FBCA; as well as, certificates that assert the common policy under the FPCPF.

1.6 Levels 3 (FiXs® equivalent “Medium High”)

The digital certificates at this level shall assert:

- Medium hardware assurance as stipulated by the DoD PKI CP, the ECA CP
- Federal Common Hardware as stipulated by the FPCPF; or,

- High or medium hardware assurance as stipulated in the FBCA CP that are also approved for DoD use, refer to Section 1.10.3 below.

1.7 Level 4, (FiXs® equivalent “High”)

The digital certificates at this level shall assert:

- Medium hardware assurance as stipulated by the DoD PKI CP and the ECA CP;
- Federal Common Hardware as stipulated by the FPCPF; or,
- High or medium hardware assurance as stipulated in the FBCA CP that are also approved for DoD use, refer to Section 1.10.3 below.

1.8 Framework

At all levels, FiXs® members shall adhere to the policy framework governing the public key infrastructure component defined by the policy referenced for each level or higher. These policies require the use of FIPS 140 validated cryptographic modules for all cryptographic operations and the protection of trusted public keys. The policy for users with hardware cryptographic modules mandates a Level 2/medium assurance validation, which is achieved by FiXs® via the PIV card.

The CPs that comprise this framework are consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) RFC 2527, Certificate Policy and Certification Practice Statement Framework. These policies define a PKI consisting of products and services that provide and manage X.509 certificates for public key cryptography that FiXs® shall trust. The certificates issued under these policies identify the individual named in the certificate and bind that person to a particular public/ private key pair and the FiXs® credential. FiXs® will trust these PKIs for the following security management services:

- Key generation/ storage
- Certificate generation, update, renewal, rekey, and distribution
- Certificate revocation list (CRL) generation and distribution
- Directory management of certificate related items
- Certificate token initialization/programming/management
- System management functions (e.g., security audit, configuration management, archive.)

1.9 Certificate Validation

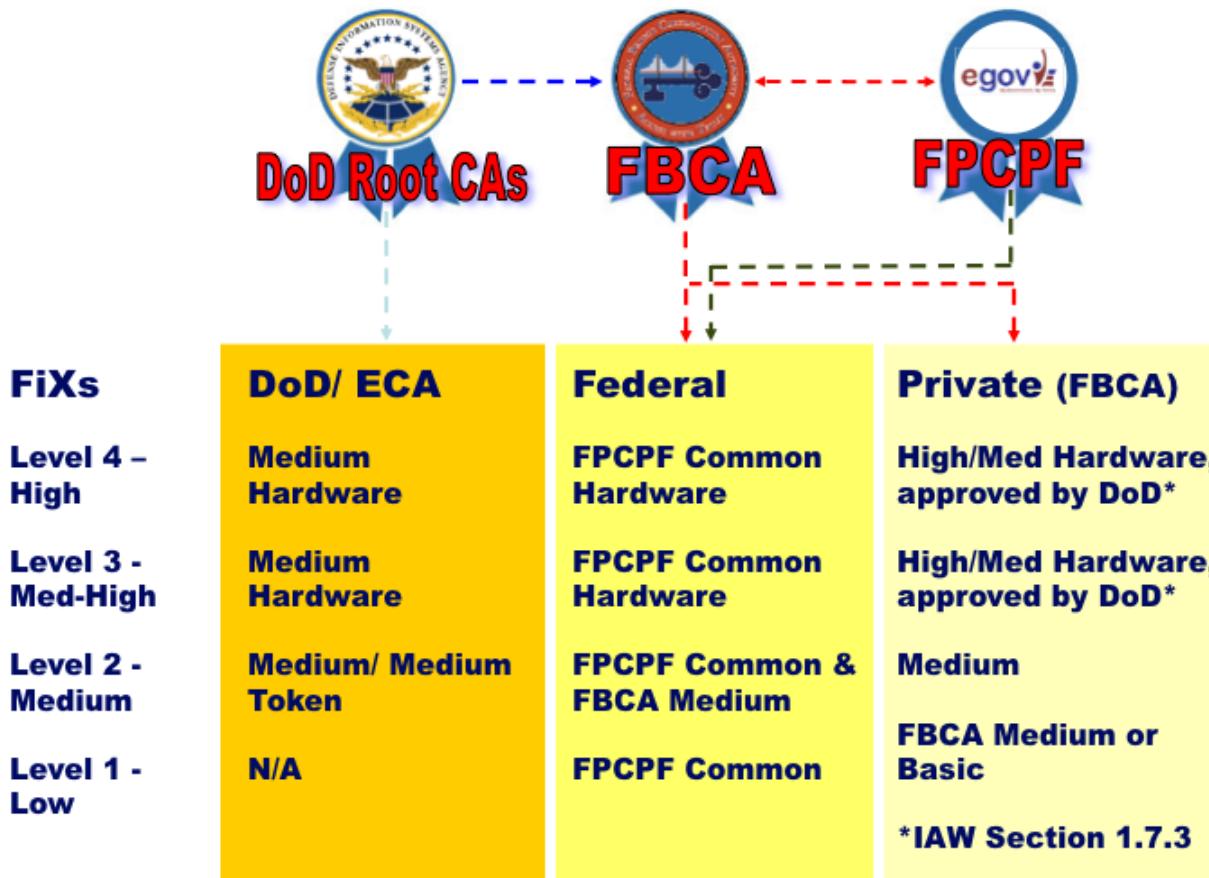
The FiXs®-Certified Network includes a cost effective, quick deployment offering that provides full relying party integration and compliance with the smart card credential deployed under DoD PKI, FBCA, and HSPD-12. The FiXs®-Certified Validation service provides monitoring and validation for all FBCA-approved, DoD internal and external ECA, ACES and others as they come online.

1.10 FiXs® Logical Trust Model

The FiXs® logical trust model supports hierarchical PKI, mesh PKI, and single certification authority implementations. As such, FiXs® adheres to the constraints established for the secure distribution of self-signed certificates for use as trust anchors, defined in each CP. Additionally, no FiXs®-Certified Credential holder shall hold more than one active FiXs®-Certified Credential.

The current FiXs® logical trust model is depicted in the following figure.

Practice note: The combination of the Certificate Policy (applied) with the FiXs® foundational documents and the FiXs® Operating Rules provide individual vetting and the credential uniqueness necessary to provide the appropriate levels of assurance, as defined above, for both physical and logical authentication.



Three primary programs, the DoD PKI, the Federal Bridge Certificate Authority, and the Federal PKI Common Policy Framework define the Federal PKI.

1.10.1 DOD PKI

Two Certificate Policies exist under the DoD PKI Policy Management Authority (PMA): the DoD PKI CP and the ECA CP.

These policies define various levels of assurance including Medium Hardware and Medium. DoD and ECA compliant certificates asserting the following Medium Hardware Assurance object identifiers (OIDs) shall be recognized by the FiXs® network as asserting FiXs® level 3 or 4:

id-US-dod-

mediumhardware::=

{2.16.840.1.101.2.1.11.9}

id-eca-medium-hardware ::= {2.16.840.1.101.3.2.1.12.2}

DoD and ECA compliant certificates asserting the following Medium assurance OIDs shall be recognized by the FiXs® network as asserting FiXs® level 2:

id-US-dod-medium ::= {2.16.840.1.101.2.1.11.5}

id-eca-medium ::= {2.16.840.1.101.3.2.1.12.1}

id-eca-mediumtoken ::= {2.16.840.1.101.3.2.1.12.3}¹

1.10.2 FEDERAL PKI COMMON POLICY FRAMEWORK (FPCPF)

The FPCPF defines two levels of assurance Common Hardware and Common. FPCPF compliant certificates asserting the following Common Hardware assurance OIDs shall be recognized by the FiXs® network as asserting FiXs® level 3 or 4:

id-fpki-common-hardware ::= {2 16 840 1 101 3 2 1 3 7}

id-fpki-common-authentication ::= {2 16 840 1 101 3 2 1 3 13}

id-fpki-common-High ::= {2 16 840 1 101 3 2 1 3 16}

FPCPF compliant certificates asserting the following Common assurance level OIDs shall be recognized by the FiXs® network as asserting FiXs® level 2:

id-fpki-common-policy ::= {2 16 840 1 101 3 2 1 3 6}

id-fpki-common-devices ::= {2 16 840 1 101 3 2 1 3 8}

id-fpki-common-cardAuth ::= {2 16 840 1 101 3 2 1 3 17}

1.10.3 FEDERAL BRIDGE CERTIFICATION AUTHORITY (FBCA)

FBCA-compliant CAs do not assert a FBCA OID the trust of these certificates must be based on the issuing CAs cross certificate with the Federal Bridge.

In accordance with the DoD CIO Memorandum, dated July 22, 2008, “Approval of External Public Key Infrastructures” and DoD Instruction 8520.2, upon successful completion of interoperability testing [defined in Attachment 1 of that memorandum], those policy oids and root CAs approved for use within DoD information systems, shall be incorporated into this document, by reference. NOTE: the DoD document to be referenced is TBD.

FBCA-compliant certificates cross-certified with the federal bridge at High or Medium Hardware assurance and approved for DoD use, shall be recognized by the FiXs® network as asserting FiXs® level 4 or 3. FBCA compliant certificates cross-certified with the federal bridge at Medium assurance shall be recognized by

¹ Medium Token Assurance is intended for applications handling sensitive medium value information. These certificates are vetted in accordance with the requirements of FBCA Medium Hardware Assurance.

the FiXs® network as asserting FiXs® level 2. FBCA compliant certificates cross-certified with the federal bridge at Basic assurance shall be recognized by the FiXs® network as asserting FiXs® level 1.

1.10.3.1 Access Certificate for Electronic Services (ACES)

The ACES Program makes available the services that federal agencies need to implement PKI and digital signature services required by the Paperwork Reduction Action of 1995, the Government Paperwork Elimination Act of 1998 (GPEA), the E-SIGN Act, and the E-Government Act of 2002. Cross-certified with the Federal Bridge at the medium assurance level, the ACES CP provides an outward looking PKI from the Government and is intended to be trusted across Federal agencies that provide electronic services to the Public. ACES compliant certificates asserting the following Medium assurance level OIDs shall be recognized by the FiXs®-Certified Network as asserting FiXs® medium assurance or “level 2”:

- ACES Authorized CA Certificates: {2 16 840 1 101 3 2 1 1 1}
- Business Representative Digital Signature Certificates: {2 16 840 1 101 3 2 1 1 3}
- Business Representative Encryption Certificates: {2 16 840 1 101 3 2 1 1 3}
- Federal Employee Digital Signature Certificates: {2 16 840 1 101 3 2 1 6}
- Federal Employee Encryption Certificates: {2 16 840 1 101 3 2 1 1 6}
- State and Local Employee Digital Signature Certificates: {2 16 840 1 101 3 2 1 1 6}
- State and Local Employee Encryption Certificates: {2 16 840 1 101 3 2 1 1 6}

ACES-compliant certificates asserting the following medium hardware assurance level OIDs shall be recognized by the FiXs® Network as asserting FiXs® “medium high” (level 3) or “high” (level 4):

- Digital Signature Certificates on hardware: {2 16 840 1 101 3 2 1 1 7}
- Encryption Certificates on hardware: {2 16 840 1 101 3 2 1 1 7}

1.11 Certificate Profile

All certificates issued to a FiXs®-Certified Credential must be constructed in accordance with the Certificate Policy that is asserted in the certificate. Certificates may also include the following FiXs® attributes in the CN or as a dnQualifier:

1.11.1 FIXS® PERSON DESIGNATOR IDENTIFIER (PDI)

Certificates issued on a FiXs®-Certified, that are used to identify the credential as such, will include the FiXs® PDI that will consist of a *unique identification string* [unique to the credential holder]. The unique identifier shall be same for all certificates issued to a single credential holder and is unique to all credentials

across the FiXs®-Certified Network.

1.11.2 FIXS® ASSURANCE LEVEL

Certificates issued on a FiXs®-Certified that are used to identify the credential as such will include an identifier preceding the *unique identification string* that will designate the FiXs® assurance level [or the level of identity vetting that was employed] as follows:

- FiXs4, for FiXs®-Certified Credentials asserting FiXs® equivalent “High”
- FiXs3, for FiXs®-Certified Credentials FiXs® equivalent “Medium High”
- FiXs2, for FiXs®-Certified Credentials FiXs® equivalent “Medium”
- FiXs1, for FiXs®-Certified Credentials FiXs® equivalent “Low”

The following sample DNs are provided:

cn=Smith.John.J.FiXs®41234567890, ou=<subscribing organization>, ou=<CA provider>, o=U.S. Government, c=US

dnQualifier=FiXs®41234567890, cn=John J. Smith, ou=<structural container>, ou=<subscribing organization>, o=U.S. Government, c=US

2 FIXS®-CERTIFIED CREDENTIAL ISSUANCE

This Section describes the responsibilities for FiXs®-Certified Credentials Credential Issuers in initiating and maintaining an ***operational*** FiXs®-Certified System. FiXs®-Certified Credentials Issuers issue FiXs®-Certified Credentials to qualified users for themselves and/or other Sponsors, whether a Primary Trusted Organization or a Subscribing Party, and processes and responds to *Authentication Inquiries*. An Issuer Sponsor is a FiXs®-Certified Credentials Issuer that issues credentials to its own employees or sponsors other FiXs®-Certified Credentials Issuers and performs some or all of the FiXs®-Certified Credentials Issuer duties defined herein that the sponsored FiXs®-Certified Credentials Issuer chooses not to perform. In this case, the Issuer Sponsor assumes some or all of the following functions on behalf of the sponsored Issuer: enrollment and issuance; participant records management; FDS management; standards and specifications compliance; transaction processing; application integration; and coordination of human resources and security departments.

FiXs®-Certified Credentials Issuers shall have primary responsibility and liability for performance of the obligations of a FiXs®-Certified Credentials Issuer under these Rules, regardless of whether the obligations are performed by the FiXs®-Certified Credentials Issuer, Issuer Sponsor or a third party on behalf of the FiXs®-Certified Credentials Issuer. No delegation of duties by a FiXs®-Certified Credentials Issuer to an Issuer Sponsor or any other third party shall relieve such FiXs®-Certified Credentials Issuer of its liability for performance of such duties hereunder. The legal agreements process that binds FiXs® member organizations are depicted in Figure 1.1.

There is a distinction to be made between credentials and a badge. **Credentials** refer to the representations of an individual's identity -- such as biometric images, photographs, and unique identifiers (social security numbers or employee IDs) – that are approved by an organization to authenticate an individual for access. A **badge** or **token** can either 1) “hold” these credentials (such as a photo on the face of a badge or a biometric on a bar code) or 2) hold the “keys” or “pointers” to the credentials that are accessible in a record on a remote system (such as a number stored on a bar code that identifies the system and the record); the credentials can be downloaded to a local client.

Note that as the issuer of the CAC card, DoD is exempt from Section 2.1, *Credential Issuance* because CAC holders are automatically enrolled to the DCCIS system without any alterations to the CAC credential and identifier.

2.1 Credential Issuance

The ***FiXs®-Certified Credential Issuance*** process consists of four steps: 1) validate applicant's need for FiXs®-Certified Credentials; 2) verify applicant identification; 3) enroll applicant into FiXs®-Certified System; and 4) issue or record Participant's valid FiXs® identifier. These steps are described in the section that follows.

2.1.1 VALIDATE APPLICANT'S NEED FOR FiXs® CREDENTIALS

As a requisite for starting the FiXs®-Certified Credentials issuance process, the Facility Verifier must receive a request in writing from the sponsoring FiXs® Program Manager, or his/her designated agent on behalf of the applicant.

2.1.2 VERIFY APPLICANT IDENTIFICATION (VETTING/IDENTITY PROOFING)

Verifying the applicant's identification is the process by which the FiXs®-Certified

Credentials Issuer validates the identity information provided by the Applicant. This process must be completed for all FiXs® Applicants regardless of whether the same or similar documentation has been verified as part of the organizations' regular employment process. This process can also be referred to as "Vetting" or "Identity Proofing."

2.1.3 VERIFICATION PROCESS REQUIREMENTS

The identity proofing, registration and issuance process shall adhere to the principle of separation of duties to ensure that no single individual has the capability to issue a credential without the cooperation of another authorized person.

2.1.3.1 Verify Employee's Identification

The Facility Verifier must verify the applicant's identification per the procedures prescribed below.

2.1.3.1.1 *FiXs® Member Participant Applicants*

Upon validation of an Applicant's need for FiXs®-Certified Credentials, the FiXs®-Certified Credentials Issuer is required to fulfill application requirements specified in FiXs® Guidelines:

2.1.3.1.1.1 *AUTHENTICATE DOCUMENTS*

The Facility Verifier must validate a Social Security Number or an Alien Registration number in addition to other presented documents and electronically verify the authenticity of the ID documents. If the Social Security Number or the Alien Registration number and one other from of identification cannot be validated, the participant cannot be enrolled in the FiXs®-Certified System.

2.1.3.1.1.2 *COLLECT AND STORE APPLICANT BIOMETRIC(S)*

The Facility Verifier will capture the Applicant's digitized photo, collect, and store fingerprints to bind the identification documents to the Applicant's biometrics for the first time. The Facility Verifier must collect the applicant's fingerprints using the 10-fingerprint system at a Fingerprint Capture Station that complies with *FiXs® Technical Architecture and Specifications* for fingerprint capture and storage and store the record.

2.1.3.1.1.3 *ELECTRONICALLY STORE APPLICANT'S SOURCE DOCUMENTS*

Documents that are verified to complete the I-9 Form must be electronically stored either by: 1) scanning the documents or 2) retaining an electronic version of the document that is otherwise available.

2.1.3.1.1.4 *CERTIFY AUTHENTICATION PROCESS*

Either on the I-9 Form or as an attachment, the Facility Verifier

will include and electronically sign the following statement: "Addendum to Certification, Section 2: I also attest, under the penalty of perjury, that I have examined the photo identification document presented by the employee and that to the best of my ability I conclude that the photographic image and the employee are one in the same individual."

2.1.3.1.1.5 COMPLETE NATIONAL AGENCY CHECK

The Facility Verifier must have a background check conducted on the Applicant, which, at a minimum, must include:

For Level 2: local, county, state, and federal criminal history checks; as well as, sex offender registry and terrorist watch list checks.

For Level 3: commercial National Criminal History Check process through a certified FBI channel partner.

For Level 4: National Agency Check (NAC) in accordance with DoD Directive 5200.2-R Personnel Security Program. An active security clearance or NAC that has been conducted within four years will satisfy the requirements contained in this subparagraph, and a new NAC does not have to be conducted.

The process shall ensure completion and successful adjudication of a National Agency Check (NAC) and National Agency Check with Written Inquiries (NACI). A completed NAC is sufficient for interim credential issuance; however, the NACI must still be completed within six (6) months of the application date. The credential shall be revoked if the results of the investigation so justify. If the NACI is not completed within six (6) months, the NAC will be deemed revoked. A new NAC must be completed if the NAC will expire within six (6) months of the application date.

Note that this requirement may also be satisfied by locating and referencing a completed and successfully adjudicated NACI.

No person that has not been adjudicated via a federal process shall be granted a FiXs certified credential if a background check reveals any of the following:

- * Has had a felony conviction;
- * Is or is suspected of being a terrorist; or
- * Is on the Sex Offenders List.

2.1.4 ENROLL APPLICANT INTO FiXs®-Certified SYSTEM

Once the Applicant's identity has been verified, he or she can be enrolled into the FiXs®-Certified Credentials Issuer's FDS. This process makes the Applicant's (now a FiXs® Participant) record of credentials available for retrieval by a Relying Party for authentication. The Enrollment process is described in the sections that follow.

2.1.4.1 Verify Applicant's Reference Biometric

The Facility Enroller instructs the Applicant to scan his biometric and initiates a biometric verification check. If there is a positive match, the Facility Enroller proceeds to the next step. (If the Identity Proofing – Section 2.1.2 – and Enrollment – Section 2.1.4 – are performed at the same time, this step can be omitted.)

2.1.4.2 Enroll Applicant into FiXs®-Certified FDS

Enrolling an applicant refers to the creation of a valid FiXs® Participant record in the FiXs®-Certified Data Repository. All FiXs® Participants must be enrolled (have a valid record) in the Issuer's FiXs® Data Repository. To enroll a new employee as a FiXs® Participant, the Facility Enroller must collect the required enrollment ID data as prescribed in Section 2.1.3.

2.1.4.2.1 Create a New Participant Record

The Facility Enroller creates a new record for the Applicant in the FiXs®-Certified Data Repository and performs the following steps:

2.1.4.2.1.1 ENTER REQUIRED APPLICANT DATA

The Enrollment Operator enters the Applicant's first and last names, ORGANIZATION name; and, Employee ID number into the record. (See *FiXs® Technical Architecture and Specifications* for details.)

2.1.4.2.1.2 UPLOAD FiXs® ENROLLMENT ID DATA INTO APPLICANT'S RECORD

The Facility Enroller uploads the Applicant's Photograph File and Biometric File of the Applicant's fingerprints taken during the vetting/identity proofing process to the Applicant's record.

2.1.5 ISSUE PARTICIPANT VALID FiXs® IDENTIFIER

The final step in the FiXs®-Certified Credentials Issuance process is to issue the Participant a valid FiXs® Identifier that can be used to access the Participant's credentials. Valid identifiers include:

2.1.5.1 DoD EDI PIN for CAC Cardholders

The DoD EDI PIN (as the DoD's Employee ID) associated with the CAC card with the selected organization (e.g., Army, Navy, etc.) is a valid FiXs® identifier.

2.1.5.2 Organization Name and Employee ID for non-CAC Cardholders

The combination of the Participant's Member/Organization Code and ID and organization-assigned Employee ID number is a valid FiXs® identifier.

2.1.5.3 Identifier Access Method

The Authentication Station Operator must be able to access the valid FiXs® identifier to initiate the authentication process. The Participant can provide the Authentication Station Operator access to the identifier in one of four ways:

2.1.5.3.1 No Token/Verbal Communication of Organization and Employee ID

The Participant can verbally provide the Authentication Station Operator with the Member Organization name (from which the ID is obtained) and Employee ID number.

2.1.5.3.2 Presentation of Company/Organization Badge

The Participant can present the Authentication Station Operator with a Company or Organization Badge from which the valid FiXs® identifier can be read visually or by machine (e.g., all valid Barcode 39 codes can be scanned and sent in their entirety to a FiXs® member organization as a credential string). (See *FiXs® Technical Architecture and Specifications*.)

2.1.5.3.3 Presentation of FiXs® Badge

The Participant can present the Authentication Station Operator with a FiXs®-Certified Credentials (organizations can opt to issue separate FiXs®-Certified Credentials rather than use the existing employee badge) from which the valid FiXs® identifier can be read visually or by machine.

2.1.5.3.4 DoD EDI PIN for CAC Cardholders

The DoD EDI PIN (as the DoD's Employee ID) associated with the CAC card with the selected organization (e.g., Army, Navy, etc.) is a valid FiXs® identifier.

2.1.5.4 Expiration Date

All FiXs®-Certified Credentials must have an expiration date. A revocation process must exist such that an expired or invalidated credential is swiftly revoked.

2.1.6 APPEALS PROCESS

FiXs®-Certified Credentials Issuers shall maintain an appeals process for employees who are denied a credential or whose credentials are revoked.

2.2 Transaction Request Processing

The FiXs®-Certified Credentials Issuer is required to process Authentication Inquiries from its Authentication Clients and from Relying Parties. An **Authentication Inquiry** is an

electronic transaction originating either from 1) the Issuer's Authentication Client or 2) a Relying Party (through the FTB), which requests the authentication of a credential and credential holder. The Credential Issuer must return an Authentication Response to the originator of the Authentication Inquiry. An **Authentication Response** is a reply from the FiXs®-Certified Credentials Issuer to an Authentication Inquiry that sends a denial or transmits credential information (photo and fingerprints) to the Relying Party.

2.2.1 PROCESSING AUTHENTICATION INQUIRIES

When a FiXs®-Certified Credentials Issuer receives an Authentication Inquiry from an Authentication Client (either its own or from that of a Relying Party), the FiXs®-Certified Credentials Issuer's FDS checks that the credential information matches a valid record in its FiXs®-Certified Data Repository. If it does, an Authentication Response is prepared and sent back as described below.

2.2.2 INITIATING AUTHENTICATION RESPONSES

The FiXs®-Certified Credentials Issuer's FDS retrieves the applicable files, as specified in the appropriate FiXs® Guidelines, creates a valid XML Authentication Response message and transmits it back to the Authentication Client.

2.3 CERTIFICATE ISSUANCE

In addition to the responsibilities defined above, it is the responsibility of the FiXs®-Certified Credential Issuer to ensure that the certificates issued to the FiXs®-Certified Credentials are in compliance with the CPS associated with the CA or Certificate Manufacturing Authority (CMA) being employed, that applies to the X.509 version 3 certificates with assurance levels as defined in the appropriate CP. The processes and procedures in each CPS are applicable to individuals who manage the certificates, who directly use these certificates, and individuals who are responsible for applications or servers that rely on these certificates.

The chosen PKI shall be co-operated and managed by the FiXs®-Certified Credential Issuer and the CA, where the FiXs®-Certified Credential Issuer is responsible for management of the FiXs®-Certified Card Management System (CMS) including communications, facility, etc. and the roles described in the CP regarding entities responsible for enrollment and registering of individuals; and, adjudication/ issuance of the FiXs®-Certified Credential and associated certificates. The FiXs®-Certified Credential Issuer's responsibility for performing all associated roles and functions controlling CMS including the registration, identification and authentication, issuance, and customer service processes; includes the auditing of these roles and functions.

The following services are necessary to meet the requirements of the associated CP, but may be provided external to the CA or CMA:

- Registration: A FiXs®-Certified Credential applicant must appear in person before a Registrar to witness and certify the validity of documents and to take affidavits and depositions), as stipulated by the Policy Authority, present valid identification and accept the FiXs® credential holder obligations.
- Enrollment: A Federal Information Processing Standards (FIPS) 140-2 Level 3 Secure Socket Layer (SSL) connection from the FiXs®-Certified CMS to the CA/ CMA.
- Enrollment Validation: The FiXs®-Certified CMS registration process validates the applicant's enrollment information.

- Adjudication/ Issuance: Face-to-face custody exchange of the FiXs®-Certified Credential by the Issuer to the credential holder.

Based on the FiXs® (FIPS-201 compliant) enrollment and registration provided by the FiXs®-Certified Credential Issuer, the CA/ CMA provides the following:

- Certificate Manufacturing: When notified by the FiXs®-Certified Credential CMS of a valid enrollment request, the CA/ CMA manufactures the requested certificate(s) for delivery to a FIPS 201 compliant card.
- Certificate Publishing: The CA/ CMA publishes it to a directory. The directory may be accessed via Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS) gateway or via the LDAP protocol.
- Encryption Key Storage: Optional storage of escrowed encryption keys.
- Key Recovery: If encryption key escrow is selected, a Key Recovery Practice Statement (KRPS) shall detail the escrow and recovery processes.
- Certificate Status information: In the form of Certificate Revocation Lists (CRLs) distribution and Online Certificate Status Protocol (OCSP) responses.

It is the responsibility of the FiXs®-Certified Credential Issuer and the CA/ CMA to ensure that all of the requirements of the appropriate CP are met and are periodically audited by its independent auditor against the CPS and operates primary and secondary secure data centers in conformance with the Department of Defense (DoD), National Security Agency (NSA), U.S. General Services Administration (GSA) and best commercial practices.

2.4 Certificate Practice Statement

While the referenced CP defines the assurance can be placed in a certificate issued by a CA, the Certificate Practice Statement (CPS) states how the CA establishes that assurance. Each CA that issues certificates to FiXs®-Certified Credentials shall have an approved CPS corresponding to one or more of the referenced CPs, for the appropriate level of assurance. A FiXs®-Certified Credential Issuer shall only issue credentials with certificates that hold and assert the appropriate level of assurance as defined by this document.

2.5 Registration Practice Statement

The FiXs®-Certified Credential Issuer and the CA will define the separation of roles and special procedures used to manage FiXs®-Certified Credentials in accordance with the requirements of the appropriate CP or as may be more stringent than that set forth in the policy and the FiXs® Operating Rules. Prior to issuance of certificates to a FiXs®-Certified Credential, the Issuer will coordinate with the CA/ CMA to ensure that the procedures for authentication of personnel are documented in a Registration Practice Statement (RPS) and comply with the appropriate CP, and submitted to FiXs® for approval. The RPS shall require that registration, issuing and activation functions ensure that the applicant's identity information is verified. The RPS shall require that minimal procedures for authentication of employees and affiliated personnel are detailed, and shall clearly define those functions that are internal or outsourced. At a minimum, the RPS shall require authentication procedures include the following steps:

- The identity of the person performing the identification
- A signed declaration by that person that he or she verified the identity of the Applicant as required by the CPS using the format set forth at 28 U.S.C. 1746 (declaration under

penalty of perjury)

- Unique identifying number(s) from the ID(s) of the applicant
- The biometric of the applicant
- The date and time of the verification
- A declaration of identity signed by the applicant using a handwritten signature and performed in the presence of the person performing the identity authentication, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury).

In all cases a biometric of the applicant (e.g., a photograph and fingerprint in accordance with FIPS 201) shall be recorded and maintained by the Issuer (as defined in the RPS) to establish an audit trail for dispute resolution. (Handwritten signatures and other behavioral characteristics are not acceptable as biometrics for the purposes of this environment.)

Certificates issued on a FiXs®-Certified Credential shall be delivered via a GSA FIPS-201 approved CMS, refer to FIPS 201 Evaluation Program Approved Product List (<http://fips201ep.cio.gov/apl.php>).

The RPS will also define the process for the periodic FiXs® File Updates, in accordance with Section 1.2.7.1 of the FiXs® Operating Rules. In particular, a mechanism will be defined that will require the Subscribing Party to verify the Credential Holders authority to hold a FiXs®-Certified Credential. It is the responsibility of the FiXs®-Certified Credential Issuer to ensure proper firewall connectivity in order to receive, accept, process, and internally disseminate (if necessary) these updates. As a requisite for continued use of the FiXs®-Certified Credential, the FiXs®-Certified Credential Issuer must receive periodic updates from the FiXs® Sponsor's Program Manager, or his/her designated agent on behalf of the applicant. This verification shall be in writing and signed, or digitally signed, with an active FiXs®-Certified Credential or CAC credential using a Medium Hardware Assurance certificate.

2.6 Life Cycle Technical Controls

Individuals with FiXs® “trusted” roles shall use security management tools and procedures to ensure that the operational systems and networks adhere to the security requirements that check the integrity of the system data, software, discretionary access controls, audit profiles, firmware, and hardware to ensure secure operation.

Security management controls shall include the execution of tools and procedures to ensure that the operational system and network adhere to configured security. These tools and procedures include checking the integrity of the security software, firmware, and hardware to ensure their correct operation.

Components used for the issuance of FiXs®-Certified Credential shall be protected at the border and protection rules monitored. A network traffic recording, intrusion detection, and forensic analysis system shall be used to monitor intrusion attempts and policy verification (rated at EAL 2 in accordance with Intrusion Detection System Protection Profile (IDSPP)). Firewall, IDS, and network system configurations shall be documented and updates controlled and documented. Weekly review of the firewall and network system configurations against installation plans and procedures shall be made to ensure that no unauthorized changes are made to these systems. Detailed procedures for maintaining and inspecting the Firewall/ IDS and network devices and any anomaly detected shall be documented.

2.6.1 PHYSICAL SAFEGUARDS

Physical security safeguards and access controls shall continuously provide for protection against access or modifications to hardware/ software by unauthorized individuals. Hardware tokens will be stored in a security container. The CPUs, Redundant Array of Inexpensive Disks (RAID)/ external drives, monitors, keyboards, and mice will be sealed with Tamper Resistant Seals in accordance with paragraph 8-308, ISM and Tab B, Code A, Quantum Information and Computation (QUIC); in order to detect surreptitious entry into the equipment and associated peripherals. The seal will be inspected (and results logged) every month to ensure that it serves its intended use.

2.6.2 ACCESS CONTROLS

Unescorted entry to the facility hosting the CMS or access to any server components (hardware/ software) shall be limited to personnel who are cleared for access and whose need to access the components has confirmed.

2.6.3 EQUIPMENT

A FiXs®-Certified Credential CMS server is to be dedicated to administrating the system and shall only have software installed necessary to perform CMS functions. All upgrades will be from the original equipment manufacturers and software vendors.

2.6.4 UPGRADES

The configuration of related systems, as well as any modifications or upgrades, shall be documented. These systems shall have the capability installed and operating to detect unauthorized modifications to these systems software and configurations.

2.6.5 DEVELOPMENT ENVIRONMENT SECURITY

Assembly and maintenance of related systems will be accomplished in the controlled environment. Only designated personnel will perform maintenance on the related system.

2.6.6 CONFIGURATION MANAGEMENT SECURITY

Issuing related system(s) Configuration Management (CM) records shall be maintained and controlled (stored in a locked container).

2.6.7 NETWORK SECURITY CONTROLS

Access to any enrollment/ issuance data shall be protected. The issuer organization will certify compliance with these requirements, in writing to within the constraints of the RPS, annually.

2.7 Uniqueness Across the FiXs®-Certified Network

Each FiXs®-Certified Credential Issuer shall enforce credential uniqueness and ensure the following:

- The applicant does not hold an active FiXs®-Certified Credential
- The name contains the applicant's identity and organization affiliation that is meaningful

to humans

- The naming convention is as described in the corresponding CP and CPS

Practice note: *This does not prevent devices from sharing a Fully Qualified Domain Name (FQDN) as CN.*

Each FiXs®-Certified Credential Issuer will support special procedures that ensure that each individual holds only one active FiXs®-Certified Credential.

In all cases a biometric of the applicant (e.g., a photograph or fingerprint) shall be recorded and maintained by the FiXs®-Certified Credential Issuer to verify uniqueness across the FiXs®-Certified Network and establish an audit trail for dispute resolution (handwritten signatures and other behavioral characteristics are not accepted as biometrics for the purposes of this requirement). Prior to credential issuance the FiXs®-Certified Credential Issuer will verify that the FiXs®-Certified Credential holder's biometric does not exist in any FiXs®-Certified Domain Server.

Practice note: All certificates issued on a *FiXs®-Certified Credential Issuer* shall be issued via a GSA FIPS-201 approved CMS, refer to FIPS 201 Evaluation Program Approved Product List (<http://fips201ep.cio.gov/apl.php>).

Additionally, the FiXs®-Certified Credential Issuer shall record the process (es) followed for issuance of each certificate. The process documentation and authentication requirements shall include the following:

- The identity of the person performing the identification
- A signed declaration by that person that he or she verified the identity of the Applicant as required by the CPS using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) and that he or she verified, via the FiXs®-Certified Credential Network that the applicant does not hold another FiXs®-Certified Credential
- Unique identifying number(s) from the ID(s) of the applicant, or a facsimile of the ID(s)
- The biometric of the applicant
- The date and time of the verification
- A declaration of identity signed by the applicant using a handwritten signature that includes that assertion that the applicant does not hold another FiXs®-Certified Credential, performed in the presence of the person performing the identity authentication, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury).

3 SPONSORING ORGANIZATIONS INTO THE FiXS®-CERTIFIED NETWORK

Primary Trusted Organizations (PTO) and/or Subscribers are known as "Sponsors". They sponsor individual users who are employees or contractual agents of the Sponsor to receive a FiXs®-Certified Credentials and into the FiXs®-Certified Network by assuming responsibility for the acts and omissions of the Participants they sponsor.

3.1 Vetting

Any organization applying to be a PTO or Sponsor must be vetted by a FiXs®-Approved Vetting Organization.

3.2 Sponsorship of Employees

To sponsor an employee and/or contractual agent to receive a FiXs®-Certified Credentials and into the FiXs®-Certified Network, the Sponsor must assert in writing to the FiXs®-Certified Credential Issuer that its employees, contractual agents, or other users have a bona fide need a FiXs®-Certified Credential. The Sponsor must indemnify FiXs® and FiXs® Member Organizations that provide services in support of FiXs®, for the acts and omissions of the applicants it sponsors through the execution of a Terms of Use Agreement.

3.3 Adhere to FiXs® Foundational Documents

Sponsors must abide by the Terms of Use Agreement, adhere to the governance framework as provided for in the FiXs® Foundational Documents, and adhere to the seven-step credential management process outlined in the Trust Model.

3.4 PROCESS FOR ENABLING SPONSOR ORGANIZATIONS

In accordance with FiXs®' agreements for populating the metadata tables to inter-operate with the DCCIS Gateway Broker and the FTB, updated versions of the FiXs® Assigned Commercial Organization Codes table will be provided to the Department of Defense (DoD) on a regular basis. The criteria for providing these updated are as follows:

1. All firms who apply for FiXs® membership will be subject to the standard FiXs® organizational vetting process.
2. Upon successful adjudication of the vetting process FiXs® and acceptance into membership in FiXs®, a unique organizational code will be assigned and maintained in a local FiXs®-Certified database.
3. FiXs® will then query the newly vetted company and ascertain if they have a need/requirement to have FiXs®-Certified Credentials issued to their employees and/or contractual agents.
4. If the company respond affirmatively and intends to have FiXs®-Certified Credentials issued to their employees and/or contractual agents, they will be asked to sign the FiXs® standard "Terms of Use Agreement". This agreement is a legal document which compels the company to abide by all these FiXs® Operating Rules; policies; standards; security requirements; and audit procedures.
5. Upon the proper execution of this document, FiXs® will then notify DoD via formal letter entitled, "FiXs® Assigned Commercial Organizational Codes," and request DoD coordination on adding the company's organization code to the metadata table.

6. DoD will turn around the request within 72 hours.
7. FiXs® will load the Organization Codes in the FiXs® Trust Broker and DoD will load the Organization Codes in the DCCIS Trust Broker and then the next time the Brokers synch, the updates will be reflected in both tables.
8. FiXs® will maintain a repository of all executed Terms of Use Agreements and DoD will have access to that repository.
9. The Terms of Use Agreements will be subject to audit and process review by both the FiXs® audit team and the DoD audit team.
10. This process is to be set forth in the MOU between DoD/DMDC and FiXs®.
11. All companies are subject to the described process before FiXs® will notify and coordinate with DMDC on updates to the metadata tables.
12. FiXs® also maintains a process of assigning a unique system that is comparable to a FASC-N code for all FiXs®-certified FiXs®-Certified Credential Issuers. These codes will be assigned sequentially.

4 RELYING PARTY RESPONSIBILITIES

FiXs® Relying Parties are responsible for electronically authenticating FiXs® Participants who visit their facilities. This chapter describes the responsibilities of Relying Parties in the FiXs® system. Relying parties are also those persons and entities that accept and rely upon FiXs®-Certified Credentials for purposes of verifying digital signatures. A Relying Party is an individual or organization that, by using another's certificate can:

- Verify the integrity of a digitally signed message.
- Identify the creator of a message, or establish confidential communications with the holder of the certificate.
- Rely on the validity of the binding of the credential holder's name to a public key.

A Relying Party, at their own risk, may use information in the certificate (such as certificate policy identifiers) to determine the suitability of the certificate for a particular use.

To assist Relying Parties to meet their responsibilities for logical authentication a FiXs® Relying Parties are responsible for electronically authenticating FiXs® Participants who visit their facilities. This chapter describes the responsibilities of Relying Parties in the FiXs®-Certified System to provide the following:

- Clear verification of medium hardware assurance via Federal OIDs, as stipulated in Section 1.6
- Unique identity across all FiXs®-Certified Credentials
- Identification of FiXs® assurance level
- Highly available revocation information
- The assurance of a FiXs®-Certified Credentials, as stipulated in these FiXs® Operating Rules, that includes a background investigation of all Level 3 and 4 FiXs® credential holders

4.1 Visitor Transaction Processing

In the FiXs®-Certified System, the Relying Party will be responsible for initiating and processing the transactions that will authenticate the FiXs® Participant.

4.1.1 CREDENTIAL VALIDATION AND TRANSACTION ROUTING

The processing or re-routing of a transaction to the FTB is determined at the Relying Party's FDS. When compiling an Authentication Inquiry, the software determines whether it is a home or remote transaction and transmits the Inquiry either to its FDS or to the FTB for routing to the appropriate Member's FDS. A **Home Transaction** refers to an Authentication Inquiry that is processed at the same FDS as the originating Relying Party. In this case, the employee is being authenticated at an employee facility. A **Remote Transaction** refers to an Authentication Inquiry that is routed through the FTB to be processed at a FDS other than of the originating Relying Party. In this case, the employee is a visitor to the location of the Authentication Station. The credential validation is processed as described in the sections that follow:

4.1.1.1 Initiating Authentication Inquiry

When a visitor arrives, the Authentication Station Operator asks whether the individual is a FiXs® member. If yes:

4.1.1.1.1 Enter Data to FiXs® Application

The FiXs®-Certified Authentication Station Operator selects the visitor's home organization on the first FiXs® screen. The system displays instructions as to what data to enter or which credentials to use for authentication. Depending on the level of the credential being read, the FiXs®-Certified Authentication Station Operator will be instructed to perform one of the following procedures:

4.1.1.1.1.1 READ BAR CODE DATA

The FiXs®-Certified Authentication Station Operator inserts the token/badge into the bar code reader, which reads the ID number and transmits it as a string of data to the FDS.

4.1.1.1.1.2 READ CAC CHIP DATA

The FiXs®-Certified Authentication Station Operator inserts the CAC card into the smart card reader. The FiXs® Participant enters his/her PIN using either a PIN pad or keyboard and a string of data is extracted from the card chip and sent to the FDS.

4.1.1.1.1.3 REQUEST EMPLOYEE ID NUMBER

The FiXs®-Certified Authentication Station Operator will be required to request and enter the employee's ID number into the Authentication Web Application Software.

4.1.1.2 Transaction Routing

Using the organization data selected, the Authentication Inquiry with the credential information can be routed to the record-holding FDS. A transaction is a "home" or "remote" transaction as described below.

4.1.1.2.1 Home Transactions

If the FiXs®-Certified Authentication Client determines that a request can be processed internally, this is a Home transaction. In this case, the Relying Party's FDS processes the transaction in the same manner as described below in Section 3.1.2; however, the transaction is locally processed and no data is transmitted to the FTB.

4.1.1.2.2 Remote Transactions

If the FiXs®-Certified Authentication Client determines that a request cannot be processed internally based on the selected organization code, it then creates an Authentication Inquiry and

fowards it to the FiXs® Trust Broker for processing as per Section 3.1.2 below.

4.1.2 PROCESSING AUTHENTICATION RESPONSES

Based on the information the FiXs®-Certified Authentication Station Operator submits during the visitor intake process, the system will return instructions to perform one or more of the following transactions to authenticate the individual.

4.1.2.1 Complete Credential Holder Authentication

To complete an authentication transaction, the FiXs®-Certified Authentication Station Operator must perform one or more of the following operations.

4.1.2.1.1 *Visual Comparison of Downloaded Photo to Badge Holder*

The FiXs®-Certified Authentication Station Operator visually compares the photo transmitted from the server or downloaded from the card to the Credential Holder/Visitor. The Operator enters the results of the visual match onto the FiXs®-Certified Authentication Client application.

4.1.2.1.2 *Biometric Scan and Comparison*

The FiXs®-Certified Authentication Station Operator instructs the visitor to initiate a biometric scan using the fingerprint reader. The system performs a comparison against the downloaded biometric and indicates the results of the comparison on the FiXs®-Certified Authentication Client.

4.1.2.2 Determine Access Authorization

Based on the results of the authentication process, the FiXs®-Certified Authentication Stations Operator decides whether the FiXs® Participant will be offered access based on local operating procedures. The FiXs®-Certified Authentication Station Operator shall enter his or her decision into the FiXs®-Certified Authentication Station and the decision shall be recorded in the system Audit Log. Note that the FiXs® authentication process does not automatically authorize access; it is only an authentication procedure. Access decisions will always be left to the discretion and procedures established at the Relying Party's organization.

4.2 Exception Processing

Exception Processing refers to the procedures that will be followed when the FiXs System as per the normal procedures described in these Operating Rules cannot authenticate a credential or participant. The requirements for addressing these conditions are described in the section that follows.

4.2.1 BADGE/TOKEN-NOT-PRESENT

In the event that an individual claiming to be a FiXs Participant requests entry to a FiXs Member facility but does not have a badge or token, the Authentication

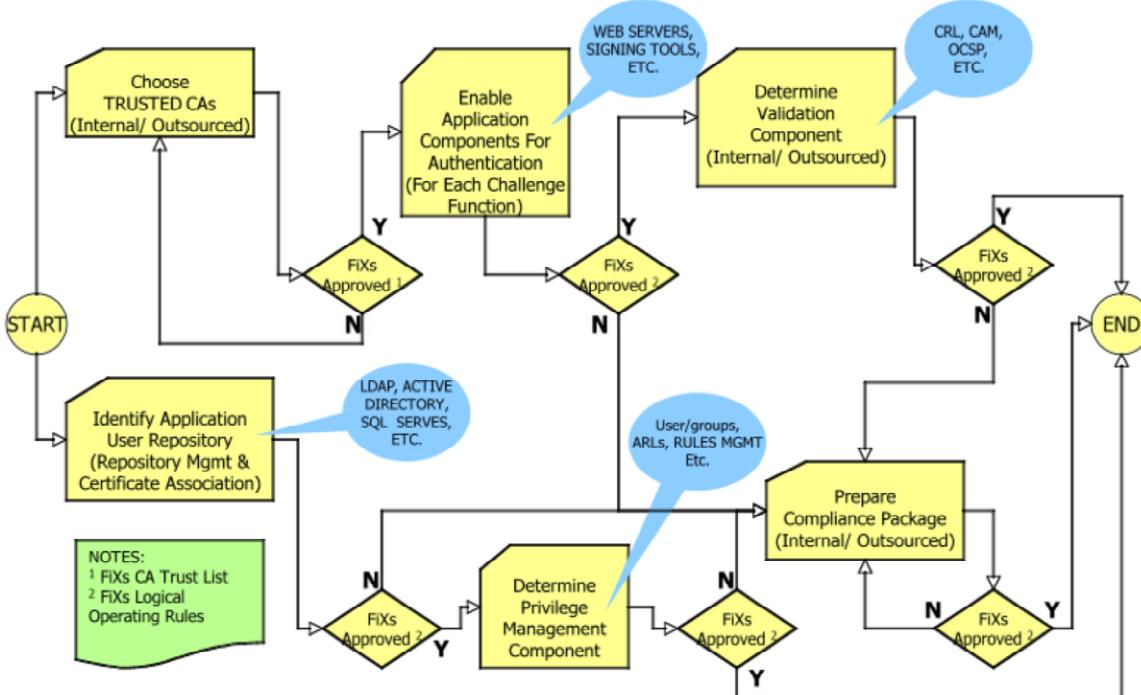
Station Operator will ask for the individual's company name and Employee ID number and continue with the normal authentication procedures as described in Section 3.1.1.1.

4.2.2 OTHER EXCEPTIONS

In the event that an individual claiming to be a FiXs Participant cannot be authenticated by means of a FiXs Authentication Inquiry/Response, then the individual cannot be admitted as a FiXs Member and the entry admittance process can no longer be considered a FiXs Transaction. In such cases, the Relying Party Organization may choose local security processes and procedures to allow or deny admittance. Such exception conditions can include, but are not necessarily limited to: unrecognized participant, unreadable badge/token and inability to reach an employer's FDS (issuer system down, FiXs Trust Broker down, relying party system down, etc.).

4.3 Application Provisioning

In the FiXs®-Certified System, the Relying Party will be responsible for initiating and processing the transactions that will validate the FiXs® participant's digital certificate. A relying party must determine the level of assurance (or trust) that will be acceptable for authenticating to a particular application or network.



4.3.1 TRUST DETERMINATION TECHNIQUES AND PARAMETERS

A FiXs® Relying Party can establish cross-domain PKI trust using a variety of techniques. Manually, a relying party can review and add the appropriate trust anchors for each applicable PKI into their application or network trust store(s). A

FiXs®-Certified Validation Service can be used to automate this by providing trust based on (a) path discovery and path validation, and/or (b) specific trust lists either derived from the Federal Bridge Certificate Authority.

4.3.2 ENABLE APPLICATION AUTHENTICATION

Possibly the single most important function the digital certificates on the FiXs®-Certified Credential can perform for Relying Parties is Identification and Authentication for applications and implementing such that it builds a Reduce Sign On (RSO) enterprise.

FiXs® Relying Parties need to be cognizant of X.509 Digital Certificate technology in order to plug directly into the FiXs® recognized PKIs. In order to use certificates for user authentication, an application today needs to recognize and correctly use Trusted Third Party (TTP) certificates. The application needs to correctly parse the CA chain hierarchy containing a Root CA, Intermediate CA and End Entity certificates.

4.3.2.1 APPLICATION (COMPONENT) CERTIFICATES

Relying Party computing and communications components (web servers, routers, firewalls, authentication stations, etc.) may be named as certificate subjects. In such cases, the component must have a human PKI Sponsor as described in the ECA CP. The PKI Sponsor is responsible for providing the approved Registration Authorities, through an application form, correct information regarding:

- Equipment identification
- Equipment public keys
- Equipment authorizations and attributes (if any are to be included in the certificate)
- Contact information to enable the ECA to communicate with the PKI sponsor when required in accordance with the appropriate CPS.

4.3.2.2 APPLICATION (COMPONENT) PRIVATE KEY PROTECTION

At a minimum FiXs® Relying Party computing and communications components (web servers, routers, firewalls, authentication stations, etc.) shall protect the certificate private key(s) in a hardware device such as a Trusted Platform Module, as stipulated in the DoD CIO Memorandum, *Encryption of Sensitive Unclassified Data at rest on Mobile Computing Devices and Removable Storage Media*, dated July 03, 2007.

4.3.3 USER REPOSITORY/ PRIVILEGE MANAGEMENT

Possibly the single most important function the digital certificates on the FiXs®-Certified Credential can perform for Relying Parties is Identification and Authentication for applications and doing it in a way that builds a Reduce Sign On (RSO) enterprise. Arguably, the most important part of any application is the design of the user database. Many times the user database becomes a stovepipe database joining hundreds of others for which each user must have a name and password. Additionally, the application program office must take on the responsibility of verifying the identity of individuals before they are given an

account. The Federal PKIs provide an efficient and elegant method to solve this most important aspect of application development.

Managing access control efficiently remains a challenge. In a broad sense, there are two prevalent types of applications. One type has many users across regions and would benefit from the integration of role-based access. The other type has fewer users and requires a higher degree of assurance in explicitly granting and denying access. Although the integration of the digital certificates on FiXs®-Certified Credentials into access control can help with the problem of expired accounts and globally revoked access, it does not address the general access management problem. The use of directories can provide support, but only if both types of access requirements are addressed.

4.3.3.1 Basic Access Control

Individual certificates include a Distinguished Name (DN), which contain as a minimum, a common name, organization and country; and, may contain organizational units. This information constitutes a branch in the Directory Information Tree (DIT). For some applications, digital certificates containing a branch within the DIT (e.g., Service, specific contractor affiliation, foreign national, etc.) may be satisfactory for access. For this case, access may be granted to all holders of approved certificates within the tree branches accepted by the server. For example, by configuring an open systems secure web server to trust ECA certificates, a particular web enabled database could allow access to only ECA certificate holders with a ou=<any>. The application would then only allow user or external application interactions through that authenticated route. For all other potential activity, its resources and that of its server would be unavailable or strictly controlled.

4.3.3.2 More Defined Access Control

Some Relying Party applications may require stricter access control based on the identity of the certificate holder. This is a local issue managed by the server administrator. In this case, the application not only needs to authenticate the user, but provide a mechanism that determines roles and privileges based on user identity. For example, affiliated users may be able to view data posted by a specific application; however, to make changes or updates to that data, it may be necessary for the user to be a member of a small sub-group that is not identified by the certificate.

The Relying Party's application must have a repository of access control information that facilitates the desired privilege control based on the user identified in the certificate. The repository would contain entries for all registered users of any application within the network (Note: It does not need contain user entries for all certificate holders within the FiXs® community) and contain groups representing roles and access privileges. In many cases, this information would parallel user name and password repository information currently employed by the application.

Application owners can also determine if existing roles meet access requirements or provide a group manager who can maintain explicit access permissions. Given

this capability, the Relying Party can then apply its own local access rules to ensure only those with a need to know can access particular data files. By using an open systems LDAP directory (to manage users and groups/roles), access control management can be accomplished across the Internet securely. The application may also maintain the access control lists that reside in another repository at the discretion of the application manager. This approach is particularly efficient when user roles, privileges and allowed accesses change frequently, and when an enterprise contains diverse applications.

4.3.3.3 Access Control Mechanisms

The mechanism by which an enterprise repository should be populated with user information must be addressed. By using a secure repository gateway, first time users can establish accounts by presenting their certificates to a directory validated by the gateway. A registration request web form can be used to create a user account, based on the user certificate presented, and to record access privilege request information. Upon reviewing the requests of the user, each application owner can assign privileges to individual accounts, confident of the identity of the requester. Alternatively, the application owner can make provisions for bulk registration by downloading certificate information, in whole or part, from each trusted CA repository.

Many applications use a DBMS to hold the user database. Web applications may use the authorization features of the DBMS or the authorization features of the web server. Many web applications have web servers with mechanisms that interoperate with LDAP directories.

A common scenario is for local application and process owners to independently manage user access and privileges via access control lists (ACLs) or similar mechanisms on the application server. This is done on a recurrent, dynamic, ongoing basis across the enterprise for each and every different application environment --- quite a significant amount of overhead when viewed as an aggregate effort, enterprise-wide.

A directory can be the repository for user information, user public key certificates, and lookup information (email, phone, address, etc.). Numerous commercial organizations have reduced administrative costs and increased administrative accuracy and efficiency by leveraging an enterprise directory as a unifier and control mechanism; for example, by integrating human resources and network access controls with the enterprise PKI and its directory. Application access and privilege management can also be automated using the existing repository of a PKI, reducing administrative overhead and strengthening ownership controls, with minimal impact to existing application systems. This approach retains full control for the data owners within strict accordance to enterprise security policies. The repository can accommodate access control and other user information (attributes) down to the individual entry, so that it can be used to implement security policies as well as application owner-directed access control. Servers can build and store ACLs using the users and groups/roles according to the application owners controlled processes.

4.3.4 DIGITAL SIGNATURES AND STORAGE CONSIDERATIONS

If you are receiving or collecting something that is signed digitally, whether once or several times by several signatories, you must have (1) a means to capture the form and the data on that form; (2) a means to capture the signature (hash) and the public key to decipher the hash and (3) a validation of the signature at that time and place (proven time-stamp).

This means the recipient will need three signatures to establish non-repudiation of the signed document/ form. First is the signature of the person or persons who signed the form; second is the signature of the validation mechanism; and third is the signature of the time stamping entity.

To complete the transaction and provide a complete record for the recipient and the provider, a receipt (also signed and date-stamped) could be provided and filed with the document/form.

As a related matter having nothing to do with non-repudiation, the recipient must be able to use the information received, so his file must be such that the data on the form can be parsed and reassembled, sorted and/or collected with other information received from other providers.

At the time the information is first received, recall and use of the information is straightforward, but many users do not consider the fact that they must be able to determine non-repudiation of electronic data and electronic signatures years later, just as is required for signed (paper) legal documents. In order to do this, one must be able to recreate the ability to decipher the information using a public key no longer in use, and prove the signatures were valid at the time they were affixed.

This means the recipient will need three signatures to establish non-repudiation of the signed document/form. First is the signature of the person or persons who signed the form; second is the signature of the Validation Authority; and third is the signature of the time stamping entity.

4.4 Documenting Compliance

FiXs® certified Relying Parties operating under the standards of the Federation, shall conduct a compliance audit no less than once every three (3) years. Additionally, the FiXs® has the right to require periodic or ad hoc inspections.

4.4.1 IDENTITY/QUALIFICATIONS OF COMPLIANCE AUDITOR

The auditor must demonstrate competence in the field of compliance audits, and must be thoroughly familiar with the CPS' and CP's trusted by the Relying Party.

4.4.2 COMPLIANCE AUDITOR'S RELATIONSHIP TO AUDITED PARTY

The compliance auditor either shall be a private firm, which is independent from the entities being audited, or it shall be sufficiently separated organizationally from those entities to provide an unbiased, independent evaluation. An example of the latter situation may be the approach of an Agency Inspector General. The FiXs® shall determine whether a compliance auditor meets these requirements.

The Relying Party is responsible for identifying and engaging a qualified auditor of

operations.

4.4.3 LIFE CYCLE MANAGEMENT STRATEGY

The most important features of sound life cycle management are:

- Keeping the system fully functional throughout installation of any change;
- Ensuring security is not breached and the auditability of system security is maintained throughout;
- Ensuring system archives are unaffected and the ability to retrieve signed documents is maintained;
- Developing a rigorous and comprehensive test and evaluation process as part of the planning for each step of the modernization;
- Ensuring training is conducted for operators and managers beforehand such that personnel are fully prepared to deal with display and procedural changes.

5 FiXs®-CERTIFIED TRUST BROKER (FTB) RESPONSIBILITIES

This Section describes the responsibilities of FTB in the FiXs®-Certified System. Serving as the operation intermediary between the FiXs®-Certified Credential Issuers and Relying Parties, the FTB is responsible for management and administration of the FTB function as well as the day-to-day operations of the FTB including system administration. These requirements are described in the sections that follow.

5.1 System Administration Requirements

This section describes the system administration requirements associated with the FTB.

5.1.1 DESIGNATE FTB SYSTEM ADMINISTRATOR

Any organization that has a component that connects to the FTB must designate an Administrator. The Administrator shall be responsible for the tasks described in Sections 5.1.2 and 5.1.3.

5.1.2 MEMBER INTERFACE MANAGEMENT

The Administrator is responsible for configuration management of the FiXs®-Certified System communications and interfaces.

5.1.3 MAINTENANCE OF CONTROL DATA

The Administrator is responsible for maintaining a set of control tables that is used to share and update FiXs® Member organization names, characteristics, and list of acceptable tokens. In this role, the FTB must update the control tables upon activation of new FiXs® Member Organizations; de-activation of existing FiXs® Member Organizations and Participants; and changes submitted by existing FiXs® Member Organizations and Participants. Control table changes are transmitted to all FDSs on a regular and frequent basis. Upon receiving changes to the control tables from FiXs® Members, the FTB must update them as soon as possible, but no later than 24 hours after receiving the changes.

5.1.3.1 FiXs Node Transacting with DMDC

Each FiXs nodes to be added to the FTB for the purpose of transacting with DMDC shall be formally presented to the FiXs Configuration Control Board (CCB) for review and acceptance. After the node has gone through formal "testing" in the FiXs-Certified Test/ Lab environment it will undergo a Certification and Accreditation with the FiXs-Certified Network Provider prior to approval.

5.1.3.2 FiXs Node Approval

Each FiXs node must be approved by the FiXs DAA for IATO and ATO matters, who will be the "Authorizing Agent" for additions to the Network, in accordance with the FiXs Certification and Accreditation process.

5.1.4 ACTIVATION AND DE-ACTIVATION OF FiXs®-Certified DOMAINS

Upon authorization of the Administrator of connecting components, the FTB Administrator will activate and de-activate FDSs from the FTB.

5.1.4.1 Initiation of Domain Enrollment Process

For security purposes, Domain Enrollment Process Initiation begins with

the Member's official representative signing the trading partner agreement using a "chain-of-trust" process linked to the Member's first system enroller. Membership in the FiXs®-Certified System is initiated when a senior management representative of the applying Member Company or organization signs a trading partner agreement with the Operating Entity. (For the POC and pilot, the Operating Entity is the DMDC.) A letter is sent to the Operating Entity (DMDC) by the authorized representative appointing two individuals from the company or organization to serve as the Domain Technical Administrator and the first Facility Enroller.

The Operating Entity sends an Authorized Agent to the company location to officially open the FDS and to witness the initial enrollees being entered into the FiXs®-Certified System. (This Authorized Agent's credentials were included on the application prior to delivery to the company or organization.) At the same time, the credentials of the Authorized Agent are removed from the FDS. This process is certified on paper by the Authorized Agent and the company/organization representative and is placed in the audit files of the new Member and of the Operating Entity.

Refer to the *FiXs® Technical Architecture and Specifications* regarding key management associated with this Initiation of Domain Enrollment Process.

5.1.4.2

Activation of FiXs®-Certified Domains

For new FiXs® Members, a FDS ID will be assigned to the new FDS and entered into the system along with contact and control information. The control information will then be transmitted to other FDSs. Upon receiving notification of activation of a new Participant, the FTB Administrator must update the Control Tables as soon as possible, but no later than three (3) hours after receiving the notification.

5.1.4.3

De-Activation of FiXs®-Certified Domains

For dis-enrollment of FiXs® Member Organizations, the FDS ID will be de-activated in the FiXs®-Certified System and contact and control information removed. Notification of de-activation will then be transmitted to the remaining FDSs.

5.1.4.4

Dis-Enrollment, Reinstatement and Re-Enrollment of Participants

Upon receiving notification that a Participant is no longer eligible to be included in FiXs®, the FTB Administrator must dis-enroll them as soon as possible, but no later than three (3) hours after receiving the notification.

Upon receiving notification that an employee who was formerly enrolled in the system is again eligible for enrollment, the Facility Enroller can reinstate the employee into the FiXs®-Certified Data Repository without conducting the identity vetting process specified under 2.1.2, Verify Applicant Identification (Vetting/Identity Proofing), provided the reinstatement occurs within twelve (12) months of dis-

enrollment.

If an employee becomes eligible for enrollment twelve (12) months after dis-enrollment, the employee must be re-enrolled in accordance with Section 2.1.3.

5.1.5 SYSTEM PERFORMANCE REQUIREMENTS

The FTB must be operational 24 hours a day, 7 days a week, with an up-time availability of 99.99%. Authentication Inquiry Transactions must be transmitted to the FiXs®-Certified Credential Issuing FDS in no more than 2.5 seconds. Authentication Responses must be processed and transmitted to the Relying Party in no more than 2.5 seconds.

5.2 Transaction Processing and Routing

The FTB must route and process transactions between FiXs®-Certified Credential Issuers and Relying Parties. The FTB receives Authentication Inquiries from Relying Parties and transmits them to FiXs®-Certified Credential Issuers for processing. It then receives the Authentication Responses and relays them back to the appropriate Relying Parties. In addition, the FTB Administrator performs control data transactions. Refer to the *FiXs® Technical Architecture and Specifications* for transaction/message format and encryption requirements.

5.2.1 AUTHENTICATION INQUIRIES

When a transfer is sent from a Relying Party to the FTB requesting authentication of a FiXs® Participant of a Remote FiXs®-Certified Credential Issuer, the FTB: 1) decrypts the header to determine the FDS destination; 2) validates the digital signature of the originating FDS; 3) adds FDS control data to the transfer and re-encrypts it; and 4) transmits it to destination FDS.

5.2.2 AUTHENTICATION RESPONSES

When a remote FiXs®-Certified Credential Issuer returns an Authentication Response, the FTB: 1) decrypts the transfer; 2) adds FDS control data to the response and re-encrypts it; and 3) transmits the response to the Relying Party.

5.2.3 AUDIT CONTROL DATA TRANSACTIONS

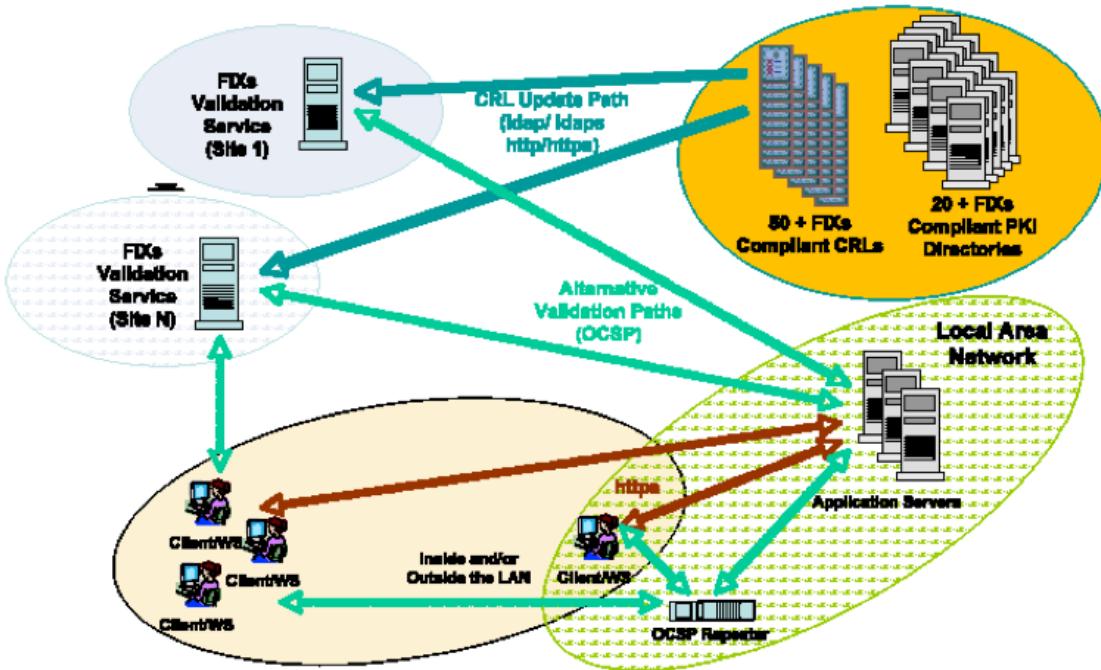
The FTB must notify FDS domains of control table updates by: 1) updating the internal Control Date and Time that accompanies all transfers, and 2) responding to FiXs®-Certified Control Data Requests with a FiXs®-Certified Control Data Response that updates control data and resets the Control Date and time in the FiXs®-Certified Domain(s).

5.3 FIXS®-CERTIFIED CERTIFICATE VALIDATION

A FiXs®-Certified Validation Service is a FiXs®-Certified Network component, similar to a trust broker that provides revocation status. A FiXs®-Certified Validation Service Provider shall conform to the stipulations of the CPs for which it serves validation information. All FiXs® Validation Service Provider practice updates, as well as any subsequent changes will be updated in their compliance documentation and submitted to the FiXs® Board for conformance assessment. The Validation Service Provider practices include:

- Conformance to the stipulations of the US Government CPs
- Ensuring that certificate and revocation information is accepted only from valid CAs
- Include only valid and appropriate responses
- Maintain evidence that due diligence is exercised in validating certificate status

A FiXs®-Certified Validation Service Provider resides on the FiXs®-Certified Network as depicted in the figure below.



A FiXs®-Certified Validation Service Provider provides OCSP responses to credential holders and is responsible for:

- Providing certificate revocation status to the Relying Parties upon request
- Ensuring that the status and validation responses contain authentication and integrity services commensurate with the assurance level of the certificate being checked
- Two party administration of the Validation Service Components

A FiXs®-Certified Validation Service Provider shall ensure that:

- An accurate and up-to-date CRL, from the authorized CA, is used to provide the revocation status
- Revocation status responses provide authentication and integrity services commensurate with the assurance level of the certificate being checked

5.4 TRUST DETERMINATION

A FiXs®-Certified Validation Service shall support different validation parameters (i.e., a list of trust anchors, or a list of CAs on a trust list), and shall support applications selection of these parameters by applications for validation based on rules provided by the application and specific instructions provided in the validation request.

In some cases, the type of trust determination possible is dictated by the validation request protocol. For example, in OCSP, only hashed data from the certificate is provided, rather than the certificate itself. In general, this precludes path discovery and validation, which require the entire certificate to seed the process. For OCSP, the Federal Government recommends a trust list based trust based validation process.

In cases where the specifics of the request protocol do not preclude particular trust determination techniques, a validation service can provide a variety of techniques. At a minimum, a FiXs®-Certified Validation Service shall be capable of providing trust based on both (a) path discovery and path validation, and (b) trust lists.

The FiXs®-Certified Validation Service shall support the application's capability to specify validation parameters either as required settings for all validation requests from the application, or by providing a default with the option of per-request overrides of the path settings when transmission of per-request settings is supported by the validation protocol.

5.4.1 PATH-BASED TRUST

For path-based trust, the FiXs®-Certified Validation Service shall support the application's capability to specify (at a minimum) allowable trust anchors and has the option of setting path processing starting point policy requirements. For trust lists, a FiXs®-Certified Validation Service shall support the application's capability to be able to list either the direct issuing CA or the hierarchical root of the issuing chain.

5.4.2 VALIDATION PROTOCOLS

For validation protocols that do not provide a mechanism for the application to identify themselves (and thus select their validation parameters), a FiXs®-Certified Validation Service shall provide a method outside the protocol for identification of the requestor, such as identifying the network address from which an address comes, or by providing different service network addresses to each application.

This validation parameter selection mechanism shall also be extensible such that an application may have multiple validation parameter sets that they may utilize. For example, this could be implemented by an application using multiple "virtual" identities, each of which select a particular set of validation parameters.

5.4.3 OTHER TRUST DETERMINATION TECHNIQUES

There are other possibilities for trust determination. For example, an application manager may decide that it must determine trust locally and wish to utilize the FiXs®-Certified Validation Service for a near real-time status check only, or it may designate an external service for trust determination.

FiXs® shall take these trust determination options, and the possibility of future options, into account when enhancing their technical architecture.

5.4.4 CHECKING CERTIFICATE REVOCATION LIST

FiXs® standards support checking of CRLs to determine certificate validation status, online, near real-time, including all subtypes of CRLs (delta, indirect, partitioned, etc). The requirements for path validation of CRLs is provided by the PD-VAL documentation will specify the exact types of CRLs that the FiXs® recognized PKIs process.

As part of the application defined validation parameters, the FiXs®-Certified validation system supports controls over the caching of CRLs. Some applications require constraints on the amount of time a CRL is cached for (or disable caching completely) regardless of the CRL's expiration date. Other applications may require caching of CRLs until their internal expiration.

The FiXs®-Certified Validation Service supports a number of techniques to obtain CRLs, at a minimum: processing CRL Distribution Point (CDP) extensions when present and querying one or more directory systems (such as the FBCA LDAP servers), based on the assumption that CRLs will be stored under the distinguished name of the issuer of the certificate. Optionally, the FiXs® validation system could provide support for a local "hint database" of rules to obtain commonly needed CRLs that are not located by either of the above methods.

The FiXs®-Certified Validation Service could also provide support pre-fetching of large CRL's that particular applications use frequently. This feature would be further enhanced if the FiXs®-Certified Validation Service could automatically determine the list of CRLs that would be useful to pre-fetch, and if the system automatically scheduled downloading replacements when pre-fetched CRLs expire.

5.4.5 ONLINE CERTIFICATE STATUS CHECK

A FiXs®-Certified Validation Service shall support multiple techniques to determine whether OCSP is supported for a particular certificate, and if so, determining the correct OCSP responder to contact. At a minimum, a FiXs®-Certified Validation Service shall support processing the Authority Information Access (AIA) extension to search for OCSP server addresses, and shall support a database of OCSP responders for known CA's that utilize OCSP but do not populate the AIA extension.

A FiXs®-Certified Validation Service shall support the OCSP protocol as specified in IETF RFC 2560 or latest specification. This provides a Managed OCSP responder for applications unable to use AIA fields to directly contact issuer's responders and/or the application-specific trust determination in addition to an online status check.

5.4.6 STANDARD CERTIFICATE VALIDATION PROTOCOL (SCVP)

A FiXs®-Certified Validation Service shall support SCVP, as SCVP is the protocol identified as "proper" by the IETF for use in requesting delegated path validation (DPV). There are a number of features within the SCVP protocol definition that are "optional." That is, it either indicates that a server "SHOULD" or "MAY" support the option or combination of options. For such functionality, FiXs® shall implement the "optional" component if any authorized application requires it. Otherwise the functionality need not be implemented; although the FiXs® validation system

should return a correct “not implemented” code should a request for an unimplemented feature be received.

5.4.7 FULLY PD-VAL CAPABLE WEB SERVERS

A FiXs®-Certified Validation Service shall toolkits that can be plugged into web servers that provide full, pd-val (path discovery and validation). Because this model is necessitated by COTS web server design, but has an unfortunate side effect: if the native mechanism rejects a certificate, the toolkit will never have a chance to validate the certificate. To ensure that the native mechanism does not cause false negatives, the native mechanism requires a high degree of trust. A FiXs®-Certified Validation Service shall maintain a “hints list” approved by the FiXs® Operations Committee.

5.4.8 OTHER TECHNIQUES AND PROTOCOLS

As part of support for application defined validation it is likely that other near real-time, online status checking protocols will come into common use in the future, and/ or that applications may come up with other special exception rules (for example, they may wish to override certificate AIA fields in certain circumstances, or have test certificates return fixed status results without actually processing an on-line check). A FiXs®-Certified Validation Service will update capability as the FiXs® \Operating Rules evolve.

5.5 OCSP Responder Self-Signed Certificate

Any self-signed OCSP responder used for verifying certificates asserting a policy OID reference herein are required to meet the certificate profile stipulated below and the stipulations above.

FiXs® disclaims any liability for loss due to use of any validation information relied on by any party that does not comply with this stipulation.

Note: The following profile is for a FiXs® entity that chooses to deploy a Self-Signed OCSP responder.

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Issuer Distinguished Name	cn=<OCSP Responder Name>, ou=<Company Name>, ou=<CA Name>, o=U.S. Government, c=US
Validity Period	3 years from date of issue in Generalized Time format
Subject Distinguished Name	cn=<OCSP Responder Name>, ou=<Company Name>, ou=<CA Name>, o=U.S. Government, c=US
Subject Public Key Information	1024 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Extensions	Not Present

5.6 OCSP Responder Certificate

Note: This profile is used only for Validation Service Provider

Field	Value
Version	V3 (2)
Serial Number	Must be unique
Issuer Signature Algorithm	Refer to Certificate Policies referenced
Issuer Distinguished Name	Refer to Certificate Policies referenced
Validity Period	1 month from date of issue in UTCT format
Subject Distinguished Name	Refer to Certificate Policies referenced
Subject Public Key Information	Refer to Certificate Policies referenced
Issuer Unique Identifier	Not Present
Subject Unique Identifier	Not Present
Issuer's Signature	Refer to Certificate Policies referenced
Extensions	
Authority key identifier	Octet String, Refer to Certificate Policies referenced
Subject key identifier	Octet String, Refer to Certificate Policies referenced
Key usage	c=yes; nonRepudiation, digitalSignature
Extended key usage	c=yes; id-kp-OCSPSigning {1 3 6 1 5 5 7 3 9}
Certificate policies	c=no; Refer to Certificate Policies referenced
Subject Alternative Name	http URL for the OCSP Responder
Authority Information Access	c=no; caIssuers= <http URL for the issuers root>
No Check	id-pkix-ocsp-nocheck; {1 3 6 1 5 5 7 48 1 5}

5.7 OCSP Request Format

FiXs®-Certified OCSP requests are not required to be signed. A FiXs®-Certified Validation Service's OCSP responder will not check the signature on the request. See RFC2560 for detailed syntax. The following table lists which fields that are required by a FiXs®-Certified Validation Service's OCSP responder.

Field	Expected Value
Version	V1 (0)
Requester Name	Not Required
Request List	List of certificates – generally this should be the list of two certificates: ECA certificate and end entity certificate
Signature	Not Required
Extensions	Not Required

5.8 OCSP Response Format

The following table lists fields to be populated by a FiXs® compliant OCSP Responder. Refer to RFC 2560 for detailed syntax.

Field	Expected Value
Response Status	Successful Malformed Request Internal Error Try Later
Response Type	id-pkix-ocsp-basic {1 3 6 1 5 5 7 48 1 1}
Version	V1 (0)
Responder ID	Hash of Responder public key
Produced At	Generalized Time
List of Responses	Each response will contain certificate id; certificate status ² , thisUpdate, nextUpdate ³ ,
Extension	
Nonce	Will be present if nonce extension is present in the request
Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Signature	Present
Certificates	Applicable certificates issued to the OCSP Responder

² If the certificate is revoked, the OCSP Responder will provide revocation time and revocation reason from CRL entry and CRL entry extension.

³ The OCSP Responder will use thisUpdate and nextUpdate from CA CRL.

6 SECURITY REQUIREMENTS

In addition to the security requirements set forth in this Section the security requirements set forth in the appropriate CP shall be adhered to.

6.1 General Security Requirements

Each Participating FiXs® organization, shall comply with the *FiXs® Security Guidelines*, which specify procedures to prevent unauthorized access or misuse of any FiXs® related component including hardware, software, peripherals, data, system components, network, security keys, credentials and documentation. The *FiXs® Security Guidelines* are hereby incorporated by reference.

6.2 Infrastructure Requirements

The FDS must be capable of supporting HTTPS (SSL) protocol. The Member Organization's network and firewall must be configured to allow HTTPS incoming and outgoing transmissions, with outgoing transmissions being limited to the FTB. In addition, the FDS must be placed within the Organization's firewall. For additional details, please refer to the *FiXs® Technical Architecture and Specifications* and the *FiXs® Security Guidelines*.

6.3 Audit Requirements

Each participating organization is responsible for maintaining complete and up-to-date records of events related to the FiXs®-Certified Network. FiXs®-Certified transactions must be re-creatable from start to finish including identification of the individual(s) performing the transaction. Event logs and transaction audit data will be held indefinitely by each participating organization or until directed otherwise via direction from the FiXs® Program Manager. FiXs® event logs will be maintained in a secure manner and made available for reference from an authorized Government official.

Note that installing the FiXs®-Certified application software ensures compliance with the minimum level of FiXs® auditing requirements.

6.4 Security Authorizations

6.4.1 GENERAL

Authority to access any FiXs®-Certified System component is based upon the required functions associated with the employee's position. Below are functions attributed to specific functions/positions within the FiXs®-Certified Domain that require authorized access.

Note that there can be no duplication in the following roles: 1) the Domain Program Manager cannot serve as either a Facility Enroller or Facility Verifier, and 2) Facility Enrollers and Facility Verifiers must always be separate personnel.

6.4.2 DOMAIN TECHNICAL ADMINISTRATOR

The FiXs®-Certified Facility Domain administrator is authorized to:

- initialize a FiXs®-Certified Domain for enrollment according to the procedures described in Section 4.1.4.1 and authorize the participating organizations initial participants;

- perform all software maintenance and trouble shooting functions. This includes system configuration, network connectivity, database initialization, and installation of Server and client components and peripherals;
- install operating system patches, FiXs®-Certified software and COTS patches; and
- operational and troubleshooting procedures of the local system components, FiXs®-Certified Domain Server FiXs® Clients and FiXs®-Certified Data Repository.

6.4.3 DOMAIN FUNCTIONAL ADMINISTRATOR

The FiXs®-Certified Domain Administrative Enroller is authorized to:

- enroll and train Facility Administrative Enrollers.
- authorize applicants to receive FiXs®-Certified Credentials or to designate other individuals within the facility authorize applicants.

6.4.4 FACILITY DOMAIN ADMINISTRATORS

The FiXs®-Certified Facility Domain Administrator is authorized to enroll, train and certify Authentication Station Operators.

6.4.5 FACILITY ADMINISTRATIVE ENROLLER

The FiXs®-Certified Facility Administrative Enroller authorized to enroll, train and certify Facility Enrollers.

7 LIABILITIES AND INDEMNIFICATION

This Section describes the liabilities associated with participation in the FiXs®-Certified System. In addition, the liabilities and indemnifications stipulated in the appropriate CP shall apply.

7.1 Liability under these Rules

These Rules are made solely and specifically among and for the benefit of Members and Participants. No Person who is not a Member or a Participant shall have any rights, interest or claims under these Rules or be entitled to any benefits under or on account of these Rules, whether as a third party beneficiary or otherwise. A Member or Participant shall have no liability for violation of these Rules to any person who is not a Member or a Participant and the liability of a Member or Participant to any other Member or Participant for any violation of these Rules shall be strictly limited to any remedy or liability provided in Subsection 6.2.

7.2 Liability to Members and Participants

A Member or Participant shall be liable to another Member or Participant for a violation of these Rules to the extent that such liability is provided for under a contract or agreement between individual Members or Participants, all as modified under Subsection 8.1.2 of these Rules, or is provided for under other law, including the SAFETY Act (Pub. Law 107-296) or other applicable federal law.

8 PRIVACY

8.1 Privacy

Member Organizations must comply with the Privacy provisions of the *applicable CPs and FiXs® Policy*, which are hereby incorporated by reference.

8.1.1 BADGE/TOKEN-NOT-PRESENT

In the event that an individual claiming to be a FiXs® Participant requests entry to a FiXs® Member facility but does not have a badge or token, the Authentication Station Operator will ask for the individual's company name and Employee ID number and continue with the normal authentication procedures as described in Section 3.1.1.1.

8.1.2 OTHER EXCEPTIONS

In the event that an individual claiming to be a FiXs® Participant cannot be authenticated by means of a FiXs® Authentication Inquiry/Response, then the individual cannot be admitted as a FiXs® Member and the entry admittance process can no longer be considered a FiXs® Transaction. In such cases, the Relying Party Organization may choose local security processes and procedures to allow or deny admittance. Such exception conditions can include, but are not necessarily limited to: unrecognized participant, unreadable badge/token and inability to reach an employer's FDS (issuer system down, FiXs® Trust Broker down, relying party system down, etc.).

9 FIXS® GOVERNANCE

The Federation for Identity and Cross-Credentialing Systems (FiXS®) is the legal and business entity that manages Member Partnership Agreements and maintains the FiXS® Foundational Documents. FiXS® shall develop membership criteria, voting procedures, and an Operating Rules Committee for the updating of these Operating Rules. The FiXS® Bylaws shall also set forth the protocol for establishing a Board of Directors, Committees and official meetings.

This Section describes the business requirements and responsibilities of the operating entities.

9.1 FiXS® Business Requirements

9.1.1 ESTABLISH FiXS® MEMBER PARTNERSHIP AGREEMENT(S)

An organization seeking membership in FiXS® is required to enter into an agreement with FiXS®. By this agreement, the Member Organization agrees to comply with the FiXS® Operating Rules and other documents incorporated herein by reference.

9.1.2 EFFECT OF RULES

To the extent that individual Member Organizations have agreed to be bound by these Rules and have entered into, or enter into, a contract or agreement between such Members where the performance of the contract or agreement will involve these Rules or credentials issued under these Rules, these Rules will serve as a supplement to the contract or agreement as if these Rules were fully set forth in the contract or agreement. To the extent that there is a conflict between the terms of the contract or agreement and these Rules, between the parties to the contract or agreement, the terms of the contract or agreement shall control. With respect to all other parties these Rules shall control.

9.2 Public Statements

Unless the consent of the Operating Entity is first obtained, Participants shall not in any manner advertise or publish or release for publication any statement regarding the FiXS® project.

10 MEMBERSHIP APPROVAL, AUTHORIZATION TO OPERATE AND COMPLIANCE MONITORING

10.1 Summary

This chapter explains the process for vetting and accepting members and for certifying members to perform roles defined in these Rules. The process for Founding Members is depicted in Figure 9.1. The process for new members is depicted in Figure 9.2.

10.1.1 Membership Process

Founding members in good standing, as defined by the Membership Committee, shall be Member Organizations without going through the membership vetting process. Any other organization that wants to become a FiXs® Member Organization must submit an application to the Membership Committee for review. The applicant must then be vetted by a FiXs®-approved financial institution. The Membership Committee will then make a recommendation to the FiXs® Executive Board with regard to approval or denial of the application.

10.1.2 Certification of Member Organizations

Organizations approved for membership will be eligible to apply for certification for an Authorization to Operate (ATO), and thereby perform roles defined in these rules. Founding Members may receive an ATO certification as a FiXs®-Certified Credential Issuer, Issuer Sponsor, Relying Party, or as a Member Service Provider. Full Members and Network User Associate Members, as defined in the FiXs® Bylaws, may receive ATO certification as a FiXs®-Certified Credential Issuer, Issuer Sponsor or Relying Party. In order to be an ATO certified Member Service Provider, Relying Party, FiXs®-Certified Credential Issuer, or Issuer Sponsor, an applicant must submit an application to the Performance Monitoring and Compliance Subcommittee of the Membership Committee to be assessed by a Third Party Assessor certified by the International Information System Security Certification Consortium and the National Security Agency's InfoSec Assessment Methodology, as recognized by the Department of Defense. The Subcommittee will make a recommendation to the Executive Board about whether to certify an applicant.

10.1.3 Issuing Identifiers to Individuals

A FiXs®-Certified Credential Issuer or Issuer Sponsor is authorized to issue identifiers to individuals as provided for in these Rules.

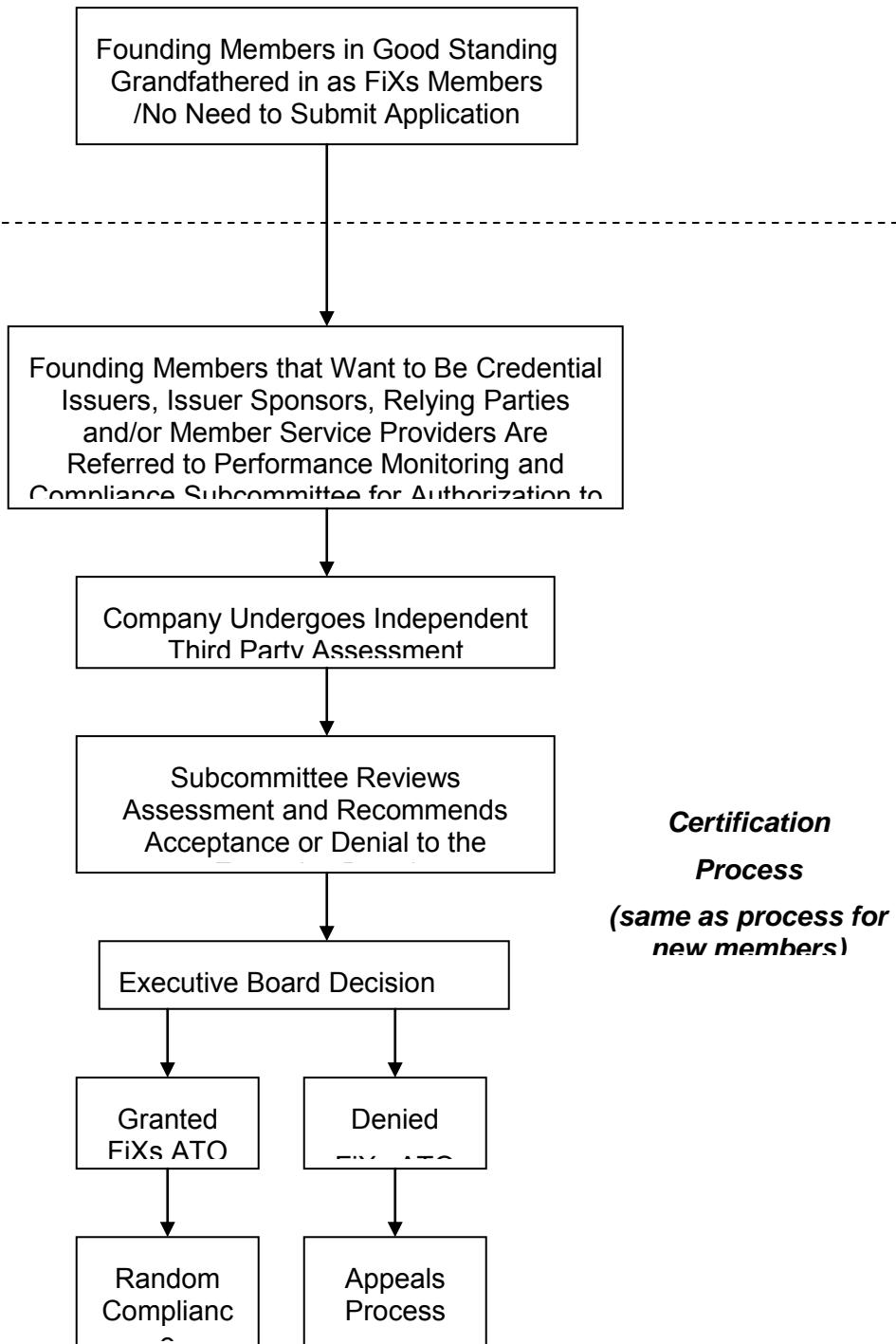


Figure 10.1. Process for Founding Members

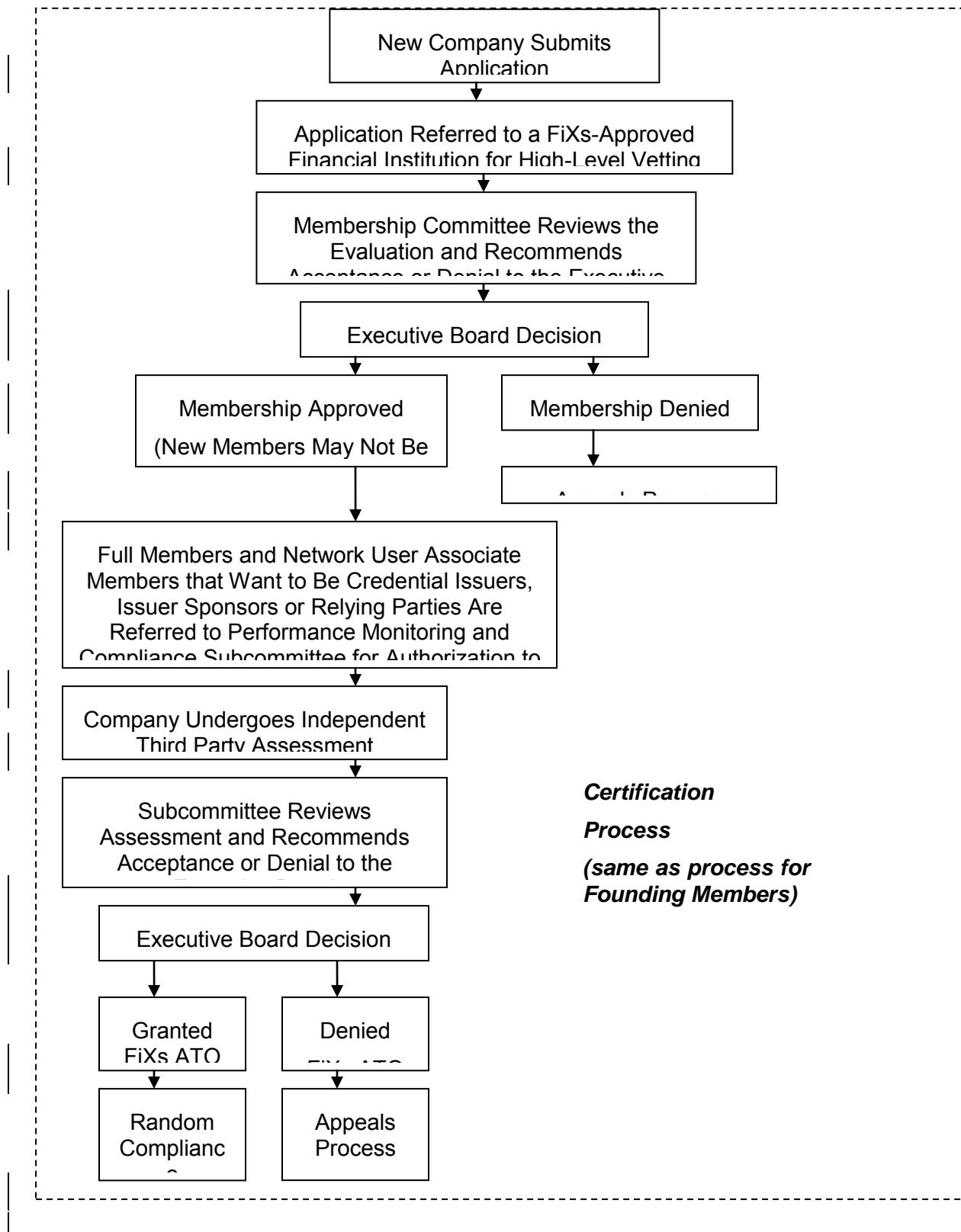


Figure 10.2 – Membership Process For New Members

10.2 Vetting Requirements for Member Organizations

This section specifies how organizations may be approved as FiXs® Member Organizations.

10.2.1 APPLICATION FOR MEMBERSHIP

10.2.1.1 Founding Members

Founding Members as defined in the FiXs® Bylaws shall be Member Organizations as long as they remain in good standing, as defined by the Membership Committee.

10.2.1.2 Other Members

Any organization that seeks to become a FiXs® Member Organization, with the exception of Founding Members, must submit an application to the Membership Committee.

10.2.2 MEMBERSHIP REVIEW AND APPROVAL PROCESS

10.2.2.1 Review by a FiXs®-Approved Vetting Organization

When the Membership Committee has received an application for membership, it shall request that the applicant obtain a review by a financial institution approved by FiXs® as a vetting organization. The Approved Vetting Organization shall provide a written report to the Membership Committee warranting that the applicant meets the criteria specified by the Membership Committee for FiXs® Member Organizations. The Committee may opt to waive review of an Association or non-profit organization, an organization that meets federal government bonding requirements, or of any member that joined FiXs® prior to June 1, 2005.

10.2.2.2 Membership Committee Recommendation to the Executive Board

The Membership Committee shall consider the review by the FiXs®-approved vetting organization in recommending approval or denial of a membership application to the FiXs® Executive Board.

10.2.2.3 Decision by the Executive Board

The FiXs® Executive Board shall approve or deny membership applications.

10.2.2.4 Appeals Process

Any applicant whose membership application is denied by the FiXs® Executive Board may appeal the decision to a Review Panel comprised of the FiXs® Officers. The decision of the Review Panel will be final and binding.

10.2.3 CERTIFICATION OF AUTHORIZATION TO OPERATE

10.2.3.1 Authorization To Operate

In order to serve as a FiXs®-Certified Credential Issuer, Issuer Sponsor, Relying Party or a Member Service Provider, a Member Organization must be certified as having Authorization to Operate (ATO) under these Rules.

10.2.3.2 Eligible Organizations

The following organizations may apply for ATO certification:

10.2.3.2.1 Full Members

Full Members may apply to serve as a FiXs®-Certified Credential Issuer, Issuer Sponsor, Relying Party or a Member Service Provider.

10.2.3.3 Application for ATO Certification

Member Organizations that want to be ATO certified, shall submit an application to the Performance Monitoring and Compliance Subcommittee of the Membership Committee.

10.2.3.4 Independent Assessment of Applicants for an ATO

Applicants for ATO certification must be assessed by an Independent Third Party Assessor certified in accordance with the Information System Security Certification Consortium and the National Security Agency's InfoSec Assessment Methodology, which are recognized by the Department of Defense. Independent Third Party Assessors shall use the Compliance Matrix and Check list referenced in Section 9.2.3.5 in assessing the applicant.

10.2.3.5 Performance Metrics and Compliance Assessment Checklist

FiXs® shall develop a matrix of compliance factors from each of the FiXs® policy documents listed below. From this compliance matrix, a series of independent checklists will be developed, each of which may be applied independently or jointly. The FiXs® Executive Committee will approve the checklists. Once approved, a Board-appointed FiXs® Member will negotiate the matrix and checklist(s) with the government. After consensus approval, the independent Third Party Assessors will begin assessments of FiXs® elements using the approved checklists that are designed to assess the applicant's compliance with the following FiXs® documents:

- FiXs® Trust Model;
- FiXs® Policy;
- FiXs® Operating Rules;
- FiXs® Technical Architecture and Specifications; and
- FiXs® Security Guidelines.

The assessing organization shall report to the Performance Monitoring and Compliance Committee, which shall make a recommendation with regard to certification to the FiXs® Executive Committee.

10.2.3.6

FiXs® Executive Committee Action

The FiXs® Executive Board shall either approve or deny ATO certification to the applicant.

10.2.3.7

Appeals Process

Any applicant whose ATO is denied by the FiXs® Executive Committee may appeal the decision to a Review Panel comprised of the FiXs® Officers. The decision of the Review Panel will be final and binding.

10.2.3.8

Random Compliance Assessments

FiXs®-Certified Credential Issuers, Issuer Sponsors and Member Service Providers will be assessed on a random, periodic basis for compliance with FiXs®/DCCIS policies and procedures. Such random compliance assessments will be performed by Independent Third Party Assessors, which shall be conducted using the matrix of compliance factors provided for in 9.2.3.5.

10.2.3.9

Government Compliance Assessment

Federal agencies may assess the entire FiXs® system or any of its components to ensure compliance with its regulations and conformance with the intent of FiXs®/DCCIS policy. These assessments are random, with or without notice, prompted by indicators from the network or other forms of inspection. The government assessments will conform to the assessment format used by Independent Third Party Assessors, using the same FiXs®/government negotiated checklist(s) as provided for in 9.2.3.5.

11 MISCELLANEOUS

11.1 Voluntary Termination of Members

Each FiXs®-Certified Credential Issuer, Issuer Sponsor or Relying Party that voluntarily terminates its processing of transactions shall provide written notice to FiXs® and shall continue to be bound by these Rules with respect to transactions occurring before such termination.

11.2 Amendment to These Rules

These Rules may be amended from time to time in accordance with the procedures set forth in the FiXs® Bylaws; as such Bylaws may be amended from time to time in accordance with its terms.

12 DEFINITIONS

Applicant. An employee or user designated by a Subscriber or Subscribing Party who applies to become a Participant in the FiXs® Network and completes the requirements of the identity proofing process.

Approved Vetting Organization. An organization that has a written agreement with FiXs® to review applications to become a Member Organization.

Audit Control Data Transaction. A transaction to update to the FDS control tables. These updates include new data and modifications regarding new Members and Participants and dis-enrolled Members and Participants.

Authenticate. Relates to a situation where one party has presented an identity and claims to be that identity. Authentication enables another party to gain confidence that the claim is legitimate.

Authentication Client. A personal computer with a standard Web browser for access to the *Authentication Web Server* that contains software and drivers for a bar code reader, a smart card reader, and a fingerprint reader with software. The *Authentication Station Operator* uses the *Authentication Client* to conduct *Authentication Inquiries*.

Authentication Inquiry. A transaction originating from an Authentication Client, which requests the authentication of a credential holder from, the credential holder's home FDS.

Authentication Response. A reply from the FiXs®-Certified Credential Issuer to an Authentication Inquiry that sends a denial or transmits credential information (photo and fingerprints) to the Relying Party.

Authentication Station. The physical area which houses the Authentication Client, Fingerprint Reader, Smart Card Reader and Bar Code Reader and where the Authentication Station Operator performs Authentication Transactions (usually a Visitor Security Station).

Authentication Station Operator. An employee or contractor of the Relying Party who operates the *Authentication Client* and conducts *Authentication Inquiries*.

Authentication Web Server. A standard web server that processes Authentication Inquiries and Responses between the Relying Party's Authentication Client and the FiXs® Trust Broker.

Authentication Web Server Application. The application, which receives and processes the ID credential information from the Client and returns identity information and fingerprint data for matching on the Client.

Badge/Token. A card or other device that holds these bearer's credentials (such as a photo on the face of a badge or a biometric on a bar code) or that holds the "keys" or "pointers" to the credentials that are accessible in a record on a remote system.

Bar Code Reader/Printer. A device that stores and accepts current token barcodes or that prints new barcodes for existing tokens.

Biometric. For the purposes of the FiXs® Operating Rules, a biometric refers to the file of the Participant's scanned fingerprints that are stored at his/her home FDS and retrieved for comparison at the time of an Authentication Inquiry.

Card Management System. FIPS-201 compliant application to manage PIV-compliant card life-cycle management.

Certificate Authority Administrator. A Certificate Authority Administrator (CAA) is an individual who is the responsible party for a CMA. The CAA possesses the private key of the CMA's certificate. The CAA may be collocated with the CMA, but may also perform administration tasks remotely.

Certificate Policy. A Certificate Policy is a document that defines the policy requirements that must be met by any CMA implemented under the policy.

Certificate Practice Statement. A Certificate Practice Statement (CPS) is a document that details the requirements and procedures that are followed by a CA in issuing and maintaining certificates, and the purposes and allowed uses of those certificates.

Certificate. A data record that, at a minimum: (a) identifies the CMA issuing it; (b) names or otherwise identifies its credential holder; (c) contains a public key that corresponds to a private key under the control of the credential holder; (d) identifies its operational period; and (e) contains a certificate unique serial number and is digitally signed by the CMA issuing it. As used in this CPS, the term of "Certificate" refers to certificates that expressly reference the OID of this CMA in the "Certificate Policies" field of an X.509 v.3 certificate.

Certificate Management System. A Certificate Management System (Netscape and RSA Keon) provides a highly scalable, easily deployable certificate infrastructure for supporting encryption, authentication, tamper detection, and digital signatures in networked communications. It is based on open standards and protocols such as Public-Key Cryptography Standard (PKCS) #7, 10, 11, and 12, Secure Sockets Layer (SSL), Lightweight Directory Access Protocol (LDAP), and the X.509 certificate formats recommended by the International Telecommunications Union (ITU). Certificate Management System is highly customizable and configurable, permitting rapid integration with existing client and server software, customer databases, security systems, and authentication procedures.

Certificate Manufacturing Authority (CMA). An entity that is responsible for the manufacturing and delivery of certificates, but is not responsible for identification and authentication of certificate subjects (i.e., a CMA is an entity that is delegated or outsourced the task of actually manufacturing the certificate).

Certificate Practice Statement (CPS). A Certification Practice Statement is a statement of the practices that a certification authority employs in issuing, suspending, revoking, and renewing certificates and providing access to same, in accordance with specific requirements (i.e., requirements specified in this CPS, requirements specified in a contract for services).

Certificate Repository. A certificate repository is a system that holds certificates and information about all active certificates including revocation information.

Certificate Revocation List. A Certificate Revocation List (CRL) is a list of certificates that have been revoked but have not yet expired. A CRL should be digitally signed by the CMA to ensure its validity to relying parties.

Certification Authority. A certification authority is an entity that is responsible for authorizing and causing the issuance of a Certificate. The actual certificate is from the CMA.

Chain of Trust. The trust that is established by a series of agreements that bind Member Organizations, Subscribing Parties, the FiXs® Trust Model, the FiXs® Policy, the FiXs® Operating Rules, the FiXs® Technical Architecture and Specifications, the FiXs® Security Guidelines and other FiXs® Foundational Documents as may be specified from time to time by the FiXs® Board of Directors.

Contractual Agent. An individual, other than an employee, who is sponsored as a user on the FiXs® Network

Credential Holder: A person who (1) is the subject named or identified in a FiXs® credential and associated certificate issued to such person and (2) holds a private key that corresponds to a public key listed in that certificate, and (3) the person to whom digitally signed messages verified by reference to such certificate are to be attributed.

Credential Issuance: The process by which a FiXs® participant (applicant) is provided with a FiXs® Identifier which consists of four steps: 1) validate applicant's need for FiXs® credentials; 2) verify applicant identification; 3) enroll applicant into FiXs® system; and 4) issue or record the Participant's valid FiXs® identifier.

Cross Credential Request Handler Software. Installed on the Authentication Client, this software interfaces with the Authentication Web Server to transmit Authentication Inquiries to the FTB.

Common Access Card (CAC). The official identification card issued to DoD personnel that includes applications for physical and logical access. CAC cards are de facto FiXs® Identifiers.

Defense Cross-Credentialing Identification System (DCCIS).

Digital Camera. A camera capable of capturing digital photos and storing them in file formats as per the *FiXs® Technical Architecture and Specifications*.

Digital Certificate. A digital certificate is electronic information that indicates the identity of the credential holder, the identity of the CMA, the operational period of the certificate, and the public key of the credential holder. The certificate is digitally signed by the issuing CMA to show validity.

Digital Signature. A digital signature is a string of bits associated with a collection of data (e.g., a file, document, message, transaction); this string of bits can only be generated by the holder of a private key, but can be verified by anyone with access to the corresponding public key.

Some algorithms include additional steps (e.g., one-way hashes, timestamps) in this basic process.

Document Verification Service. A service that provides responses to authentication queries from multiple databases to verify identification documents.

Domain Functional Administrator. A Member Organization employee responsible for the enrollment functions and management of the enrollment personnel within the Member Organization.

Domain Technical Administrator. A Member Organization employee who has the authority to perform infrastructure maintenance applications on the Enrollment System and/or the

Authentication System for the FiXs® Program.

Encoding Reader Device. Device that reads and displays the data on the bar code and/or magnetic stripe.

End Entity. An end entity is any individual or server who holds a digital certificate. See also credential holder.

Enrollment. Refers to the creation of a valid FiXs® Participant record in the FiXs® Data Repository.

Enrollment Client. A PC with a standard Web browser for access to the *Enrollment Web Server* that includes software, a bar code reader and a fingerprint reader. The *Facility Enroller* uses the Enrollment Client to capture FiXs® ID data and issue the FiXs® Certified Credential.

Enrollment Web Server. A standard web server that processes enrollments from the Authentication Client and stores the records in the Sponsor's FiXs® Data Repository.

Enrollment Web Application Software. Software that enables entry of new FiXs® Participants into the Sponsor's FiXs® Data Repository.

Exception Processing. Procedures to be followed when a credential or participant cannot be authenticated by the FiXs® System as per the normal procedures described in these Operating Rules.

Facility Administrative Enrollers. Member employees who are responsible for enrolling and terminating new local Facility Enrollers using the Enrollment Operator Maintenance Web Application.

Facility Enrollers. Employees of a FiXs® FiXs®-Certified Credential Issuer or Issuer Sponsor who perform enrollment services for FiXs®-Certified Credential Issuers.

Facility Domain Administrators. Member employees who have the technical and operational responsibilities for individual FiXs® facilities within a domain.

Facility Verifier. Employee of a FiXs® FiXs®-Certified Credential Issuer who has the authority to perform the identity proofing tasks.

Federal Information Processing Standards (FIPS). The federal standards that prescribe specific performance requirements, practices, formats, communications protocols, etc. for hardware, software, data, telecommunications operation, etc. Federal agencies are expected to apply these standards as specified unless a waiver has been granted in accordance to agency waiver procedures.

Federated Model of Trust. An approach to establishing trust that relies on agreements, standards and technologies to make identity portable across disparate organizations.

Federation for Identity and Cross-Credentialing Systems (FiXs®). A non-profit, non-stock 501c(6) trade association incorporated under the laws of the Commonwealth of Virginia. FiXs® is the legal and business entity that manages the FiXs® Network and maintains standards oversight and compliance with established operating principles of the FiXs® Network.

Fingerprint Capturing Device. A device with software for capturing, reading, storing and

comparing fingerprints that is used at enrollment.

Fingerprint Reader. A device used at the Authentication Station to scan the Participant's fingerprint for comparison against the downloaded image.

FiXs® Applicant. See **Applicant**.

FiXs® Certified Credential. An identity credential issued by an approved FiXs® FiXs®-Certified Credential Issuer who has contracted to follow the FiXs® Trust Model and all corollary policies, rules, guidelines and implementation standards for vetting, enrolling, maintaining and revoking identity credentials. The organization has also agreed to allow an independent FiXs® contractor to certify and periodically audit the above conditions for issuance and use of the credential(s).

FiXs®-Certified Credential Issuer. A FiXs® Member that issues FiXs®-Certified Credentials to qualified users for themselves and/or other Sponsors or Subscribing Parties and processes and responds to *Authentication Inquiries*.

FiXs®-Certified Data Repository. Database that stores the identification credentials and audit files associated with the FiXs® Participants of the Member Organization and interfaces to the Member's FDS.

FiXs®-Certified Domain Server (FDS). The platform that contains the enrollment and authentication server software and that interfaces to the FiXs® Data Repository, the FiXs® Trust Broker, the Enrollment Client, and the Authentication Client.

FiXs® Foundational Documents. Documents approved by the FiXs® Board of Directors that form the logical and functional foundation for the FiXs® Network: These documents include, but are not limited to: the Trust Model; the FiXs® Policy; the FiXs® Operating Rules; the FiXs® Implementation Guidelines; the FiXs® Security Guidelines and the FiXs® Technical Architecture and Specifications .

FiXs® Identifier. The unique identifier used to access a Participant's or user's authentication files. For CAC holders, this identifier is the DoD EDI PIN. For non-CAC holders, it is the combination of the FiXs® designated Participant's Member/Organization Code and ID and the Organization-assigned Employee ID number.

FiXs® Member or FiXs® Member Organization. See **Member or Member Organization**.

FiXs®-Certified Network. The end-to-end system comprising the physical infrastructure, operating principles and processes to authenticate FiXs® Certified Credentials.

FiXs® Operating Entity. See **Operating Entity**.

FiXs® Participant. See **Participant**.

FiXs® Relying Party. See **Relying Party**.

FiXs®-Certified System. See **Federation for Identity and Cross-Credentialing Systems (FiXs®)/Defense Cross-Credentialing Identification System (DCCIS)**.

FiXs®-Certified Trust Broker (FTB). The intermediary between FiXs®-Certified Credential Issuers and Relying Parties that serves as the *operational intermediary* by processing Authentication Inquiries from Relying Parties to FiXs®-Certified Credential Issuers and Authentication Responses from FiXs®-Certified Credential Issuers to Relying Parties via the

FiXs® Trust Broker.

FiXs® Program Manager. See **Program Manager**.

Government. Federal Government and authorized agencies and entities.

Hardware Security Module. A device is used to encrypt messages that are being sent to the FiXs® Trust Broker and to verify the digital signatures of messages received from the FiXs® Trust Broker.

Home Transaction/Home FDS. Refers to an Authentication Inquiry that is processed at the same DCCIS FDS as the originating Relying Party. In this case, the employee is being authenticated at an employee facility.

Hypertext Transfer Protocol over SSL (HTTPS). HTTPS is the use of Secure Socket Layer (SSL) for data transfer via the World Wide Web. HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP. SSL uses a 128-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.

Independent Third Party Assessor. An independent organization certified in accordance with the Information System Security Certification Consortium and the National Security Agency's InfoSec Assessment Methodology that performs assessments for compliance with the Compliance Matrix and Checklist approved by the FiXs® Executive Board.

Identity Proofing. The process by which the Member Organization validates the identity information provided by the applicant at the time of employment.

Internet Engineering Task Force (IETF). The Internet Engineering Task Force is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

Issuer Sponsor. A FiXs®-Certified Credential Issuer that also sponsors other FiXs®-Certified Credential Issuers and performs some or all of the FiXs®-Certified Credential Issuer duties defined herein that the sponsored FiXs®-Certified Credential Issuer chooses not to perform. In this case, the Issuer Sponsor assumes some or all of the following functions on behalf of the sponsored Issuer: enrollment and issuance; participant records management; FiXs® domain server management; standards and specifications compliance; transaction processing; application integration; and, human resources and security departments coordination.

Key Changeover. The procedure used by an Authority to replace its own private key (e.g., due to compromise) and replace current valid certificates issued with old key.

Key Pair. Means two mathematically related keys, having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key, and (2) even knowing one key, it is computationally infeasible to discover the other key.

Member. See **Member Organization**.

Member Organization. A company, agency, or organization that formally applies, and is accepted, for membership in FiXs® on other than a Subscriber basis. This organization may then participate in either a voting or non-voting capacity in the FiXs® governance process to

help set the vision and evolution of the FiXs® Network

Member Partnership Agreement. Legal document signed by Member Organization representatives with the FiXs® Operating Entity, which binds the Member to the FiXs® Operating Rules.

Member Service Provider. A Member Service Provider (MSP) is a FiXs® Founding Member that has agreed to provide equipment procurement and management services to FiXs® Issuers and/or FiXs® Relying Parties. In its role as MSP, designated Founding Members will supply domain servers, enrollment equipment and authentication equipment (including required peripherals) to FiXs® Issuers and Relying Parties that request these services. MSP services include equipment procurement, delivery and deployment; inventory management; equipment certification; equipment configuration; and documentation. Optionally, MSPs may also provide local application development and integration as well as consultative services to FiXs® Issuers and Relying Parties.

Mutual Authentication. Parties at both ends of a communication activity authenticate each other (see authentication).

Object Identifier (OID). An object identifier is a specially formatted number that is registered with an internationally recognized standards organization.

Operational Period of a Certificate. The operational period of a certificate is the period of its validity. It would typically begin on the date the certificate is issued (or such later date as specified in the certificate), and ends on the date and time it expires as noted in the certificate.

Operator Maintenance Web Application Software. Software that enables new local site Enrollment Operators to be created and terminated on the Sponsor's FiXs® Data Repository.

Organizational Code. The unique identifying number that is assigned to a FiXs®-Certified Credential Issuer or Issuer Sponsor.

Out-of-band. Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party using U.S. Postal mail to communicate with another party where current communication is online communication).

Participant. Refers to the individual employee or subcontractor of a Member Organization that qualifies to participate in the FiXs® System.

Primary Trusted Organization or PTO. The entity that sponsors individual users who are to be issued a FiXs®-Certified Credential in accordance with all FiXs® processes, and policies and that agrees to be responsible for the acts and omissions of its employees or Contractual Agents. A PTO may also be a FiXs®-Certified Credential Issuer, Issuer Sponsor or Subscriber.

Private Key. The key of a key pair used to create a digital signature. This key must be kept a secret.

Program Participants. Collectively, the CMAs, Registrars, Certificate Manufacturing Authorities, Repositories, credential holders, Relying Parties, and Policy Authority authorized to participate in the public key infrastructure defined by this CPS.

Program Manager. A Program Manager (PM) is an employee who manages and

administers the FiXs® program within a Member company or organizational domain. The PM has technical oversight of the program and is responsible for appointing the Domain Technical Administrator and Domain Functional Administrator for the Program.

POC and pilot. Refers to the “Proof-of-Concept” and pilot Phase of the FiXs® System.

Public Key. The key of a key pair used to verify a digital signature. The public key is made freely available to anyone who will receive digitally signed messages from the holder of the key pair. The public key is usually provided via a certificate issued by an CMA and is often obtained by accessing a repository. A public key is used to verify the digital signature of a message purportedly sent by the holder of the corresponding private key.

Public Key Infrastructure. A Public Key Infrastructure (PKI) is a system of policies, CAs, certificates, information repositories, and trusted individuals, that is used to verify and authenticate individuals and servers, and to encrypt and decrypt information exchanged by these individuals and servers.

Registrar. An entity that is responsible for identification and authentication of certificate subjects, and issues certificates.

Relying Party. A FiXs® Member that either relies on the FiXs® credential to authenticate the identity of a Participant and/or initiates authentication inquiries to the FiXs®-Certified Credential Issuer and processes the responses in accordance with FiXs® Operating Rules.

Remote Transaction. Refers to an Authentication Inquiry that is routed through the FiXs® Trust Broker to be processed at a FDS other than of the originating Relying Party.

Repository. A database containing information and data relating to certificates, and a CA, as specified in this CPS.

Responsible Individual. A trustworthy person designated by a Sponsoring Organization to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.

Revoke a Certificate. Means to prematurely end the operational period of a Certificate from a specified time forward.

Secure Sockets Layer. A protocol for providing data security layered between application protocols (such as HTTP, Telnet, NNTP, or FTP) and TCP/IP. This security protocol supports data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection.

Smart Card Reader. A device used to read and process data that resides on a smart card.

Smart Card Writer. A device used to write ID data to a smart card and record images for comparison to a scanned image on the Authentication Client.

Sponsor. An organization that uses the services of an Issuer Sponsor to host its FiXs® operations and that sponsors Participants into the FiXs® Network. A Sponsor is responsible for the acts and omission of the Participants that it sponsors. There are two kinds of Sponsors a member and a non-member . In this case, the Issuer Sponsor hosts the Sponsors FDS and processes its FiXs® authentication transactions.

Subscriber or Subscribing Party. A non-member organization that is a Primary Trusted Organization sponsoring individual users to be issued FiXs® Certified Credentials.

Subscribers agree to Terms of Use policies. .

Suspend a Certificate. Means to temporarily suspend the operational period of a Certificate for a specified time period or from a specified time forward.

Terms of Use. The legal agreement between FiXs®, FiXs® Member Organizations, and Subscribing Parties regarding each parties agreement to adhere to FiXs® rules, policies, and procedures for utilizing a FiXs® Certified Credential.

Transaction. Refers to an **Authentication Inquiry**, an **Authentication Response** or an **Audit Control Data Transaction**.

Trusted Adjudicator. An administrator who assigns privileges at the customer level for granting privileges, to include physical or logical access.

Trustworthy System. Means computer hardware, software, and procedures that: (a) are reasonably secure from intrusion and misuse; (b) provide a reasonable level of availability, reliability, and correct operation; (c) are reasonably suited to performing their intended functions, and (d) adhere to generally accepted security procedures.

Valid Certificate. Means a certificate that (1) an Authorized CA has issued, (2) the credential holder listed in it has accepted, (3) has not expired, and (4) has not been revoked. Thus, a certificate is not “valid” until it is both issued by a CA and has been accepted by the credential holder.

13 REFERENCES

The following documents contain information that provides background, examples, or details about the contents of this policy.

Number	Title	Revision	Date
DoD Instruction 8520.2	Public Key Infrastructure (PKI) and Public Key (PK) Enabling http://www.dtic.mil/whs/directives/corres/html/852002.htm		01 April 2004
DoD CIO Memo	Approval of External Public Key Infrastructures http://www.afei.org/documents/20080722DoDExternalPKIMemo.pdf		22 July 2008
HSPD-12	Policy for a Common Identification Standard for Federal Employees and Contractors, http://csrc.nist.gov/policies/Presidential-Directive-Hspd-12.html		27 Aug 2004
OMB Circular No. A-123	Management Accountability and Control, http://www.whitehouse.gov/omb/circulars/a123/a123.html		Revised June 21, 1995
ABADSG	Digital Signature Guidelines, http://www.abanet.org/scitech/ec/isc/dsgfree.html		1 Aug 1996
FIPS112	Password Usage, http://csrc.nist.gov/publications/index.html		5 May 1985
FIPS140	Security Requirements for Cryptographic Modules, http://csrc.nist.gov/publications/index.html		21 May 2001
FIPS186	Digital Signature Standard, http://csrc.nist.gov/fips/fips186-2.pdf		20 Jan 2000
FIPS201	Personal Identity Verification of Federal Employees and Contractors, http://csrc.nist.gov/publications/index.html		25 Feb 2005
FOIACT	5 U.S.C. 552, Freedom of Information Act, http://www4.law.cornell.edu/uscode/5/552.html		
FWPP	U.S. Department of Defense Traffic-Filter Firewall Protection Profile for Medium Robustness Environments, http://www.iatf.net	Version 1.4	1 May 2000
IDSPP	Intrusion Detection System Protection, http://www.iatf.net	Version 1.4	4 Feb 2002
ISO9594-8	Information Technology – Open Systems Interconnection – The Directory: Authentication Framework, ftp://ftp.bull.com/pub/OSIdirectory/ITU/97x509final.doc		1997
ITMRA	40 U.S.C. 1452, Information Technology Management Reform Act, http://www4.law.cornell.edu/uscode/40/1452.html		

Number	Title	Revision	Date
NAG69C	Information System Security Policy and Certification Practice Statement for Certification Authorities,	Revision C	Nov 1999
NS4009	NSTISSI 4009, National Information Systems Security Glossary		Jan 1999
NSD42	National Policy for the Security of National Security Telecom and Information Systems, http://snyside.sunnyside.com/cpsr/privacy/computer security/nsd_42.txt (redacted version)		5 Jul 1990
PKCS-1	PKCS #1 v2.0: RSA Cryptography Standard, http://www.rsa.com		1 Oct 1998
PKCS-12	Personal Information Exchange Syntax Standard, http://www.rsa.com/rsalabs/pubs/PKCS/html/pkcs-12.html		Apr 1997
ECA CP	<i>US Government Certificate Policy for External Certification Authorities</i>	Version 3.1	30 August 2006
ECAKRP	<i>Key Recovery Policy for External Certification Authorities</i>	Version 1.0	4 Jun 2002
FBCA CP	X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA), http://www.cio.gov/fpkipa/documents/FBCA_CP_RFC3647.pdf	Version 2.6	16 Aug 2007
ACES CP	<i>Revised Certificate Policy For Access Certificates for Electronic Services</i>		6 May 2004
FPCPF CP	X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, http://www.cio.gov/fpkipa/documents/CommonPolicy.pdf	Version 3647-1.1	16 Aug 2007
FPKI-PROF	Federal PKI Certificate and CRL Extensions Profile, http://csrc.nist.gov/pki/		31 May 2002
CCP-PROF	X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program	Draft	5 Jan 2006
RFC3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, http://www.ietf.org/rfc/rfc3647.txt		Nov 2003
RFC2510	Certificate Management Protocol, Adams and Farrell, http://www.ietf.org/rfc/rfc2510.txt		Mar 1999

Number	Title	Revision	Date
SDN702	SDN.702, Abstract Syntax for Utilization with Common Security Profile (CSP), Version 3 X.509 Certificates and Version 2 CRLs, http://www.armadillo.Huntsville.al.us/Forteza_docs/sdn702_rev3.pdf	Revision 3	31 Jul 1997

The following Federal laws, mandates, and instructions provide the security policy framework for the EI development, operations, and security:

- Privacy Act of 1974 (Public Law 93-579), December 1974
- Federal Managers Financial Integrity Act (FMFIA), September 1982
- Computer Security Act of 1987, January 1988
- Paperwork Reduction Act (Public Law 104-13), May 1995
- Information Technology Management Reform Act of 1996 (Clinger-Cohen Act) (Public Law 104-106), February 1996
- USA PATRIOT Act (Public Law 107-56), October 2001
- E-Government Act of 2002 (Public Law 107-347), December 2002
- Federal Information Security Management Act of 2002 [FISMA] (Public Law 107-347, Title III), December 2002
- Code of Federal Regulations, Title 5, Administrative Personnel, Part 731, Suitability, Subpart A, Scope, Section106, *Designation of Public Trust Positions and Investigative Requirements*, (5 C.F.R.731.106)
- Code of Federal Regulations, Title 5, Administrative Personnel, Part 930, Programs for Specific Positions and Examinations, Subpart C, Sections 930.301 through 930.305, *Employees Responsible for the Management or Use of Federal Computer Systems*, (5 C.F.R. 930.301-305)
- Presidential Decision Directive 63 (PDD-63), *Critical Information Protection*, May 1998
- Homeland Security Presidential Directive (HSPD) 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004
- Homeland Security Presidential Directive (HSPD-7), *Critical Infrastructure Identification, Prioritization, and Protection*
- Department of Defense Instruction 8500.2, *Information Assurance Implementation*, February 2003
- Department of Defense, Chief Information Officer Memorandum, *Encryption of Sensitive Unclassified Data at rest on Mobile Computing Devices and Removable Storage Media*, July 03, 2007
- Director of Central Intelligence Directive 6/3 Manual, *Protecting Sensitive Compartmented Information within Information Systems*, June 1999
- Director of Central Intelligence Directive 6/3 Manual, *Protecting Sensitive*

Compartmented Information within Information Systems, May 2000

- Office of Management and Budget (OMB) Circular A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000
- Office of Management and Budget, Circular A-130, Management of Federal Information Resources, Appendix III, *Security of Federal Automated Information Systems*, as revised November 2000
- Office of Management and Budget Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, October 2001
- Office of Management and Budget Memorandum M-03-19, *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting*, August 2003
- Office of Management and Budget, Federal Enterprise Architecture Program Management Office, *Business Reference Model* (v2.0), June 2003
- Office of Management and Budget Memorandum M-03-22, OMB *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 26, 2003
- Office of Management and Budget Memorandum M-04-04, *E-Authentication for Federal Agencies*, December 2003
- Office of Management and Budget Memorandum M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD)12 – Policy for a Common Identification Standard for Federal Employees and Contractors*, August 2005
- Office of Management and Budget Memorandum M-06-16, *Protection of Sensitive Information*, June 2006
- Office of Management and Budget Memorandum M-06-20, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, July 2006
- National Institute of Standards and Technology Federal Information Processing Standards (FIPS) Publication 140-2, *Security Requirements for Cryptographic Modules*, May 25, 2001
- National Institute of Standards and Technology Federal Information Processing Standards (FIPS) Publication 180-2, *Secure Hash Standard (SHS)*, August 2002
- National Institute of Standards and Technology Federal Information Processing Standards (FIPS) Publication 186-2, *Digital Signature Standard (DSS)*, January 2000
- National Institute of Standards and Technology Federal Information Processing Standards (FIPS) Publication 188, *Standard Security Labels for Information Transfer*, September 1994
- National Institute of Standards and Technology Federal Information Processing Standards (FIPS) Publication 190, *Guidelines for the Use of Advanced Authentication Technology Alternatives*, September 1994
- National Institute of Standards and Technology Federal Information Processing

Standards (FIPS) Publication 197, *Advanced Encryption Standards (AES)*, November 2001

- National Institute of Standards and Technology Federal Information Processing Standards (FIPS) Publication 198, *The Keyed-Hash Message Authentication Code (HMAC)*, March 2002
- National Institute of Standards and Technology Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004
- National Institute of Standards and Technology Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006
- National Institute of Standards and Technology Federal Information Processing Standards (FIPS) Publication 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, March 2006
- International Organization for Standardization/International Electrotechnical Commission 17799, *Code of Practice for Information Security Management*, June 2005
- International Organization for Standardization/International Electrotechnical Commission 27001, *Information Security Management System Requirements*, October 2005
- National Security Telecommunications and Information Systems Security (NSTISSI) 7003, *Protective Distribution Systems (PDS)*, December 13, 1996
- NIST Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995
- NIST Special Publication 800-13, *Telecommunications Security Guidelines for Telecommunications Management Network*, October 1995
- NIST Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996
- National Institute of Standards and Technology Special Publication 800-15, *Minimum Interoperability Specifications for PKI Components (MISPC)*, Version 1, September 1997
- National Institute of Standards and Technology Special Publication 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, April 1998
- National Institute of Standards and Technology Special Publication 800-17, *Modes of Operation Validation System (MOVS): Requirements and Procedures*, February 1998
- National Institute of Standards and Technology Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006
- National Institute of Standards and Technology Special Publication 800-19, *Mobile Agent Security*, October 1999
- National Institute of Standards and Technology Special Publication 800-20, *Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures*, April 2000

- National Institute of Standards and Technology Special Publication 800-21-1, *Second Edition, Guideline for Implementing Cryptography in the Federal Government*, December 2005
- National Institute of Standards and Technology Special Publication 800-22, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, May 2001
- National Institute of Standards and Technology Special Publication 800-23, *Guideline to Federal Organizations on Security Assurance and Acquisition/Use Tested/Evaluated Products*, August 2000
- National Institute of Standards and Technology Special Publication 800-24, *PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does*, August 2000
- National Institute of Standards and Technology Special Publication 800-25, *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*, October 2000
- National Institute of Standards and Technology Special Publication 800-27, Revision A, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, June 2004
- National Institute of Standards and Technology Special Publication 800-28, *Guidelines on Active Content and Mobile Code*, October 2001
- National Institute of Standards and Technology Special Publication 800-29, *A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2*, June 2001
- National Institute of Standards and Technology Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, July 2002
- National Institute of Standards and Technology Special Publication 800-31, *Intrusion Detection Systems (IDS)*, November 2001
- National Institute of Standards and Technology Special Publication 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, February 2001
- National Institute of Standards and Technology Special Publication 800-33, *Underlying Technical Models for Information Technology Security*, December 2001
- National Institute of Standards and Technology Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002
- National Institute of Standards and Technology Special Publication 800-35, *Guide to Information Technology Security Services*, October 2003
- National Institute of Standards and Technology Special Publication 800-36, *Guide to Selecting information Security Products*, October 2003
- National Institute of Standards and Technology Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004
- National Institute of Standards and Technology Special Publication 800-38A,

Recommendation for Block Cipher Modes of Operation – Methods and Techniques, December 2001

- National Institute of Standards and Technology Special Publication 800-38B, *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*, May 2005
- National Institute of Standards and Technology Special Publication 800-38C, *Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality*, May 2004
- National Institute of Standards and Technology Special Publication 800-38D, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) for Confidentiality and Authentication* (Draft), April 2006
- National Institute of Standards and Technology Special Publication 800-40, Version 2, *Creating a Patch and Vulnerability Management Program*, November 2005
- National Institute of Standards and Technology Special Publication 800-41, *Guidelines on Firewalls and Firewall Policy*, January 2002
- National Institute of Standards and Technology Special Publication 800-42, *Guide on Network Security Testing*, October 2003
- National Institute of Standards and Technology Special Publication 800-43, *Systems Administration Guidance for Windows 2000 Professional*, November 2002
- National Institute of Standards and Technology Special Publication 800-44, *Guidelines on Security Public Web Servers*, September 2002
- National Institute of Standards and Technology Special Publication 800-45A (Draft), *Guidelines on Electronic Mail Security*, August 2006
- National Institute of Standards and Technology Special Publication 800-46, *Security for Telecommuting and Broadband Communications*, August 2002
- National Institute of Standards and Technology Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems*, August 2002
- National Institute of Standards and Technology Special Publication 800-48, *Wireless Network Security: 802.11, Bluetooth, and Handheld Devices*, November 2002
- National Institute of Standards and Technology Special Publication 800-49, *Federal S/MIME V3 Client Profile*, November 2002
- National Institute of Standards and Technology Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*, October 2003
- National Institute of Standards and Technology Special Publication 800-51, *Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme*, September 2002
- National Institute of Standards and Technology Special Publication 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementation*, June 2005
- National Institute of Standards and Technology Special Publication 800-53 Revision 1,

Recommended Security Controls for Federal Information Systems, December 2006

- National Institute of Standards and Technology Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems* (Second Public Draft), April 2006
- National Institute of Standards and Technology Special Publication 800-54, *Border Gateway Protocol Security* (Draft), September 2006
- National Institute of Standards and Technology Special Publication 800-55, *Security Metrics Guide for Information Technology Systems*, July 2003
- National Institute of Standards and Technology Special Publication 800-56A, *Recommendations for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, March 2006
- National Institute of Standards and Technology Special Publication 800-57, *Recommendation on Key Management*, August 2005
- National Institute of Standards and Technology Special Publication 800-58, *Security Considerations for Voice Over IP Systems*, January 2005
- National Institute of Standards and Technology Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003
- National Institute of Standards and Technology Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, June 2004
- National Institute of Standards and Technology Special Publication 800-61, *Computer Security Incident Handling Guide*, January 2004
- National Institute of Standards and Technology Special Publication 800-63, Version 1.0.2, *Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Guidelines*, April 2006
- National Institute of Standards and Technology Special Publication 800-64, Revision 1, *Security Considerations in the Information System Development Life Cycle*, June 2004
- National Institute of Standards and Technology Special Publication 800-65, *Integrating Security into the Capital Planning and Investment Control Process*, January 2005
- National Institute of Standards and Technology Special Publication 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, March 2005
- National Institute of Standards and Technology Special Publication 800-67, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, May 2004
- National Institute of Standards and Technology Special Publication 800-68, *Guidance for Security Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*, October 2005
- National Institute of Standards and Technology Special Publication 800-69, *Guidance for Security Microsoft Windows XP Home Edition: A NIST Security Configuration Checklist*,

September 2006

- National Institute of Standards and Technology Special Publication 800-70, *Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers*, May 2005
- National Institute of Standards and Technology Special Publication 800-72, *Guidelines on PDA Forensics*, November 2004
- National Institute of Standards and Technology Special Publication 800-73, Revision 1, *Interfaces for Personal Identity Verification*, April 2006
- National Institute of Standards and Technology Special Publication 800-76-1, *Biometric Data Specification for Personal Identity Verification* (Draft), September 2006
- National Institute of Standards and Technology Special Publication 800-77, *Guide to IPsec VPNs*, December 2005
- National Institute of Standards and Technology Special Publication 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, April 2005
- National Institute of Standards and Technology Special Publication 800-79, *Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations*, July 2005
- National Institute of Standards and Technology Special Publication 800-81, *Secure Domain Name System (DNS) Deployment Guide*, May 2006
- National Institute of Standards and Technology Special Publication 800-82, *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security* (Draft), September 2006
- National Institute of Standards and Technology Special Publication 800-83, *Guide to Malware Incident Prevention and Handling*, November 2005
- National Institute of Standards and Technology Special Publication 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, September 2006
- National Institute of Standards and Technology Special Publication 800-85A, *PIV Card Application and Middleware Interface Test Guidelines*, April 2006
- National Institute of Standards and Technology Special Publication 800-85B, *PIV Data Model Test Guidelines*, July 2006
- National Institute of Standards and Technology Special Publication 800-86, *Guide to Integrating Forensic Techniques into Incident Response*, August 2006
- National Institute of Standards and Technology Special Publication 800-87, *Codes for the Identification of Federal and Federally-Assisted Organizations*, January 2006
- National Institute of Standards and Technology Special Publication 800-88, *Guidelines for Media Sanitization*, September 2006
- National Institute of Standards and Technology Special Publication 800-89, *Recommendation for Obtaining Assurances for Digital Signature Applications*, November 2006
- National Institute of Standards and Technology Special Publication 800-90,

Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2006

- National Institute of Standards and Technology Special Publication 800-92, *Guide to Computer Security Log Management*, September 2006
- National Institute of Standards and Technology Special Publication 800-94, *Guide to Intrusion Detection and Prevention (IDP) Systems* (Draft), August 2006
- National Institute of Standards and Technology Special Publication 800-95, *Guide to Secure Web Services* (Draft), August 2006
- National Institute of Standards and Technology Special Publication 800-96, *P/V Card/Reader Interoperability Guidelines*, September 2006
- National Institute of Standards and Technology Special Publication 800-97, *Guide to IEEE 802.11: Establishing Robust Security Networks* (Draft), June 2006
- National Institute of Standards and Technology Special Publication 800-98, *Guidance for Security Radio Frequency Identification (RFID) Systems* (Draft), September 2006
- National Institute of Standards and Technology Special Publication 800-100, *Information Security Handbook: A Guide for Managers* , October 2006
- National Institute of Standards and Technology Special Publication 800-101, *Guidelines on Cell Phone Forensics* (Draft), August 2006
- Government Accountability Office, *Federal Information System Controls Audit Manual*, GAO/AIMD-12.19.6, January 1999
- DISA Security Technical Implementation Guides (STIGs) and Checklists at <http://csrc.nist.gov/pcig/cig.html>
- GSA Order CIO 2140.2, System Development Life Cycle (SDLC) Policy Handbook, April 20, 2004
- GSA Order CIO 2160.2, GSA Electronic Messaging Policy
- GSA Order CIO 2100.2, GSA Wireless Local Area Network (LAN) Security, October 30, 2005
- GSA Order CIO P 2100.1D, GSA Information Technology (IT) Security Policy, June 21, 2007
- GSA Order CPO 1878.2, Conducting Privacy Impact Assessment, May 28, 2004
- GSA Order CPO 1878.1, GSA Privacy Act Program, October 27, 2003
- GSA Order CIO 2104.1, GSA Information Technology (IT) General Rules of Behavior, July 3, 2003
- GSA Handbook ADM P 9732.1C, Suitability and Personnel Security, February 17, 2006
- CIO Instructional Letter 05-03 Mandatory IT Security Training for Agency and Contractor Employees with Significant Security Responsibilities, April 21, 2005
- IT Security Procedural Guide: Bluetooth Security Hardening, CIO-IT Security-07-36, March 7, 2007

- IT Security Procedural Guide: Web Application Security Guide, CIO-IT Security-07-35, Revision 1, February 12, 2007
- IT Security Procedural Guide: CISCO CALL Manager and Unity Hardening, CIO-IT Security-07-34, February 12, 2007
- IT Security Procedural Guide: McAfee VirusScan 8.0i, CIO-IT Security-06-33, Revision 1, February 21, 2007
- IT Security Procedural Guide: Media Sanitization Guide, CIO-IT Security-06-32, December 21, 2006
- IT Security Procedural Guide: Firewall Change Request, CIO-IT Security-06-31, November 8, 2006
- IT Security Procedural Guide: Handling IT Security Incidents, CIO-IT Security-01-02, Revision 3, July 23, 2006
- Standard Operating Procedure For GSA HSPD-12 Personnel Security Process, October 26, 2005
- IT Security Procedural Guide: Home Users Guide, CIO-IT Security-04-24, Revision 1, September 29, 2005
- IT Security Procedural Guide: Developing a Configuration Management (CM) Plan, CIO-IT Security-01-05, Revision 1, September 9, 2005
- IT Security Procedural Guide: Termination and Transfer, CIO-IT Security-03-23, Revision 1, August 29, 2005
- IT Security Procedural Guide: Auditing and Monitoring, CIO-IT Security-01-08, Revision 1, June 29, 2005
- IT Security Procedural Guide: Password Generation and Protection, CIO-IT Security-01-01, Revision 1, June 23, 2005
- IT Security Procedural Guide: Access Control, CIO-IT Security-01-07, Revision 1, June 23, 2005
- IT Security Procedural Guide: FISMA/POA&M Implementation, CIO-IT Security-04-26, Revision 4, May 26, 2005
- IT Security Procedural Guide: IT Security Training and Awareness Program, CIO-IT Security-05-29, Revision 1 April 27, 2006
- IT Security Procedural Guide: Contingency Plan Testing, CIO-IT Security-06-29, Revision 1, February 22, 2007
- IT Security Procedural Guide: Managing Enterprise Risk, CIO-IT Security-06-30, Revision 3, March 20, 2007
- IT Security Procedural Guide: Windows XP Professional Hardening, CIO-IT Security-03-22, Revision 6a, March 3, 2006
- IT Security Procedural Guide: Oracle Database Hardening, CIO-IT Security-05-28, March 29, 2005
- IT Security Procedural Guide: CISCO Router Hardening, CIO-IT Security-05-27, March

8, 2005

- IT Security Procedural Guide: Windows 2000 Professional Hardening, CIO-IT Security-02-15, Revision 3, November 16, 2004
- IT Security Procedural Guide: Windows 2003 Server Hardening, CIO-IT Security-04-25, Revision 2, June 21, 2006
- IT Security Procedural Guide: Sun Solaris Hardening, CIO-IT Security-02-20, August 30, 2002
- IT Security Procedural Guide: IIS 5.0 Server Hardening Implementation Guide, CIO-IT Security-02-19, July 24, 2002
- IT Security Procedural Guide: IIS 5.0 Server Hardening, CIO-IT Security-02-18, July 24, 2002
- IT Security Procedural Guide: Windows 2000 Server Hardening Implementation Guide, CIO-IT Security-02-17, July 24, 2002
- IT Security Procedural Guide: Windows 2000 Server Hardening, CIO-IT Security-02-16, July 24, 2002
- IT Security Procedural Guide: Microsoft IIS 4.0 Hardening, CIO-IT Security-01-14, May 14, 2001
- IT Security Procedural Guide: Windows NT 4.0 Hardening, CIO-IT Security-01-13, May 14, 2001
- GSA Internet Explorer 6.0 Configuration Guide
- FTS CIO Policy Memo 03-08 Account Closeout Procedures
- FTS CIO Policy Memo 03-04 Local Workstation Access Rights
- Computer Fraud & Abuse of 1986, as amended, Public Law 99-474
- OMB Memorandum M-01-08

14 REVISION HISTORY

Version	Date	Comments
1.0	September 2005	Initial Issue
1.1		
1.2	January 2007	Pages 23-25: Added “FiXs® Assurance Levels” as Section 2
2.0	March 2007	Added Section 2.1.3.1.1.6 Complete National Agency Check
3.0	September 2007	Changes to Levels-Sections 1-4
3.1	October 1, 2008	Added as an appendix, Logical Operating Rules Version 1.0 as approved by Board vote on October 1, 2008
3.2	November 2008	Updated to comply with requirements of DMDC.
3.3	March 2010	Merges the FiXs® Operating Rules and FiXs® Logical Operating Rules. Updates entire document based on lessons learned from Belvoir deployment.



The Federation for Identity and
Cross-Credentialing Systems®

FiXS® Policy Document
Version 3.0
September 1, 2010

www.fixs.org

Copyright 2010 by the Federation for Identity and Cross-Credentialing Systems®, Inc.
All Rights Reserved
Printed in the United States of America
10400 Eaton Place, Suite 500A
Fairfax, VA 22030
(703) 591-9255

TABLE OF CONTENTS

1.0	GENERAL REQUIREMENTS AND DEFINITIONS.....	3
2.0	EXECUTIVE OVERVIEW	3
3.0	U.S. FEDERAL AGENCIES AND U.S. DEPARTMENT OF DEFENSE INTERFACES	6
4.0	FIXS MEMBER, SUBSCRIBER, AND CREDENTIAL HOLDER REQUIREMENTS.....	6
5.0	SECURITY	7
6.0	PRIVACY POLICY AND STATEMENT	8
7.0	INTELLECTUAL PROPERTY POLICY STATEMENT	12
8.0	ANTI-TRUST POLICY STATEMENT.....	15
9.0	CONFLICT OF INTEREST POLICY	21
10.0	TERMS OF USE OF FIXS INTELLECTUAL PROPERTY AND LICENSING	25
11.0	BRAND, TRADEMARK, AND GRAPHICS POLICY.....	28
12.0	DISASTER RECOVERY	35

1.0 GENERAL REQUIREMENTS AND DEFINITIONS

The purpose of this policy document is to set forth the policy framework and principles of operations of the Federation for Identity and Cross-Credentialing Systems, Inc®.(FiXs®). This policy framework is integral with other FiXs foundational and governance documents, rules, and procedures, which include, but are not limited to the: FiXs Bylaws, FiXs Operating Rules, FiXs Implementation Guidelines, FiXs Trust Model, FiXs Security Guidelines, FiXs Technical Architecture Specifications as well as the processes, the physical systems and architecture and all other elements and components of the FiXs Network.

2.0 EXECUTIVE OVERVIEW

Introduction

The Federation for Identity and Cross-Credentialing Systems (FiXs) is comprised of private companies of various sizes, not-for-profit organizations, and government organizations that support and contribute ideas, knowledge, and technologies associated with implementing a secure identity cross-credentialing network that is based on open standards, world-class processes, and proven, industrial-strength technologies and security. Similar to the financial industry in managing transactions across a myriad of financial organizations securely and reliably through their trusted financial networks, FiXs has developed an interoperable electronic means of authenticating individuals who are duly vetted through a series of audited procedures and certifying authorities to ensure system integrity.

The Federation provides a federated identity management network and certified system solutions and capabilities to provide member organizations the ability to authenticate individuals' identities. The network supports member organizations in: business to business; government to business; and business to government transactions from other member organizations which may be different, or unknown, to that organization. This capability is provided with a high-degree of accuracy and "trust" through the application of a Federated Trust Model enforced by FiXs. These solutions and capabilities can be utilized worldwide, in remote or fixed environments, wired or wirelessly, and in real-time. The network also supports revocation processes within a three-hour span.

To be clear, FiXs itself is predominantly a standard – setting body with a Governance Model, to include Trust Model. FiXs itself does not deploy nor implement identity authentication technologies or capabilities. Other than managing the oversight of the FiXs Trust Broker (through the Configuration Control Board and Executive Committee), all FiXs-based components and

capabilities are implemented by commercial entity FiXs members who have met certain deployment standards and been certified and/or authorized by FiXs to operate.

History

FiXs was formed as a coalition, in 2002, in piloting a federated identity transaction model and was incorporated as a 501(c) 6 not-for-profit corporation in 2004. FiXs maintains its' status as a 501(c) 6 "trade association" consistent with the requirements of the U.S. Internal Revenue Service and a corporation standing under the laws of the Commonwealth of Virginia. A long-standing affiliation with the Defense Manpower Data Center (DMDC) and its Defense Cross-Credentialing Identification System (DCCIS) program has enabled participating Department of Defense and industry members to achieve secure and interoperable identity verification and authentication for secure facility access. In 2005, FiXs was selected as the FCW Events Government Solution Center Pioneer Award for most "Successful Public/Private Sector Partnership." The award singled out FiXs for recognition as a premier example of a program managed collaboratively by government and non-government partners that tangibly improved government operations and that of their commercial counterparts.

Operations

The FiXs Network and FiXs-certified solutions employ a Federated Trust Model, allowing the broadest range of disparate organizations to inter-operate and authenticate identities and then to locally manage privileges. The essential underpinnings of the FiXs Federated Trust Model are based on two inter-related parts: a trusted organization and a trusted individual identity within that organization. The two parts are linked through a "chain of trust" process that permits vetted and trusted organizations the ability to create and issue an individual's identity credential that can be authenticated and managed over the trusted and secure network by other members of the Federated Trust Model. Once the identity credential is established in this manner, it can be used in various role-based workplace environments to assign privileges consistent with the objectives and unique requirements of that member organization. FiXs' role is limited to identity authentication, which occurs prior to role, privilege designations, or authorizations being assigned by member organizations. This identity authentication model can support either physical or logical privilege or "authorization" designations.

The FiXs Network applies currently proven and available identity management technologies, in conjunction with biometric identification and can be used to verify the identity of personnel seeking to physically enter government or military-controlled areas, as well as the widest range of commercial facilities as well

logical access to their systems or applications. FiXs can be used within and between public and private sector organizations and promotes a trusted mechanism for federated identity infrastructures. The FiXs interoperable identity authentication network also is currently the only network certified to inter-operate with the Defense Cross-Credentialing System (DCCIS) of the United States Department of Defense.

FiXs does not grant or deny physical or logical access or determine authorization privileges. Rather, it delivers a trusted ***infrastructure and authentication service*** that provides participating members with the necessary high confidence in the actual identity of individuals requesting access to facilities and systems. The results of the FiXs Network authentication requests can be used by facility and system managers to determine independently whether they will grant or deny access or other privileges based upon their own unique business process needs.

Privacy and Trust

FiXs is unique in that it does not replicate or store identity factors in a single data store. All personal identity information of individuals is kept and maintained at the location of or designated by the organizational sponsor of the individual in a federated manner. As such, personal identity information is “written and stored” once, at the “home location” of the individual. That information is then validated across the network with the applicable “home location” of the individual at the time a credential is presented for authentication.

PIV-1 Aligned and PIV-Interoperable (“PIV-I”)

FiXs employs a set of Operating Rules consistent with Part 1 (PIV-1) of standards issued to implement Homeland Security Presidential Directive 12 (HSPD-12). The Directive seeks to create a “mandatory, government-wide standard for secure and reliable forms of identification issued by the U. S. Federal Government to its employees and contractors (including contractor employees).” Designed to meet these requirements, FiXs provides a secure and certified network that can handle identity transactions consistent with Federal Information Processing Standard (FIPS) 201, Personal Identity Verification Part 1 (PIV-1). Only Federal government organizations can issue PIV credentials, but each Federal entity can choose to accept PIV “aligned” (PIV – 1) or PIV – Interoperable (“PIV – I”) credentials following accepted certification and assessment criteria by the Federal entity. The Department of Defense (DoD) is accepting PIV “aligned” credentials via the FiXs Network through the DoD’s DCCIS infrastructure.

3.0 U.S. FEDERAL AGENCIES AND U.S. DEPARTMENT OF DEFENSE INTERFACES

In its' initial phase, FiXs successfully worked with the U. S. Department of Defense (DoD) in establishing a mutually-trusted, inter-operable community wherein DoD contractors, vendors and trading partners are able to exchange approved data to authoritatively authenticate their identities. Currently, FiXs is the only organization inter-operable with DCCIS.

FiXs and the Department of Defense's Defense Manpower Data Center (DMDC) have signed a formal Memorandum of Understanding attesting to maintaining this trusted relationship with the DoD. FiXs is committed to including other partners throughout the Federal Government, such as the first responder community, and with other public and private sector organizations, both in the United States and internationally that seek a secure, scalable, rules-based, inter-operable identity authentication capability.

- 3.1 Federal Agencies or the DoD, as applicable, have the responsibility for informing Federal/DoD facilities and locations participating in the FiXs Network of the FiXs policy and procedures, as they may apply to them. The DoD also operates and maintains the Department of Defense's Trust Gateway Broker ("DCCIS router") and administers the Defense Cross-Credentialing Identification System (DCCIS) Rules allowing identity cross-authentication with the FiXs Network.
- 3.2 DoD members that have been issued a DoD Common Access Card (CAC) fulfill the current criteria as set by the FiXs Trust Model and, as they are registered in DCCIS, they will be allowed to have their credential authentication attributes pass across the FiXs Network.
- 3.3 This policy does not prescribe that Federal Agencies or DoD facilities and/or installations recognize FiXs members enrolled in the FiXs Network physical or logical access privileges. Access to any Federal/DoD facility or system is subject to the sole determination of the Federal/DoD site Security/Access Control Official for that federal facility or system, as applicable.

4.0 FiXs MEMBER, SUBSCRIBER, AND CREDENTIAL HOLDER REQUIREMENTS

FiXs, all FiXs Members in any membership category, subscribers, individual credential holders and all entities or individuals participating in the operations of the FiXs Network or who possess FiXs-certified Credentials have an affirmative responsibility to uphold and support the governance and operational rules and

policies of the Federation. Any misuse, abuse, or negligence in supporting these affirmative obligations may result in having such entities or individuals' ability to participate in any such capacity within FiXs or on the FiXs Network revoked along with being subject to any other criminal or civil penalties that may be available. Each FiXs participating industry member is responsible for ensuring that all industry facilities and locations participating in the FiXs Network will fully implement the FiXs policies and Trust Model and the procedures as defined in the FiXs Operating Rules.

5.0 SECURITY

The intent of this section is to ensure the integrity and availability of all FiXs connected systems, and to ensure the security and privacy of the data stored, generated, and processed by the FiXs Network. Further, it is the intent of this policy in any of its manifestations to ensure secure inter-operability with relevant DoD Networks. Additional guidelines, procedures, and technical implementations are detailed in the FiXs Security Guidelines.

- 5.1 All individuals and organizations subject to this policy shall use reasonable and practicable measures to ensure that:
 - Information will be protected from unauthorized access.
 - Confidentiality of information is assured.
 - Integrity of information is maintained.
 - Regulatory and legislative requirements are met.
 - Systems are maximally available to perform their defined functions.
 - Access to data is restricted only to those who have a specific need and authorized access.
 - All changes are logged.
 - Privacy of individual's data is appropriately protected.
- 5.2 All individuals and organizations subject to this policy shall be responsible for implementing and monitoring such security technologies and procedures as required to address the objectives of this policy.
- 5.3 All individuals and organizations subject to this policy shall be responsible for reporting any breach of this policy and for remediation, as appropriate.
- 5.4 Compliance with this security policy is subject to audit by FiXs as well as certain government authorities. Documented failure to comply with this security policy is grounds for denial of access to the FiXs Network and revocation of credentials.

6.0 PRIVACY POLICY AND STATEMENT

The Federation for Identity and Cross-Credentialing Systems, Inc. (“FiXs”) recognizes that the individuals who participate in the FiXs Network value their privacy. Protecting individual privacy is also important to FiXs. To provide notice and information to users and suppliers to the FiXs Network, FiXs is furnishing this Privacy Policy and Statement setting forth FiXs’ privacy policy related to creating and managing credentials and authentication inquiries on the FiXs Network or FiXs-certified Credentials. Use of the FiXs Network is governed by the following documents:

FiXs Trust Model*
FiXs Policy Statements/Guidelines*
FiXs Operating Rules*
FiXs Security Guidelines*
FiXs Technical Architecture and Specifications*
Federal Privacy Act

* As amended from time-to-time by FiXs

The Trust Model imposes obligations on all organizations participating in the FiXs Network to secure and protect all personally identifiable information (“*personal information*” or “*PII data*”) in conformance with the minimum standards outlined in the documents listed above. This Privacy Policy and Statement (“**Privacy Statement**”) describes the minimum privacy practices to be applied by all FiXs-certified Credential issuers and FiXs Network service provider(s) in connection with the governance model, to include the FiXs Trust Model and FiXs Operating Rules.

All FiXS member companies are expected to implement personal information protection policies to the extent practicable, and in compliance with respective laws. This includes providing notice to individuals about what the member company will do with their personal information; choice for the individual with regard to the provision of any discretionary personal information; access for the individual to information held by the member company, including the opportunity to correct personal information and a redress process if decisions are made in light of inaccurate personal information; security procedures for the systems holding personal information; and a proper enforcement process for company employees who violate those privacy policies.

The following policy serves as the standards for the collection, use, retention, and security of personal information for **all** persons or organizations that provide services in connection with the FiXs Network.

Collecting Personal Information

In order to accomplish the objective of authenticating personal identity among and between relying parties (“**Relying Parties**”) subscribed to the FiXs Network, the following personal information is collected and stored by the issuer as described below:

- a. Individual first name, last name and middle initial
- b. Employee identification number
- c. Digital photograph
- d. 10 fingerprints, as applicable
- e. A copy of the completed Immigration and Naturalization Service Form I-9.
- f. Two government-issued picture identification documents i.e. “breeder documents”
- f. Other identifying personal information that is necessary for the “trust level” of credential that the individual is applying for, as prescribed by the entity who sponsors the individual as a user

The entity that sponsors individual users is referred to as the “**Subscribing Party**.” The Subscribing Party will select a FiXs-certified solution provider to enroll, issue credentials, and manage the users that the Subscribing Party sponsors to receive a FiXs-certified Credential. The sponsor will designate the single secure Provider location that will serve as a central repository of its’ sponsored users’ personal information for purposes of identity authentication using the FiXs Network. Personal information may only be stored at this single location and may not be replicated or passed across the FiXs Network. This information will be retained for the longest period required by applicable laws or regulations.

Any personal information that is obtained solely for the purposes of vetting ones’ identity for credential issuance purposes is not required to be maintained or stored for FiXs Network authentication purposes. However, an employer or sponsor may store such information for its own records retention purposes in accordance with its own regulatory, statutory, or business requirements. In such cases, that employer or sponsor should inform the credential holder as to its record retention policies, procedures, and practices.

Disclosures of Information

Neither FiXs nor its certified Credential Issuers or solution providers shall disclose or otherwise transfer any personal information collected for credential issuance purposes, except as specified in this policy. FiXs-certified Credential Issuers and service providers are each responsible to ensure the compliance of their contractors and agents with this Privacy Statement. Certain personal information provided for credential authentication purposes will be accessible to

parties relying upon the FiXs-certified Credential that may be presented for authentication purposes.

Consistent with applicable laws and regulations, information collected about individuals who possess FiXs-certified Credentials for authentication purposes may be shared as necessary for authorized law enforcement, homeland security, or national security activities.

Use of Personal Information in Cross-Credentialing for the Purpose of Identity Authentication

Except as specified in this Privacy Statement, the personal information an individual provides for identity authentication shall not be used by any party for any other purpose.

When seeking entry to selected facilities, application, or systems of organizations, agencies, companies, or Relying Parties that are participating in the FiXs Network, an individual may be asked to produce information or provide personal information, including one or more fingerprints. This information will be transmitted across the FiXs Network, in an encrypted form, and compared with information held by the FiXs-certified Solution Provider designated by the individual's sponsor to retain such person's personal information. The FiXs-certified Solution Provider will perform a comparison of the data on file and will transmit the results of this comparison, in an encrypted form, to the Relying Party making the authentication request. Personal information that is sent for authentication to the Relying Party facility or system that an individual seek to access will not be retained by that Relying Party, but such party may create its own record of such individual's credential authentication and request for access.

All decisions regarding access, or privileges to be granted, to participating facilities and systems will be controlled by the operators of such facilities or systems based on the criteria they have independently established.

The FiXs-certified Solution Provider will keep logs of identity authentication requests received from participating parties. These logs will be retained for the purpose of audit, compliance, and other authorized purposes.

Security Procedures

The FiXs Network maintains physical, electronic, and procedural safeguards that comply with U.S. government standards to protect an individual's personal information. These safeguards are routinely monitored and communicated to FiXs representatives and FiXs Network Solutions Providers, Credential Issuers and sponsoring or subscribing parties. Each Network Solutions Provider, Credential Issuer, and sponsoring party is responsible to protect personal

information from unauthorized disclosure or loss, at a minimum, in accordance with such safeguards. Without limiting the foregoing, an individual's personal information will be stored in a database secured in at least the same manner that the individual's sponsor generally protects the personal information of its employees.

For security purposes and to ensure that the credential authentication service remains available to all users, FiXs employ software programs to monitor traffic to identify unauthorized attempts to access, upload, or change information, or otherwise cause damage.

Any Network Solutions Provider, Credential Issuer or sponsoring party that becomes aware that personal information has been disclosed or used other than in accordance with this Privacy Statement, including any unauthorized disclosure or loss of information, should immediately notify FiXs in writing of such event, and cooperate fully with FiXs in investigating the relevant circumstances. An individual that becomes aware that personal information has been disclosed or used other than in accordance with this Privacy Statement, including any unauthorized disclosure or loss of information, should immediately notify the applicable sponsor and FiXs in writing of such event, and cooperate fully with such sponsor and FiXs in investigating the relevant circumstances.

Any FiXs Solution Provider, Credential Issuer, or Subscribing Party that breaches its obligations under this Privacy Statement with respect to personal information will defend, indemnify, and hold harmless FiXs, and its officers, directors, employees, contractors and agents, from and against all liabilities, damages, expenses (including reasonable attorneys fees and costs), fines, and claims of any kind or based on any legal theory, arising from or relating to such breach.

Notification of Changes

FiXs reserves the right to change, modify, or update this Privacy Statement at any time without notice. The current version of all such governance documents will be maintained on the FiXs website (www.fixs.org). All interested persons and entities should review the published Privacy Statement regularly in order to remain knowledgeable about the Privacy Statement and any revisions to it.

How to Contact Us

FiXs' Privacy Statement is available on the FiXs web site at www.fixs.org. Any questions concerning the FiXs privacy policies should be directed to the FiXs Administrator by telephone at 703-591-9255.

7.0 INTELLECTUAL PROPERTY POLICY STATEMENT

Purpose

The purpose of this FiXs Intellectual Property Policy Statement (“**IP Policy**”) is to set forth FiXs’ policy as it pertains to the creation, management, and ownership of the intellectual property developed through the activities of FiXs or otherwise owned or licensed by FiXs.

Applicability

This IP Policy applies to all FiXs member firms in all membership categories and all FiXs officers, directors, employees, contractors and contract employees, including all individuals who support the various FiXs committees and work groups or participate in other FiXs meetings, past, present and future. This policy covers all types of intellectual property, including patents, copyrights, trade secret and other proprietary rights of any kind, e.g., inventions; discoveries; trade secrets, trademarks, service marks, writings, art works, software, and other literary works.

Background

FiXs is a registered tax-exempt, 501(c) 6 trade association whose objectives are to establish standards and, provide objective oversight of the FiXs Network and to provide a forum for discussing, defining, and developing necessary operating rules, policies, guidelines and implementation standards for use by Network users. These activities entail providing an open and trusted environment where interoperable procedures, processes, and technologies can be tested and implemented. The goal of those activities is to allow FiXs’ commercial users and the government; including the Department of Defense and U.S. civilian agencies, state and local governments and agencies (including first responders and emergency personnel), along with their contractors and constituents, to interact in a secure, efficient, and effective manner without being unduly subject to proprietary technologies or vendor influence, or having to create redundant, ineffective, or inefficient systems.

FiXs is an “open membership” organization comprised of systems integrators, solution providers, technology firms, financial institutions, consulting companies, not-for-profit associations, and various other organizations (including government agencies) representing a large community of interest, contributing in an open forum to pursue the deployment and use of open, inter-operable, and accessible industry standards, technologies, and processes to authenticate secure identity credentials.

License to Use

Expressly authorized members of FiXs may be licensed to use the intellectual property of FiXs in providing identity authentication solutions to their customers or other parties consistent with the terms of specific licensing agreements.

Proprietary Rights

Based upon the authority in the FiXs Bylaws and Operating Rules, FiXs may grant designated Members a non-exclusive license to possess and use all or portions of FiXs' Work Product(s) and Pre-existing Property, as identified in this Policy, that are required for a Member to make use of the FiXs Network consistent with the Operating Rules. FiXs may also grant authorized Members the right to grant to FiXs Issuers and FiXs Relying Parties a sublicense to possess and use those portions of the FiXs Work Product and Pre-existing Property required for a Member to make use of the FiXs Network solely in accordance with the Operating Rules.

Each Member will promptly identify to FiXs any specific portions of the Member's intellectual property that may need to be furnished to FiXs, other Members or other users to enable FiXs, its Members or other users to use or modify elements of the FiXs Network. To facilitate such purposes, the respective Member hereby grants to FiXs a non-exclusive, perpetual, worldwide, royalty-free, irrevocable license to copy, modify, distribute, display, perform, make, import and have made, and sublicense to its other Members, Credential Issuers, Issuer Sponsors, Network Service Providers, Member Service Providers, Members and other users of the FiXs Network, all intellectual property, including software, of that Member that is included in or integral to the operation of the FiXs Network or the FiXs Work Product, for purposes of the use, operation, support or enhancement of the FiXs Network. To the extent a Member wishes to obtain further clarification of such license grant, the Member and FiXs will work together to develop the appropriate form of license terms and conditions to govern any license or sublicense to be granted by any Member to the operators or users of the FiXs Network, provided that FiXs shall retain the sole authority to approve the final form and content of such license terms and conditions. Each Member's intellectual property that (1) is not the FiXs Network or FiXs Work Product or a modification of the FiXs Network or FiXs Work Product, (2) adds functionality to the FiXs Network or FiXs Work Product (i.e., the FiXs Network or FiXs Work Product are not dependent on it) and (3) was or is created without funding from FiXs, directly or indirectly, shall belong to such Member and shall not be subject to the above-stated license grant.

FiXs shall have sole and exclusive intellectual property ownership rights in any and all work product created or developed by all FiXs officer, directors, employees, contractors and contract employees, as well as any individuals who

support the various FiXs committees and work groups or participate in other FiXs meetings, regarding work product prepared by or for FiXs (“**FiXs Work Product**”).

Any intellectual property, including software that existed before such FiXs Work Product was created or that is created thereafter, other than for or on behalf of FiXs, shall remain the property of the respective owner, subject to the above-stated license grant to FiXs and its Members. In addition, intellectual property funded by or developed at FiXs expense shall be and remain the sole and exclusive property of FiXs.

FiXs Work Product and Pre-existing Property for FiXs Network

- FiXs brand, marketing collateral, FiXs-branded documents, trademark, and all other marks or designations of FiXs
- FiXs Bylaws
- FiXs Operating Rules/Guidelines
- FiXs Policies and Procedures
- FiXs Trust Model
- FiXs Security Guidelines
- FiXs Technical Architecture Specification
- FiXs Network (as defined in the FiXs Bylaws, Version 3.0, September 1, 2010, 2006, page 2, Article I, Section 4, paragraph a.), and associated interfaces
- FiXs Trust Gateway Broker (TGB) software, components and any additional TGBs to be established in the future
- FiXs software and software interfaces related to the FiXs domain server (FDS)
- FiXs software related to the authentication stations and various configurations thereto
- FiXs Recommendations for Creating a Unique Identifier for FIPS 201-aligned FiXs Credential (CHUID)
- FiXs Network additions, enhancements, updates, all associated software code versions, and all documentation related to the above artifacts.

* As may be revised, amended or modified from time to time. Other property may be created subsequent to this date, which will be similarly included.

Compliance

All member companies and individuals have an obligation to protect FiXs' intellectual property rights and an ongoing obligation not to infringe upon those rights. Strict compliance with this policy is also a condition of membership in FiXs.

It is the policy of FiXs vigorously to enforce the provisions of this IP Policy to the fullest extent of the law.

If there are questions about, or perceived violations of, this IP Policy, members will promptly report such matters to the FiXs President or FiXs Corporate Secretary.

8.0 ANTI-TRUST POLICY STATEMENT

Purpose

The Federation for Identity Cross-Credentialing Systems, Inc. ("FiXs"), a tax-exempt, 501(c) (6) trade association consisting of commercial and other non-profit entity members, as well as government agency participants, recognizes and endorses the policies underlying the nation's antitrust laws. Activities that intentionally or unintentionally reduce competition or restrain trade are contrary to FiXs' belief in competition and FiXs policy. In order to ensure that FiXs members, directors and staff understand and comply with the antitrust laws and FiXs policy, the FiXs Board of Directors has adopted the following Antitrust Policy Statement.

FiXs' activities consist of efforts by its commercial and non-profit members, as well as government agency participants, pertaining to the design, development or application of theoretically interchangeable identity management solution sets. One of FiXs' objectives is to establish a Network that will serve as a trusted environment in which interoperable identity management procedures, processes, and technologies can be tested and implemented. The goal of those activities is to allow FiXs' commercial users and government agencies such as the U.S. Department of Defense and civilian agencies, state and local governments and agencies (including first responders and emergency personnel), along with the agencies' contractors and constituents, to interact effectively and efficiently with respect to identity management.

These trade association activities are subject to federal and state antitrust laws. A trade association may be held legally responsible for the authorized and, under certain circumstances, unauthorized acts of its members that violate the antitrust laws. Therefore, in all FiXs activities, each member and FiXs staff is responsible for following FiXs' policy of compliance with all antitrust laws. FiXs officers, directors, committee chairs, and FiXs staff are responsible for making this policy known to all members of FiXs and for ensuring compliance in the course of activities pursued by FiXs.

Overview of the Antitrust Laws

FiXs and its members are subject to both federal and state antitrust laws. The federal antitrust laws are intended to prevent a wide range of conduct that interferes with or threatens to interfere with competition. In addition, most states have enacted antitrust laws that generally parallel the federal antitrust laws. The most important antitrust statutes relating to an association's activities are as follows:

Section 1 of the Sherman Act in broad terms prohibits "every contract, combination . . . or conspiracy" in restraint of trade. This prohibition covers all types of anticompetitive agreements or contracts, including but not limited to price-fixing agreements. The Sherman Act prohibits any agreement among current or potential competitors that affects any component of the price of a product or service, regardless of the purpose of the agreement and regardless of whether the price agreed to is "fair" or "reasonable." An agreement among buyers that fixes the price they will pay for a product or service is likewise prohibited. "Price" is defined broadly under the law to include all price-related terms, including discounts, rebates, commissions, and credit terms. Agreements among competitors to fix, restrict, or limit the amount of a product or service that is produced or offered may be treated the same as a price-fixing agreement.

Section 1 also prohibits, among other practices, bid-rigging agreements among actual or potential competitors, market or customer allocation agreements among competitors, and certain group boycott agreements.

An unlawful agreement need not be formal or reduced to writing; unlawful agreements may be inferred from circumstantial evidence, such as competitors taking parallel action on prices after discussing prices at a meeting, even if there were no express words of agreement at the meeting. An association's members and staff must also remember that the Sherman Act is a criminal conspiracy statute. If you are not an active participant - if you merely sit by at a meeting while the members of the association engage in an illegal discussion concerning price-fixing, you may be held criminally responsible, even though you said nothing during the discussion.

Section 5 of the Federal Trade Commission Act prohibits "unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in

or affecting commerce.” This broadly worded statute prohibits conduct that would violate one of the other antitrust laws, such as price-fixing, as well as practices that closely resemble other antitrust violations in their adverse effect on competition. The Federal Trade Commission Act reaches anticompetitive acts committed by single persons or companies whether or not there is any agreement or “combination;” it also covers joint actions. The FTC has broad power to determine what constitutes an unfair method of competition or unfair or deceptive act or practice under any given circumstances.

Penalties for Violation of the Antitrust Laws

Violations of the antitrust laws can have very serious consequences for FiXs, its members, and their employees. The Sherman Act is a criminal statute. Violations of the act may be prosecuted as felonies and are punishable by steep fines and imprisonment for up to ten years. In addition, the federal government, state attorneys general, and any person or company claiming to have been injured by an antitrust violation may sue to recover three times the amount of the damages, plus attorney’s fees.

The maximum statutory antitrust fines are \$100 million for corporations and \$1 million for individuals. The size of an organization’s fine may be increased, however, to as much as twice the pecuniary gain derived from the offense or twice the loss suffered. This can be a very large number; antitrust fines for corporations exceeding \$10 million have become common and some fines have topped \$100 million. The collateral consequences of an antitrust conviction can be devastating for corporations. They include debarment from federal contracting, exposure to follow-on treble damages suits by private parties, which are often filed as class actions, exposure to investigations and enforcement actions in other countries, disruption of business, and the expense of defending antitrust investigations and lawsuits. In addition, the events surrounding an antitrust violation may provide the basis for other charges. Prosecutors often combine antitrust charges with allegations of wire fraud, mail fraud, and providing false statements to the government, all of which carry additional penalties.

For individuals, the consequences of involvement in an antitrust offense include, in addition to potential fines and jail time, loss of job and benefits, loss of reputation, loss of future employment opportunities, and exposure to litigation.

Violation of the Federal Trade Commission Act can result in issuance of a cease and desist order, which can place extensive governmental restraints on the activities of an association and its members or call for dissolution of the trade association itself. Failure to obey such an order can result in penalties of as much as \$10,000 per day.

Recognize and Avoid High-Risk Conduct

Certain antitrust violations are so likely to result in criminal prosecution that they are often referred to as “hard core” offenses. Conduct that falls in this category is

automatically illegal; absence of actual anticompetitive effects will not be a defense. Conspiracies among actual or potential competitors to restrict competition are in this category, and include the following:

Price-Fixing Agreements

the government strictly enforces the price-fixing prohibitions of the Sherman Act. A price-fixing violation may be inferred from similar price behavior by an association's members, even in the absence of a written or oral agreement.

Agreements to Allocate Customers or Markets

Agreements among competitors (or potential competitors) to allocate or divide markets, territories, customers, or sales channels are automatically illegal and are often prosecuted as criminal offenses. Even an informal agreement whereby one company agrees to stay out of another's territory or not to solicit its customers constitutes a violation of the antitrust laws.

Bid-Rigging Agreements

Agreements or understandings among competitors (or potential competitors) on any method by which prices or bids will be determined, quoted, or awarded are illegal. This includes: rotating bids; agreements regarding who will bid or not bid; agreements establishing who will submit bids to particular customers or for particular projects; and exchanging or advance signaling of the prices or other terms of bids. Bid rigging is nearly always prosecuted as a criminal offense.

Other Potentially Risky Conduct

There are other activities which, though typically not subject to criminal prosecution, are nevertheless potentially high-risk because they frequently lead to investigations or lawsuits, and a finding of liability may have severe adverse consequences.

Group Boycotts

An agreement with competitors, suppliers, or customers not to do business with another party, or to use concerted economic leverage against another party, may be found illegal as a boycott or "concerted refusal to deal."

Membership Restrictions

Assuming that the members of an association derive an economic benefit from membership, the denial of membership to an applicant may constitute a restraint of trade if it substantially impairs the ability of the applicant to compete and is not based on objective criteria. Similarly, no member of a trade association can be forced to participate in discussions or to attend association meetings.

Exclusionary Standardization and Certification And Self-Regulation

Association voluntary standardization and certification programs and self-regulatory programs such as industry codes of ethics generally are pro-competitive and lawful. Such activities may be found unlawful, however, if they have the effect of fixing prices or if they injure competition by unreasonably excluding some firms from a market, limiting output of products or services, or discouraging innovation. Standards and certification programs and industry self-regulatory programs should be conducted according to principles of voluntarism, objectivity, and due process. “Due process” means: all stakeholders have a right to participate in the formation of the standard, certification criteria, or code of ethics; the process is open and free from dominance by any particular industry segment or company; and there is a right to appeal from adverse decisions.

FiXs Anti-trust Policy and Guidelines

It is the policy of the FiXs that no member, director, or staff member shall:

- Seek or enter an agreement among competitors to fix or stabilize prices
- Seek or enter and agreement among competitors to limit production
- Hinder non-members' access to any market
- Economically coerce members
- Seek or enter an agreement not to do business with any party, or to do business with another party only on specified terms
- Seek or enter an agreement among competitors to allocate markets, territories, or customers
- Otherwise unreasonably restrict competition or engage in activity violative of any antitrust law.

In order to ensure that the above policy is fully implemented, the FiXs Board of Directors has adopted the following guidelines:

General Guidelines

1. A full description of the FiXs' intent to comply fully with the antitrust laws will be included in its written Policy Statement.
2. All FiXs members, directors, committees and staff shall receive and familiarize themselves with the FiXs' Antitrust Policy Statement.
3. FiXs' legal counsel will periodically update members, directors and staff concerning antitrust issues and review FiXs' antitrust compliance.
4. FiXs' legal counsel will approve in advance all new FiXs programs or changes in existing programs that may have potential antitrust implications.

5. If possible, all FiXs meetings, including conference calls, shall be regularly scheduled and all members should receive reasonable advance notice. In no case shall members hold informal “rump” meetings.
6. An agenda will be prepared for each FiXs meeting, and the agenda shall be reviewed in advance by legal counsel
7. Understand the purposes and authority of each FiXs committee or other group in which you participate.
8. If possible, legal counsel will be present at all meetings of the Board of Directors and at any other meeting at which sensitive issues will be discussed.
9. The minutes of all Board and Committee meetings, as applicable, will be reviewed by legal counsel before their approval and dissemination.
10. The minutes of all FiXs meetings will be accurate, and the association executive will not sign minutes that are materially inaccurate or incomplete.
11. Any action by FiXs or its Board of Directors which has the effect of rejecting a membership application should not become final without approval by legal counsel.
12. Any FiXs member who has concerns about the propriety under the antitrust laws of any discussion or activity at any FiXs meeting should disassociate himself from any such discussions or activities, leave any meeting if the discussion or activity persists, and report the matter to a FiXs officer and/or FiXs legal counsel.

Membership Policy

FiXs will not:

1. Exclude any entity from FiXs membership unless it fails to satisfy objectively reasonable and neutral membership criteria.
2. Restrict FiXs members from dealing with nonmembers.
3. Limit access to information developed by FiXs, unless such limitation is firmly grounded upon the need to protect trade secrets or other proprietary information.

Topics of Discussion that will be Avoided at FiXs Meetings

1. Current or future prices.
2. What constitutes a “fair” profit level?
3. Possible increases or decreases in prices.
4. Standardization or stabilization of prices.
5. Pricing discounts.
6. Credit terms.
7. Control of sales or levels of output or production.
8. Allocation of markets.

9. Refusal to deal with an entity because of its pricing or distribution practices.
10. Marketing, purchasing, or pricing decisions of individual companies.
11. Whether or not the pricing practices of any industry member are unethical or constitute an unfair trade practice.
12. Individual company bids or intentions to bid for particular products, procedures for responding to bid invitations or specific contractual arrangements.
13. Plans of individual companies concerning the design, characteristics, production, distribution, marketing or introduction dates of particular products, including proposed territories or customers.
14. Discuss or exchange information regarding the above matters during social gatherings incidental to FiXs-sanctioned meetings, even in jest.

These prohibitions highlight only the most basic antitrust principles. Participants in FiXs meetings should consult counsel with respect to specific activities, interpretations or advice.

Conclusion

This policy statement is a general statement of antitrust principles. No policy statement can anticipate every issue that may arise in the course of an organization's activities. FiXs and its members must remain continuously aware of potential antitrust concerns. If any participant has a question about the legality of a proposed activity or course of action, the matter should be immediately referred to the FiXs President who will discuss it with legal counsel. In this manner, FiXs will be able to pursue its legitimate objectives while fully complying with the antitrust laws.

9.0 CONFLICT OF INTEREST POLICY

Article I. Purpose

The purpose of the conflict of interest policy is to protect this tax-exempt organization's (Organization) interest when it is contemplating entering into a transaction or arrangement that might benefit the private interest of an officer or director of the Organization or might result in a possible excess benefit transaction. This policy is intended to supplement but not replace any applicable state and federal laws governing conflict of interest applicable to nonprofit and charitable organizations.

Article II, Definitions

1. Interested Person

Any director, principal officer, or member of a committee with governing board delegated powers, who has a direct or indirect financial interest, as defined below, is an “interested person”.

2. Financial Interest

A person has a financial interest if the person has, directly or indirectly, through business, investment, or family:

- a. An ownership or investment interest in any entity with which the Organization has a transaction or arrangement,
- b. A compensation arrangement with the Organization or with any entity or individual with which the Organization has a transaction or arrangement, or
- c. A potential ownership or investment interest in, or compensation arrangement with, any entity or individual with which the Organization is negotiating a transaction or arrangement.

Compensation includes direct and indirect remuneration as well as gifts or favors that are not insubstantial.

A financial interest is not necessarily a conflict of interest. Under Article III, Section 2, a person who has a financial interest may have a conflict of interest only if the appropriate governing board or committee decides that a conflict of interest exists.

Article III, Procedures

1. Duty to Disclose

In connection with any actual or possible conflict of interest, an interested person must disclose the existence of the financial interest and be given the opportunity to disclose all material facts to the directors and members of committees with governing board delegated powers considering the proposed transaction or arrangement.

2. Determining Whether a Conflict of Interest Exists

After disclosure of the financial interest and all material facts, and after any discussion with the interested person, he/she shall leave the governing board or committee meeting while the determination of a conflict of interest is discussed and voted upon. The remaining board or committee members shall decide if a conflict of interest exists.

3. Procedures for Addressing the Conflict of Interest

- a. An interested person may make a presentation at the governing board or committee meeting, but after the presentation, he/she shall leave the

- meeting during the discussion of, and the vote on, the transaction or arrangement involving the possible conflict of interest.
- b. The chairperson of the governing board or committee shall, if appropriate, appoint a disinterested person or committee to investigate alternatives to the proposed transaction or arrangement.
 - c. After exercising due diligence, the governing board or committee shall determine whether the Organization can obtain with reasonable efforts a more advantageous transaction or arrangement from a person or entity that would not give rise to a conflict of interest.
 - d. If a more advantageous transaction or arrangement is not reasonably possible under circumstances not producing a conflict of interest, the governing board or committee shall determine by a majority vote of the disinterested directors whether the transaction or arrangement is in the Organization's best interest, for its own benefit, and whether it is fair and reasonable. In conformity with the above determination it shall make its decision as to whether to enter into the transaction or arrangement.

4. Violations of the Conflicts of Interest Policy

- a. If the governing board or committee has reasonable cause to believe a member has failed to disclose actual or possible conflicts of interest, it shall inform the member of the basis for such belief and afford the member an opportunity to explain the alleged failure to disclose.
- b. If, after hearing the member's response and after making further investigation as warranted by the circumstances, the governing board or committee determines the member has failed to disclose an actual or possible conflict of interest, it shall take appropriate disciplinary and corrective action.

Article IV Records of Proceedings

The minutes of the governing board and all committees with board delegated powers shall contain:

- a. The names of the persons who disclosed or otherwise were found to have a financial interest in connection with an actual or possible conflict of interest, the nature of the financial interest, any action taken to determine whether a conflict of interest was present, and the governing board's or committee's decision as to whether a conflict of interest in fact existed.
- b. The names of the persons who were present for discussions and votes relating to the transaction or arrangement, the content of the discussion, including any alternatives to the proposed transaction or arrangement, and a record of any votes taken in connection with the proceedings.

Article V, Compensation

- a. A voting member of the governing board who receives compensation, directly or indirectly, from the Organization for services is precluded from voting on matters pertaining to that member's compensation.
- b. A voting member of any committee whose jurisdiction includes compensation matters and who receives compensation, directly or indirectly, from the Organization for services is precluded from voting on matters pertaining to that member's compensation.
- c. No voting member of the governing board or any committee whose jurisdiction includes compensation matters and who receives compensation, directly or indirectly, from the Organization, either individually or collectively, is prohibited from providing information to any committee regarding compensation.

Article VI, Annual Statements

Each director, principal officer and member of a committee with governing board delegated powers shall annually sign a statement which affirms such person:

- a. Has received a copy of the conflicts of interest policy,
- b. Has read and understands the policy,
- c. Has agreed to comply with the policy, and
- d. Understands the Organization is charitable and in order to maintain its federal tax exemption it must engage primarily in activities which accomplish one or more of its tax-exempt purposes.

Article VII Periodic Reviews

To ensure the Organization operates in a manner consistent with charitable purposes and does not engage in activities that could jeopardize its tax-exempt status, periodic reviews shall be conducted. The periodic reviews shall, at a minimum, include the following subjects:

- a. Whether compensation arrangements and benefits are reasonable, based on competent survey information, and the result of arm's length bargaining.
- b. Whether partnerships, joint ventures, and arrangements with management organizations conform to the Organization's written policies, are properly recorded, reflect reasonable investment or payments for goods and services, further charitable purposes and do not result in inurement, impermissible private benefit or in an excess benefit transaction.

Article VIII, Use of Outside Experts

When conducting the periodic reviews as provided for in Article VII, the Organization may, but need not, use outside advisors. If outside experts are used, their use shall not relieve the governing board of its responsibility for ensuring periodic reviews are conducted.

10.0 TERMS OF USE OF FIXS INTELLECTUAL PROPERTY AND LICENSING

The FiXs Intellectual Property Policy provides that FiXs may grant designated Members a non-exclusive license to possess and use all or portions of FiXs Intellectual Property. Any possession or use of any FiXs Intellectual Property without a specific license to do so is expressly prohibited.

FiXs expressly authorizes individuals working in support of a FiXs-designated committee, work group, contract or FiXs officially-sanctioned activity a non-exclusive license to use and possess FiXs Intellectual Property solely for the further advancement and/or development of such intellectual property and the objectives of the Federation. All such efforts will be governed by the FiXs Intellectual Property Policy Statement.

Any other use of FiXs Intellectual Property is only authorized under the terms of a separate and individual license or contract. Any such license or contract to use FiXs Intellectual Property shall contain, as a minimum, in addition to any other applicable terms and conditions, the provisions of the FiXs Terms of Use Agreement set forth below.

TERMS OF USE AGREEMENT

THIS TERMS OF USE AGREEMENT (“AGREEMENT”) IS BETWEEN (1) YOU, AS AN INDIVIDUAL CREDENTIAL HOLDER AND/OR THE SPONSOR OR SUBSCRIBING PARTY OF AN INDIVIDUAL CREDENTIAL HOLDER, AS APPLICABLE, AND (2) THE FEDERATION FOR IDENTITY AND CROSS-CREDENTIALING SYSTEMS, INC. (“FIXS”) OR ITS’ AUTHORIZED CREDENTIAL ISSUERS AND SOLUTION PROVIDERS. THIS AGREEMENT APPLIES TO THE USE OF ANY AND ALL FIXS CERTIFIED CREDENTIALS ISSUED BY FIXS OR FIXS AUTHORIZED CREDENTIAL ISSUERS.

BY EITHER SPONSORING THE ISSUANCE OF A FIXS CERTIFIED CREDENTIAL TO AN INDIVIDUAL, OR BEING THE INDIVIDUAL FIXS CERTIFIED CREDENTIAL HOLDER BEING ISSUED A FIXS CERTIFIED CREDENTIAL, YOU AGREE TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THESE TERMS OF USE, PLEASE CANCEL, RETURN, AND/OR REVOKE, AS APPLICABLE, ANY FIXS CERTIFIED CREDENTIAL ISSUED OR PROPOSED TO BE ISSUED, AND CEASE IMMEDIATELY ANY USE OF SUCH CREDENTIAL.

DEFINITIONS

“FiXs Authorized Solution Provider” or “Credential Issuer” is a FiXs member that issues FiXs Certified Credentials to qualified users for themselves and/or other Sponsors or Subscribing Parties and processes and responds to authentication inquiries.

“FiXs Certified Credential” is an identity credential issued by an approved FiXs Credential Issuer who has contracted to follow the FiXs Trust Model and all corollary policies, rules, guidelines and implementation standards for vetting, enrolling, maintaining, and revoking identity credentials.

“Sponsor” is an organization that uses the services of a Credential Issuer and sponsors Subscribers or other participants to be issued FiXs Certified Credentials.

“Subscriber” or “Subscribing Party” is a member or non-member organization that is a Primary Trusted Organization sponsoring individual users to be issued FiXs Certified Credentials.

“FiXs Intellectual Property” includes, without limitation, all components of the FiXs Network; the FiXs brand, marketing collateral, trademark and other FiXs marks; as well as the FiXs Bylaws; Operating Rules, Trust Model and all governance, operational, security and technical specifications documents.

“FiXs Network” is the end-to-end system comprising the physical infrastructure, operating principles and processes to authenticate FiXs Certified Credentials.

“Licensee” is the individual holder (person) of a FiXs Certified Credential or a Subscribing Party or Sponsor of a Subscribing Party.

SCOPE OF LICENSE

Any and all FiXs Intellectual Property used in the issuance, use, and/ or revocation of a FiXs Certified Credential is licensed, not sold. You may use this FiXs Intellectual Property only as expressly permitted in this Agreement. Your use of any other intellectual property provided by, sold by, or used by any FiXs Authorized Solution Provider or Credential Issuer is subject to the separate terms of use granted by the applicable third party with regard to any such intellectual property that is not FiXs Intellectual Property.

GRANT OF RIGHTS

FiXs grants the individual holder of a FiXs Certified Credential, or Subscribing Party, (in each instance, a “Licensee”), as applicable, the non-exclusive, non-transferable, revocable, limited right to use the FiXs Intellectual Property for the sole purposes of identity authentication within, across, and between components of the FiXs Network.

LIMITATIONS AND RESTRICTIONS

The Licensee may not manipulate, alter, change, or create derivative works of FiXs Intellectual Property. Licensee shall not reverse engineer, decompile or disassemble any FiXs Intellectual Property. The Licensee shall only use any FiXs trademark or service mark as expressly authorized to do so.

The Licensee shall adhere to the applicable Operating Rules, Policies, Security Guidelines and other FiXs or third party procedures for the issuance, use, and revocation of FiXs Certified Credentials.

PRIVACY

The Subscribing Party agrees to comply with the FiXs Privacy Policy Statement which is incorporated in full in this Terms of Use Agreement and included herewith.

GOVERNING LAW

Within the United States

This Agreement, and its enforcement and construction, shall be governed in all respects by the laws of the Commonwealth of Virginia (excluding its conflicts of law principles) for all FiXs Certified Credentials issued in or used in the United States or its territories.

Outside of the United States

For all FiXs Certified Credentials issued and used outside of the United States, the laws of the applicable country of issuance and use shall apply to the extent that they conflict with the laws of the Commonwealth of Virginia, U.S.A (excluding its conflicts of law principles).

PERFORMANCE STANDARDS AND WARRANTY

FiXs requires certain minimum performance standards to govern the work to be performed by FiXs Authorized Solution Providers or Credential Issuers. Such performance standards have been promulgated by FiXs by written agreement between FiXs and the FiXs Authorized Solution Provider or Credential Issuer, as applicable.

Each FiXs Authorized Solution Provider or Credential Issuer warrants that its performance hereunder shall conform in all material aspects with such performance standards, and shall provide that if such Solution Provider or Credential Issuer's performance hereunder shall, at any time during the term of this Agreement, fail to conform in all material aspects with such performance standards, it shall correct such non-conforming performance at its sole cost and expense.

LIMITATION OF LIABILITY

FIXS AND ANY FIXS AUTHORIZED SOLUTION PROVIDER OR CREDENTIAL ISSUER SHALL NOT, IN ANY EVENT, BE LIABLE IN CONNECTION WITH ANY ASPECT OF FIXS CERTIFIED CREDENTIAL (E.G., WITHOUT LIMITATION, ISSUANCE OF, REVOCATION OF, CANCELLATION OF, USE OF, OR FAILURE TO DO ANY OF THE FOREGOING WITH RESPEC TO, A FIXS CERTIFIED CREDENTIAL) FOR SPECIAL, INDIRECT, PUNITIVE, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING WITHOUT LIMITATION LOST INCOME, LOST REVENUE, OR LOST PROFIT, WHETHER SUCH DAMAGES WERE FORESEEABLE OR NOT AT THE TIME THAT THIS AGREEMENT WAS ENTERED INTO.

THE SUBSCRIBING PARTY, SPONSOR, OR INDIVIDUAL FIXS CERTIFIED CREDENTIAL HOLDER, AS APPLICABLE, SHALL DEFEND, INDEMNIFY, AND HOLD HARMLESS FIXS, ITS OFFICERS, DIRECTORS, EMPLOYEES, CONTRACTORS AND AGENTS, FROM AND AGAINST ALL LIABILITIES, DAMAGES, EXPENSES, TO INCLUDE REASONABLE ATTORNEYS FEES, FINES, AND CLAIMS OF ANY KIND OR BASED ON ANY LEGAL THEORY, ARISING FROM THE ISSUANCE OF, REVOCATION OF, CANCELLATION OF, USE OF, OR FAILURE TO DO ANY OF THE FOREGOING WITH RESPEC TO, A FIXS CERTIFIED CREDENTIAL.

SEVERABILITY

In case any one or more of the provisions in this Agreement shall, for any reason, be held to be invalid, illegal or unenforceable in any respect, such invalidity, illegality or unenforceability shall not affect any other provisions of this Agreement, and this Agreement shall be construed as if such invalid, illegal or unenforceable provision was and is not contained in this Agreement.

MODIFICATION OR AMENDMENT

This Agreement may be modified by FiXs from time to time as deemed necessary in the sole discretion of FiXs, and Licensee's continued use of a FiXs Certified Credential after such modification will be deemed to be Licensee's agreement to such modified Agreement.

ENTIRE AGREEMENT

The Agreement constitutes the complete agreement between FiXs and Licensee as to its subject matter, and supersedes any and all written and oral communications or agreements previously existing as to this subject matter.

11.0 Brand, Trademark, and Graphics Policy

Article I. Purpose and Introduction

The purpose of this Policy is to promulgate formal standards for the usage of the brands and trademarks of the Federation for Identity and Cross-Credentialing Systems, Inc. ("FiXs" or the "Federation"). It is recognized that increasing customer awareness of FiXs

and FiXs-related offerings is an important market differentiator as well as vital for preservation and protection of the intellectual property assets and property rights of the Federation.

This market awareness and recognition requires consistent usage, presentation, and communication.

Article II. Application and Limitations on Use

Any form of reference to the Federation for Identity and Cross-Credentialing Systems, Inc.; the Federation for Identity and Cross-Credentialing Systems; or FiXs; may be made subject to the limitations set forth in this policy.

Specifically, companies or organizations who maintain membership in “good standing” under the provisions of the Bylaws of the Federation may make use of the FiXs brand and/or trademarks indicating their membership in the Federation consistent with the provisions of this policy.

Further, member organizations that may deploy FiXs-certified or duly authorized service offerings utilizing the FiXs Network or its related attributes or features may indicate that they are a “FiXs-Certified Solution Provider”, a “FiXs-Certified Service Provider”, deploying a “FiXs-Certified Credential”, or “FiXs Credential” meaning that they are deploying some form of FiXs-Certified capability, offering, or feature. The specific terminology to be used will be subject to the specific use case under which the member organization has been affirmatively certified or authorized by FiXs for usage. Only duly authorized FiXs solution or service providers may use the designation that they are FiXs-Certified; deploying any form of “FiXs-Certified” solution or service; deploying a FiXs-Certified Credential, or doing anything under the auspices of FiXs .

Any member organization of the Federation who has NOT been duly certified or authorized to have, use, or provide access to the FiXs Network, FiXs-based solutions, services or any related attributes, or credentials is expressly prohibited from making any implicit or explicit statements to the effect that they have or provide any form of FiXs-Certified solutions, services, credentials or attributes thereof.

For purposes of clarity, maintaining a membership in the Federation DOES NOT entitle any organization or company to assert or imply in any manner that they are, have been, or provide anything certified, authorized, prepared under the auspices of, or in accordance with the Federation or FiXs, nor does membership in and of itself provide any form of endorsement by the Federation or FiXs.

Article III. Brand Mark and Trademark Uses

Increasing customer and market awareness of the Federation, FiXs, and or related offerings requires absolute consistency in all forms of print and electronic media; to include descriptions in all service offerings, proposals, marketing materials, and signage on products and service components. It is also imperative that any oral communications

of these forms of reference are used consistent with the same usage in other forms of expression.

1. Use of FiXs Brand Names, Marks and Trademarks – The use of FiXs Brand Names, Marks, and Trademarks must appear prominently, consistently, legibly, and accurately and match in color when possible and at the size, color, and frequency parity when described in all forms of documents or text, in written and electronic format. When used as signage, as an “emblem” or “logo”, or on other artifacts, or as part or a service being provided or advertised, FiXs Brand Marks and Trademarks must appear prominently, consistently, legibly, and accurately and match in color when possible and at the size, color, and frequency parity.
2. Use of the FiXs Brand Marks and Trademarks with Other Marks – When used with other brand marks, the FiXs Brand Marks and Trademarks must appear prominently, consistently, legibly, and accurately and match in color when possible and at the size, color, and frequency parity comparable to FiXs participation or representation in the specific use.
3. Depicting FiXs Brand Names or Trademarks on Identity Cards and/or Credentials – All “actual” or “sample” identity cards or credentials must display the entire Brand Mark or Trademark in a clearly legible manner and at least at the same size, color, and frequency parity with other systems or network- related brand marks or trademarks shown on the card or credential.
4. Use of Correct and Consistent Language – The use of the correct and consistent terminology when referring to FiXs, FiXs Names or Trademarks throughout and in all forms of communications is an essential aspect of this Policy.

Article IV. Using Our Brand Names and Trademark(s)

The full name(s) of the Federation for Identity and Cross-Credentialing Systems, Inc. must be used at least once in all communications that refer to the Federation, FiXs, membership in FiXs, or FiXs-certified offerings, products and/or services. It is desirable that this depiction be used at the point of “first use” of any reference to the Federation.

1. Using Uppercase and Lowercase Letters – When using the full name of the Federation, or the Federation for Identity and Cross-Credentialing Systems, Inc., the trademark should be distinguished from surrounding text by at least using Initial Capital Letters, such that the “F”, “I”, “C”, “C”, “S”, and “I” always appear in uppercase. Usage of the full name of the Federation may also be portrayed in ALL CAPITAL LETTERS; **Bold Letters**, *Italic Letters*, “In Quotes”, or in stylized form.

When using the abbreviated form of reference to the Federation, or “FiXs”, the mark should be distinguished from surrounding text by at least Capital Letters for the “F” and the “X” with the other letters, “i” and “s” in lowercase. Usage of the term FiXs may also

be portrayed on ALL CAPITAL LETTERS; **Bold Letters**, *Italic Letters*, “In Quotes”, or in stylized form.

The term “and” or the symbol “&” may be used interchangeably in referring to the full name of the Federation.

2. Using Brand Names or Trademarks as Adjectives – The term “FiXs” may be used as an adjective, as in “FiXs-Certified Credential”, or “FiXs-Certified Solution Provider”, “FiXs-Service Provider” or other such form of adjectival reference. At a minimum, the Brand Name(s) or Trademark(s) must be used as adjectives in their first or most prominent mention subsequent to any use in the title, headline or cover page of any communication.
3. Usage of the Trademark Symbols – The “®” and/or “™” trademark symbols, or their local law equivalents, always should appear after the first or most prominent use of the FiXs Brand name(s)
4. Usage with Other Brand Names or “marks” – In all communications the FiXs Brand Names and Trademarks always must be presented with prominence and frequency equal to that of all other system or network related brand names, trademarks or “marks”.
5. Brand Name Translation – The Brand Names and Trademarks of the Federation may appear only in English and not be translated into other languages nor appear in another alphabet.

Article V. Using Correct Language

Using correct and consistent language in all communications is essential for the effectiveness of this policy.

1. Referring to the FiXs Network – All references to the network deployed and operated by FiXs must be referred to as the “FiXs Network”
2. Referring to FiXs Solutions, Services, Processes or Technologies – All references to solutions, services, processes or technologies that are related solely to the instantiation of FiXs intellectual property shall be used with, and as a prefix to, the name of the service or feature being utilized or deployed. The applicable trademark symbols must be used with such usage. Where a authorized service provider may be providing solutions, services, processes or technologies that are utilizing any FiXs intellectual property, the provider may apply its’ own branding applicable to the circumstances; however, clear and legible acknowledgement must be provided and accompanying marks provided indicating that an underlying component is FiXs intellectual property. (i.e. such as the “powered by Intel” mark prevalent in industry).

Article VI. Use in Advertising, Proposals, and Other Forms of Print or Electronic Media

This Policy shall be consistently applied and adhered to in any and all proposals, marketing collateral and brochures, presentation materials, contractual documents, advertisements, informational documents and any other formats in any form, whether printed or electronic, to include on or over the Internet, as well as in oral communications as applicable.

Article VII. Use at the Point of Interaction

A card or credential holder's first visual indication of the availability to use or have FiXs-Certified Credentials utilized may be as exterior signage, but it is also important to display such signage at the point of interaction as well as on any enrollment device or authentication device, as applicable.

Article VIII. Use in Depicting Cards or Card Communications

When depicting the FiXs credential or card in visual format or on the actual card, the card "format" or "topology" shall be consistent with the technical specification requirements set forth for the card "type", security level, or other attributes required by the usage case and consistent with the specifications set forth by the Federation. In all cases, the FiXs trademark shall be present in a clearly visible manner on one or more sides of any such card. In cases where the only one side is depicted in visual format or representation (i.e. in print), the FiXs trademark shall be present in a clearly visible manner on the representative card.

Article IX. Use on Signage

When displaying the FiXs Brand Mark or Trademark, the "mark" shall be displayed horizontally and in an easily recognizable manner.

Article X. Brand and Trademark Specifications

Brand marks are generally used to represent the brands on cards, products, and services and to promote the brand through advertising and marketing.

The current Brand and Trademarks of the Federation are:

"Federation for Identity and Cross-Credentialing Systems, Inc. ®";

And,

"FiXs®",

And,



The Brand Marks and Trademarks are reflected visually on the FiXs website, on all FiXs documents, and are available from the FiXs Administrative Staff at the request of a FiXs member in “good standing”.

FiXs Brand Marks may be provided to non-members for specific uses; such as marketing, advertising, trade events, publications, and other such uses on a case-by-case basis at the sole and explicit authorization of an officer of the Federation.

Article XI. Specific Examples of “Do’s” and “Don’ts”

Provided below are examples of “Do’s” and “Don’ts” as it relates to Brand Names and Trademarks.

“Do’s” Include:

1. Distinguish trademarks from surrounding text by at least using:

Initial Capital Letters
ALL CAPITAL LETTERS

Bold Letters

Italic Letters

“In Quotes”

In stylized form or logo

2. Use proper trademark form and spelling

3. Use trademarks with the generic product and/or services descriptor, e.g.:

FiXs Network

FiXs Certified Credentials

FiXs Authentication Station

FiXs Credential Issuer, etc.

“Don’ts” Include:

1. Don’t hide trademarks within other text,

E.g. “Use the fixs network to authenticate fixs credential holders”

2. Don’t purposely misspell trademarks,

E.g. FIxS
F I X S
Fed. For ID X-Credentialing Sys.

3. Don’t use alone as a generic product name,

E.g. FIXS

4. Don't use as a noun,

E.g. Use FIXS to gain access

5. Don't use a plural form of trademark,

E.g. FIXSs
FIXSes

6. Don't make trademarks possessive,

E.g. FIXS's
FIXS'
Federation for Identity and Cross-Credentialing Systems'

7. Don't use trademarks as verbs,

E.g. I am/will FIXSing your identity

8. Don't use alternative spellings or acronyms,

E.g. FICS
FICCS

Article XII. Violations of this Policy and Enforcement

Adherence to and compliance with this Policy is of significant imperative to promote and protect the market position of the Federation as well as the value of FiXs intellectual property and assets. Maintaining and ensuring compliance with this Policy is a fundamental responsibility of executing the business plan and day-to-day operation of the Federation. It is the intention of this Policy to actively manage and enforce the provisions herein.

Protection, defense, and enforcement measures for violations of this Policy shall be considered through all practical and legal means, to include all legal and financial remedies as well as injunctive relief.

Article XIII. Filing of Applications for Trademark, Patents and Other Legal Protections

A fundamental component of executing the business plan and the successful business operations of the Federation shall entail applying for and obtaining, as possible, the

relevant trademark, patent and other legal protections for Federation property and assets, as applicable.

12.0 DISASTER RECOVERY

The purpose of this Disaster Recovery Policy is to set forth the measures that have been made or will be activated in the event of a “disaster”, which is essentially any event, man-made or naturally incurring, that may attempt to destroy or otherwise impair the continuity of operations the Federation and the FiXs Network. This policy addresses the personnel, processes, technological, and operational aspects of the Federation.

Personnel (Officer) Continuity

Consistent with the Bylaws of the Federation, the Vice President of the Federation will act in the absence or unavailability of the President in the event of a “disaster”. The Corporate Secretary and the Treasurer of the Federation shall maintain the ability to serve in the capacity of the other in the event of a disaster and the incapacitation or unavailability of the other.

The organizational delegation of authority shall flow from the President, to the Vice President, to the Secretary, then to the Treasurer of the Federation. Should all of the officers be in some manner incapacitated, a majority of the then available Founding Members shall appoint designated successors to such officers until such time that the “disaster” situation is stabilized, whereupon the full Board of Directors can attain a quorum and appoint permanent replacements consistent with the Bylaws.

Organizational and Membership Continuity

The Federation will maintain complete and current documentation of all governance policies, to include: without limitation, the Trust Model; Operating Rules; Implementation Guidelines; Technical Specifications; contact lists of all officers, members, Federation service providers and contractors, and government counterparts and sponsors; contracts; licenses; financial/tax information and records; membership list including membership level and status; and all current records of the Federation. A duplicate copy in electronic format (i.e. CD, thumb drive, etc.) of such records will be provided to each current officer of the Federation for safeguarding and use in the case of a disaster situation. The “safeguarding” officer shall appropriately protect and not access, distribute, or otherwise allow the “opening” of such records except in the case of a bona fide disaster as determined by the then available Founding Members of the Federation.

Technical and Operational Continuity

The contractor providing laboratory management services for the Federation will provide, as determined by the Federation, the “failover” site for maintaining continuity of operations of the FiXs Network components and continuity of operations.

The laboratory management services contractor shall also maintain a current copy of all versions of the software code, technical specification, documentation, and other assets to

provide continuity of the core FiXs Network components such as the FiXs TGB and interface specifications. Such assets shall only be disclosed as directed by the acting officer then in charge of the Federation in the event of a disaster.

The service providers maintaining the respective data stores of the federated credential holder personal information data sets shall have their own Disaster Recovery Policy that shall be implemented to maintain continuity of operations in the event of a disaster affecting their ongoing operations. This policy and its' ability to be deployed in a timely manner are subject to periodic review and audit by the Federation.

The tertiary components of the FiXs Network, such as the authentication station providers; credential issuers, investigative services, etc. shall implement disaster recovery plans consistent with the service requirements of their respective service clients.

Periodic Disaster Recovery Plan Exercise

This Disaster Recovery Plan will undergo a “test exercise” of its basic tenants and ability to respond in case of a disaster situation on no less than an annual basis. The findings of such exercise shall be reported to the Board of Directors upon compilation of such findings as part of its’ routine operational forum.

Violations of this Policy

Any violations of this Policy, to include but not limited to the violation of ensuring proper protection and non-disclosure of “safeguarded” information, shall result in the termination of offending parties’ relationship with the Federation, at the discretion of the President, in addition to any other remedies at law, regulation, or otherwise.

Note: For FiXs Definitions/Terminology, see [Master Glossary of Terms/Definitions](#)



The Federation for Identity and
Cross-Credentialing Systems®

FiXS® Trust Model
Version 3.0

September 1, 2010

www.fixs.org

Copyright 2010 by the Federation for Identity and Cross-Credentialing Systems, Inc.®

All Rights Reserved

Printed in the United States of America

10400 Eaton Place, Suite 500A

Fairfax, VA 22030

(703) 591-9255

Table of Contents

1.0	GENERAL REQUIREMENTS AND DEFINITIONS	3
2.0	FIXS' OBJECTIVES	4
3.0	THE FIXS CHAIN OF TRUST.....	6
4.0	FIXS' SEVEN DISTINCT PROCESSES	8
5.0	BACKGROUND ON FEDERATED TRUST.....	10
	REFERENCES	12

1.0 General Requirements and Definitions

Trust in the security of personal identity information exchanged over the Internet and other networks are vital for the effective operation of all organizations, both commercial and public sector. Trust is particularly important when the intent of a transaction is to grant physical or logical access privileges to appropriately authorized personnel. This trust can only be accomplished through the establishment and operations of a strong security profile, and Trust Model, from both a governance and operational perspective.

Organizations must address the issues of user identity, authentication, confidentiality, privacy, and integrity of data accessed and/or transferred, and the ability to hold transacting parties accountable for their actions in order to establish this security profile. A Trust Model is the foundation for establishing this profile because it establishes the framework, operating rules, and a transaction model that allows for identity credentials to be trusted across organizations.

The purpose of this document is to describe the manner in which “trust”, or the “Trust Model”, is established across the Federation for Identity and Cross-Credentialing Systems, Inc. ®(FiXs) Network. It also addresses the roles and responsibilities that FiXs Member Organizations and Subscribing Parties will assume when participating in the operations of the FiXs Network.

The FiXs Network provides a highly-scalable, secure, auditable solution set, whereby FiXs Member Organizations can authenticate **FiXs-Certified Credentials** (also known as “FiXs Credentials”) issued to users from participating organizations or Subscribers. The FiXs Network provides data from identity credentials that are compatible, or “aligned”, with the precepts of HSPD-12 and PIV-I and utilize FIPS 201 standards., as well as lower-level credentials, to various authentication nodes that can then be used to authenticate the identity of employees, contract personnel, and various other authorized credential holders or “users”. Additional data authentication can also be transmitted across the Network so that local decision makers can grant physical or logical access privileges. The FiXs Network is interoperable between member organizations and with other credentialing networks (i.e. the Department of Defense Cross-Credentialing Identification System Network or “DCCIS”). Trust in the FiXs Network is built on a common set of rules, responsibilities, and contractual obligations for all participating organizations, which are set forth in the FiXs Foundational Documents (see Definitions for precise meaning of capitalized terms).

FiXs does not issue credentials directly. FiXs establishes the rules, specifications, policies, and procedures that authorized or “approved” issuing Member Organizations must use in issuing FiXs-Certified Credentials. These prescribed foundational agreements and operating rules provide a consistent and reliable level of “trust” that may be presumed across participating entities. FiXs does not participate in determining what privileges should be granted to any user or set of users. Privileges are the province of the facility or system “owner”. However, FiXs does provide a solution for organizations with role-based work environments where employees and authorized agents are afforded privileges consistent with the organization’s own unique requirements. These FiXs Certified Credentials can then be authenticated and managed over a trusted network by other Member Organizations based on this Trust Model. FiXs-

Certified Credentials shall carry the FiXs logo/mark for “branding” and/or recognition purposes consistent with FiXs Policy to support ready identity authentication operations. .

An organization decides what role it wishes to participate in FiXs either in an active membership capacity or as a Subscriber. An organization may desire to just “subscribe” to the FiXs Network, and thus be a “Subscriber Member”. In this capacity they are assigned a unique organization code and then sponsor their employees or individual users to be issued credentials for identity authentication across the Network. Other firms/organizations may desire to join as a full or associate member engaging in the governance and policy promulgation of the Federation. Some members may opt to participate as a “Credential Issuer” whereby they issue and manage credentials of their own employees as well as issue to users from other firms as part of a service that they may choose to offer.

Prior to joining the FiXs Network in any capacity, the organization must be vetted before it is accepted into the FiXs membership or allowed to Subscribe to use FiXs-Certified Credentials. This vetting process provides an assessment of the organization’s validity and corporate standing to be a “trusted organization,” which includes the vetting of the organization’s official. If the organization desires to sponsor individuals to be issued FiXs Certified Credentials, after signing the appropriate agreements they will be designated, , as the **“Primary Trusted Organization”** standing behind those individuals (credentials). These Primary Trusted Organizations are then assigned an Organizational Code which is tied to the FiXs-Certified Credentials issued to the individual(s) they have sponsored.

Once the Primary Trusted Organization is established, the individuals sponsored by that organization, undergoes the applicable level of identity verification, enrollment, and credential issuance for the trust level of credential requested.

All participating organizations are required to, sign and abide by the “Terms of Use” for credentials, adhere to the operating principles and policies of the Federation, and maintain their membership in the Federation in “Good Standing” as may be applicable.

2.0 FiXs Trust Model Objectives

The specific objectives of FiXs are to:

1. Establish the appropriate and reliable level of trust and confidence in the identification, vetting, proofing, and enrollment of every organization that participates in the FiXs Network, as well as the sponsored individuals being, issued FiXs-Certified Credentials;
2. Manage the FiXs-Certified Credentials life-cycle process in accordance with all applicable issuance, security, privacy and other applicable rules and/or legislation (i.e., state, federal or local legislation; Department of Defense Policies or Directives; or customer installation or facility policies);
3. Facilitate the secure electronic authentication of FiXs-Certified Credentials, and authentication of selected identity information, across disparate domains, in an interoperable manner that maintains the highest levels of security and privacy of data; and,

4. Provide data to a Trusted Adjudicator/Agent (i.e. gate guard or building monitor, web site or application owner/monitor) who can reliably authenticate the identity of an individual with such confidence that they can render a decision regarding the exercise of privileges, whether physical access, logical access or other type of appropriate access in accordance with the policies, rules and/or legislation that might govern that adjudicator's domain of responsibility.

Overall, FiXs does not set privileges to grant or deny any type of physical or logical access privileges. FiXs does provide the trusted infrastructure (logical, physical, and operational) which all participating members use in providing a high confidence level in the true identity of an individual who is presented for authentication. The results from that determination can then be used for the provisioning of privileges consistent with established policies or the participating organization.

FiXs has successfully worked with the U. S. Department of Defense (DoD) in establishing a mutually-trusted, interoperable community wherein DoD contractors, vendors, and trading partners are able to use approved and accepted identity credentials to authenticate data to authenticate an individual's identity. Currently, FiXs is the only organization established to inter-operate a cross-credentialing infrastructure and systems with the DoD.

FiXs and the Defense Manpower Data Center (DMDC) have signed a formal Memorandum of Understanding attesting to maintaining this trusted relationship with the DoD. FiXs is committed to including other partners throughout the Federal Government, within the first responder community, with other public and private sector organization and commercial entities that seek a scalable, rules-based, interoperable identity verification and authentication capabilities.

The FiXs operating model along with the foundational principles is depicted in Figure 1, below. In all cases, the personal identifying information of an individual credential holder is securely maintained in, and at, the single FiXs-certified location designated by the sponsoring party of the credential holder. The data may not be captured and reused for any purpose other than the authentication instance in question.

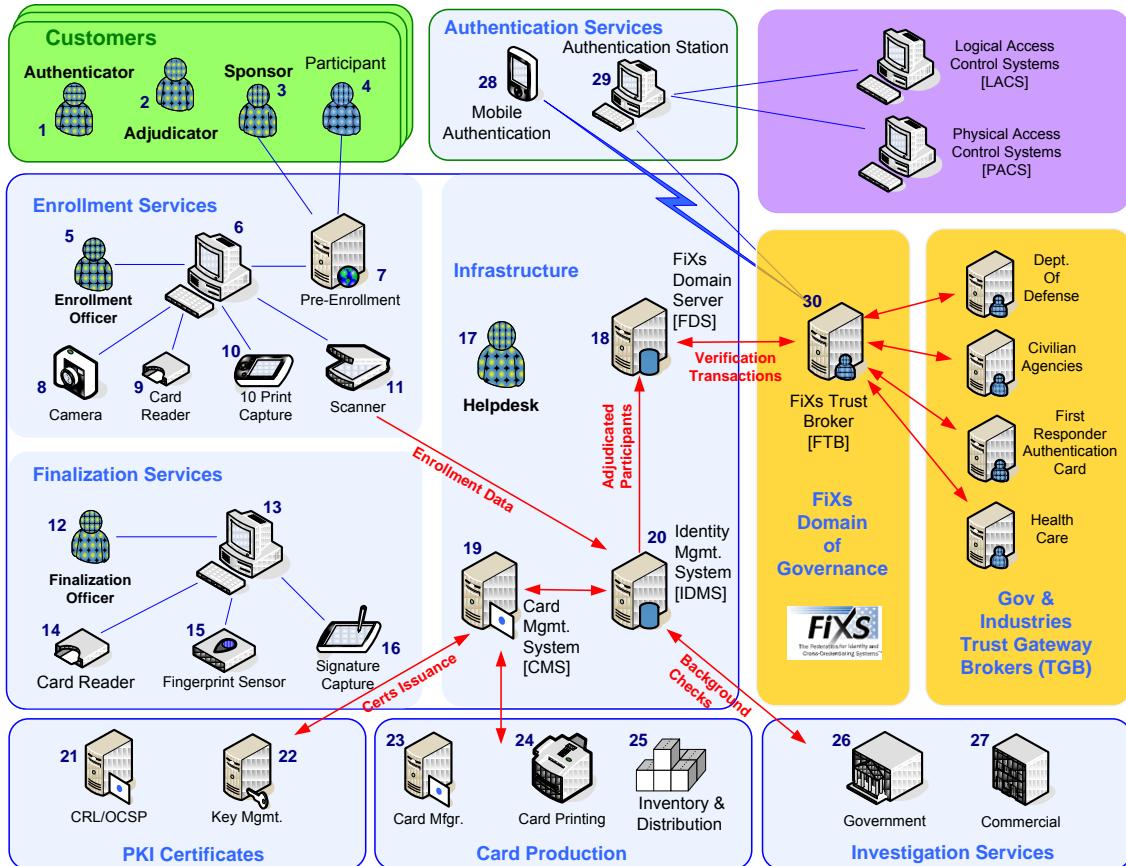


Figure 1 – FiXs Trust Model, Showing Multi-Party Trust with DoD and Various Other Member Organizations

3.0 The FiXs Chain of Trust

The “Chain of Trust” in the FiXs-Certified Credential life cycle and Network begins with two inter-related components. The first is a trusted organization and the second is a trusted individual identity. When the two components are linked, an individual’s identity can be authenticated and managed over the FiXs Network by other participating Member Organizations. Once issued, a FiXs-Certified Credential can then be used across the FiXs Network in various role-based work place environments to provision privileges consistent with the objectives and unique requirements of that member organization.

A Primary Trust Organization (“PTO”), or Sponsoring Party, initiates this Chain of Trust by agreeing to attest to the need for such a credential; the validity of their employees’ identity; and accepting responsibility for the acts and omissions of its employees or other individuals they may sponsor for obtaining FiXs-Certified Credentials to be used over the FiXs Network. In order to become a PTO and prior to the issuance of FiXs Certified Credentials to its employees, the PTO must provide sufficient information on the organization and legal representative to be vetted by a FiXs Member Organization approved to do the vetting. This vetting shall be conducted in accordance with the FiXs Operating Rules and Implementation Guidelines in order to establish a consistent and reliable measure of authenticity and trust worthiness to interact with other FiXs Member Organizations or Subscribing Member Parties.

It is possible that an individual employee of one organization may also belong to another organization(s) (i.e. volunteer groups, social organizations, second employers, etc.) who may also be a member or Subscriber to the FiXs Network. In such cases, the individual and each organization must mutually agree on which organization shall be designated as the PTO for the applicable user on the FiXs Network. After that primary designation, secondary or tertiary credentials can be tied, or linked back, to the primary credential designation, provided that the issuing organizations adhere to FiXs issuing and revocation rules.

The PTO is also responsible for initiating the process to revoke a FiXs Credential based upon the applicable credential revocation requirements. If the employee or sponsored user leaves the organization, or no longer requires a FiXs Credential, the FiXs Credential shall immediately be revoked and the Chain of Trust with the individual shall be broken. The individual may move to another organization to establish a new Chain of Trust or they may later re-establish it within the same organization, if required. At that time a new FiXs-Certified Credential will be issued.

As shown in Figure 2 below, the foundation for the Chain of Trust is built on key building blocks. Some of these building blocks are written documents that outline the FiXs Trust Model, the organization's policies, rules or technical specifications. Others are physical assets, such as the physical infrastructure of the network and endpoints, and still others are processes, like the implementation procedures and standards involved in making the system operational.

In summary, PTOs, through their adherence to this Trust Model and other Foundational Documents form the critical link upon which individual FiXs-Certified Credentials may be issued, authenticated, and, ultimately, trusted.

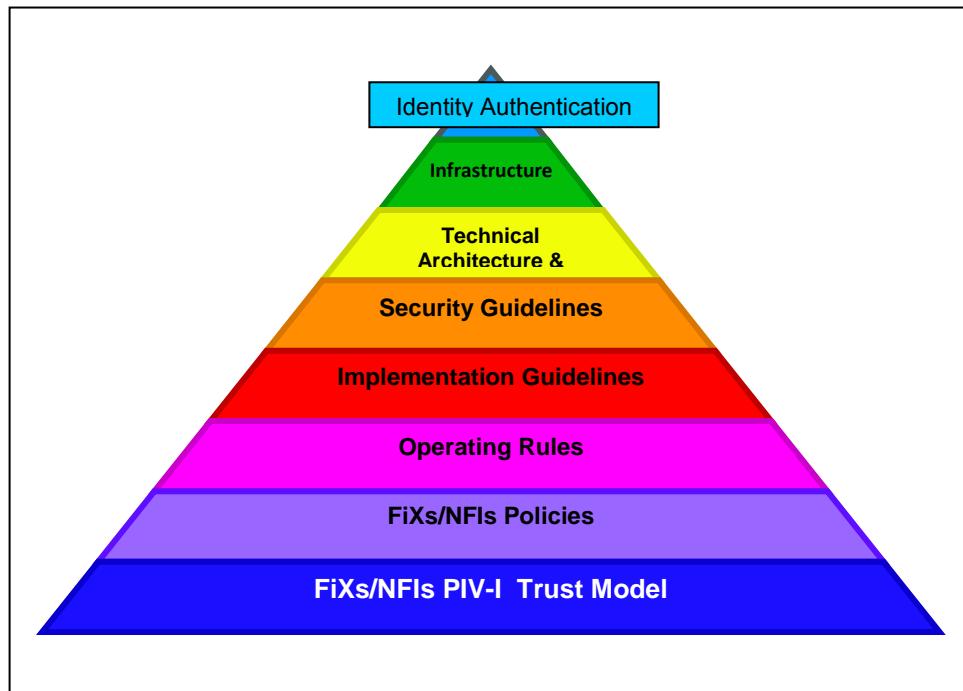


Figure 2: Trust Model, Rules, Policies, Guidelines and the Physical Infrastructure Forming the Foundation for the FiXs Chain of Trust

Summary of Roles and Responsibilities of Primary Trusted Organizations:

- Must be vetted by a FiXs-Approved Organization in accordance with the FiXs Operating Rules.
- Assert the need that its employees, contractual agents, or other users be issued trusted credentials that allow for authentication of Credentials across the FiXs Network.
- Sponsor and attest its employees and/or other users to be issued Credentials
- Abide by the Terms of Use as provided for in the FiXs Policy and Foundational Documents and Trust Model.
- Adhere to the 8-step credential management life-cycle process outlined in Figure 3 of this document.
- Indemnify FiXs and other FiXs Member Organizations, including Member Organizations that may provide services in support of the FiXs, for the acts or omissions of its employees or sponsored users.

4.0 FiXs' Eight Distinct Processes

There are seven distinct processes that support the issuance and use of FiXs Certified Credentials. These key processes are: **Validating Need; Verifying and Vetting Identity; Adjudicating; Enrolling; Issuing; Authenticating; and Revoking**. These processes are integral to the effective operation of the Trust Model.

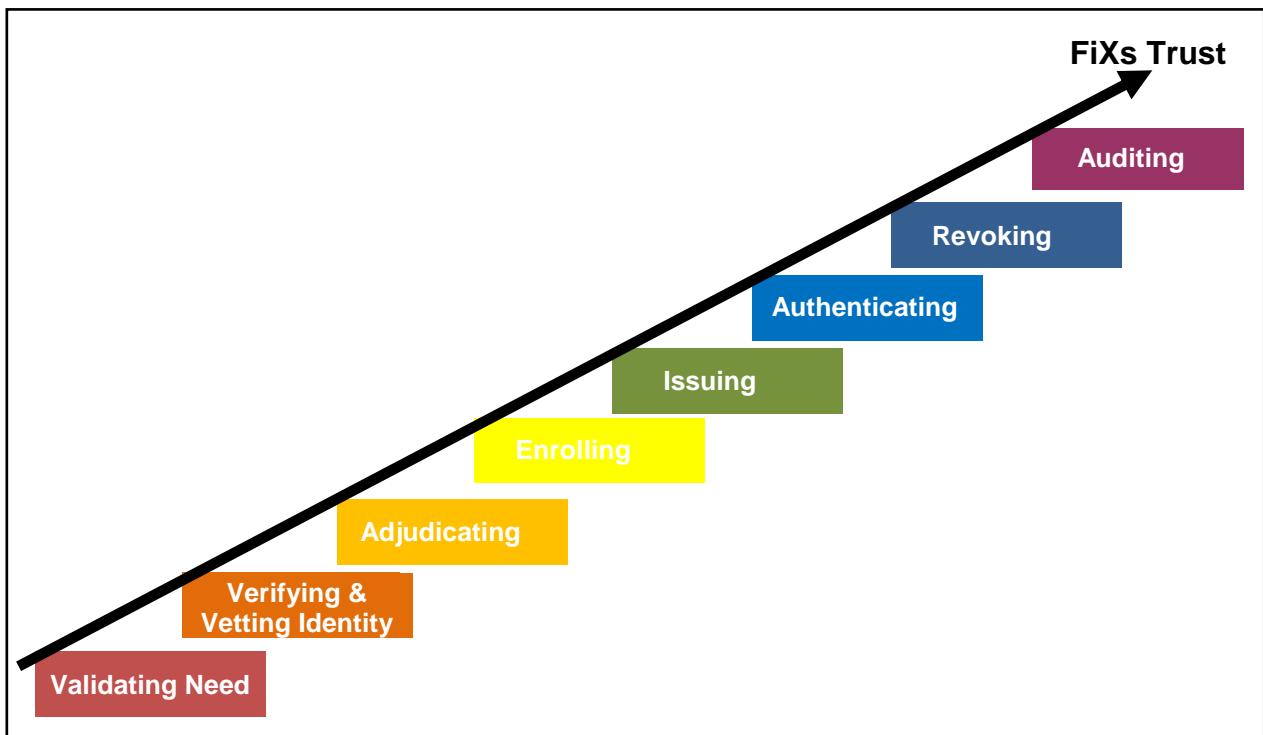


Figure 3– Eight distinct processes of Credential Management

This table provides a high-level description of the individual steps in the management of FiXs Certified Credentials. More detail on each of these steps can be found in FiXs Operating Rules and the FiXs Technical Architecture and Specifications and Implementation Guidelines.

1. Validate Need
A pre-requisite for starting the Credential issuance process is to validate the Organization's need to sponsor their employees for a FiXs Credential. The TPO must submit an application requesting the appropriate vetting as an entity doing, or having a need to do business, with the DoD. Once the organization is accepted then they must attest to their employee's need for a FiXs credential. This written request will be to the FiXs Credential Issuer verifying the Applicant's need for a credential.
2. Verify and Vetting
The FiXs Credential Issuer verifies or "proves" the Applicant's identity and then vets that identity using the process outlined in the FiXs Operating Rules of the FiXs approved organization.
3. Adjudicate
The designated Trusted Adjudicator/Agent determines whether the Applicant may be a participant/user of the Interoperable Network(s) that use data for transacting identity authentications requiring FiXs credentials by being enrolled into a trusted identity Domain Server/database.
4. Enroll
The FiXs Credential Issuer enrolls the Applicant (now a Participant) in the trusted database using the approved documentation and biometric data. This process makes the Participant's record of credentials available for retrieval by any Relying Party for Authentication whenever a credential is presented for authentication.
5. Issue
The FiXs Credential Issuer issues the Participant a Valid FiXs Identifier(s) (following the FiXs technical specifications) that can be used to access the Participant's credentials.
6. Authenticate
A Relying Party transmits an Authentication Inquiry to a trusted FiXs Domain Server/database to validate identity data presented.
7. Revoke
FiXs provides for the timely revocation of identity credentials of a Participant once the validated need lapses or is terminated. Timely revocation is critical to system security and relying party trust.
8. Audit
FiXs provides a compliance audit mechanism to ensure that the FiXs requirements are being implemented and enforced at the issuer [PKI and CMS], network gateways, and relying party environments.
All Authorized FiXs providers shall undergo a Security Certification and Accreditation (C&A), or commercial equivalent managed under a legal governance structure, in accordance with the Federal Information Security Management Act (FISMA) of the E-Government Act of 2002, and associated NIST standards, regulations, and guidelines, and DoD IT Security policies, procedures, and guidelines, as a condition of obtaining and retaining approval to operate as an Authorized FiXs provider. The purpose of the C&A process shall be to verify that the Authorized FiXs provider has in place and follows a system that assures that the quality of its services conforms to the FiXs requirements. Re-accreditation should occur after any significant change in the system, but at least every three years. It should be done more often where there is a high risk and potential magnitude of harm. This requirement does not replace any additional annual auditing requirements stipulated by the PKI(s) approved under the FiXs architecture.

5.0 Background on Federated Trust

It is important to understand what is meant by “trust”, especially in the context of FiXs as it relates to interoperability with other organizations, such as the Department of Defense (DoD), other governmental organizations, and commercial enterprises. FiXs has chosen to adopt the **Federated Model of Trust** as the basis for identity management. This model of trust was chosen for several reasons, namely:

1. The nature of its affiliations with members and advisors. Members commit to a contractual obligation whereby they agree to comply with the FiXs Foundational Documents and operating principles.
2. The DoD, acting on its own authority and guidance, has also independently chosen to collaborate with FiXs and is participating in FiXs in the role of an “advisor”.
3. Each member retains control over the location and security of its own personnel data as well as that of any subscribing parties that it may contract with for credential issuance purposes.
4. Employees and sponsored agents are vetted and only enrolled into a single FiXs domain as designated by the sponsor/subscribing party
5. There is no central database of identity credential information.
6. FiXs Members and Subscribers are bound by a multi-party contract through formal agreement or acceptance of Terms of Use.

Additionally, a variety of methods can be employed to establish trust at different levels of assurance among Subscribing parties. The appropriate level of assurance is determined by the underlying technology as well as the Operating Rules, Implementation Guidelines, and the overriding business service requirement.

The X.509 specification, a widely used standard for defining digital certificates provides a suitable clarification on trust, stating that “*Entity ‘A’ trusts entity ‘B’ when ‘A’ assumes that ‘B’ will behave exactly as ‘A’ expects it to behave.*” According to this description, trust deals with assumptions, expectations and behavior. This implies that trust cannot be measured quantitatively and there is a certain amount of risk associated with resulting trust. The FiXs Trust Model addresses this risk by establishing how trust is established and enforced throughout the lifecycle of a trusted FiXs Credential.

In order to clarify the application of a Federated Trust Model, it seems appropriate to consider other instantiations of a Trust Model. The Liberty Alliance Project¹ offers a well-recognized approach, which can be used as an objective basis for comparison.

Historically, the Liberty Alliance defined “**Community Trust**” as follows:

“**Community Trust** applies when the business trust between a pair of entities is derived from their enrollment in a common authentication infrastructure and acceptance of its practices, without reliance on other business agreement paths.

¹ The Liberty Alliance (Project) is comprised of over 100 member companies representing a wide variety of industries and over a billion customers, with operations all over the globe. Each of the member companies either owns or operates large communities of interest or is the developer of core technology that can enable a federation of online communities. The role of the Liberty Alliance Project is to support the development, deployment and evolution of an open, interoperable standard for federated network identity. For more information on the Liberty Alliance, please visit their web site at <http://www.projectliberty.org>

As such, the entities' mutual trust in a business sense is based on their membership in a community constructed and linked for authentication purposes.²

In the Community Trust model, an *organization* (e.g., an industry consortium or a community) sponsors, endorses, or adopts one or more trust establishment services to provide and manage the credentials needed by entities to create and maintain authentication trust among them. (In the FiXs Trust Model, the FiXs Federation could be seen as the "organization.") The service(s) could be operated by the sponsoring organization, or could be provided by an independent service delivery organization. In Community Trust, some level of business trust, although not provided by either direct or brokered business agreements, can be derived from participation in a shared authentication infrastructure (for example PKI, Kerberos, or PGP "webs of trust"). The assumption is that the authentication infrastructure will, in addition to allowing entities to be identified, further identify them as belonging to some community. Different options imply different degrees of organizational involvement and, potentially, of organizational liability. Liberty's Community Trust model presumes neither direct nor indirect business agreement paths between communicating entities.

In the FiXs Trust Model, members join FiXs for their unique business reasons, not necessarily because they share a common cryptographic trust establishment infrastructure. The concept of "membership in a community constructed and linked for authentication purposes" applies only to the extent that members are interested in trustfully authenticating identity credentials for the purpose of authoritatively proving identities.

The Liberty Alliance Project also defined "**Brokered Trust**" as follows:

"Brokered Trust describes the case where two entities do not have direct business agreements with each other, but do have agreements with one or more intermediaries so as to enable a business trust path to be constructed between the entities. The intermediary brokers operate as active entities, and are invoked dynamically via protocol facilities when new paths are to be established."

In Liberty's Brokered Trust model, active intermediaries are invoked and involved when federation and/or authentication transactions span multiple administrative domains. These approaches constrain the set of components that must be involved in inter-domain trust management, but require the use of additional protocol facilities. Further, Brokered Trust models depend on availability of appropriate intermediaries in order to construct a path to federate a user's relationship and/or to authenticate a particular session.

As an example situation where Brokered Trust may be applicable, Member A receives a request to be processed from Member B, with which it shares no prior formal business relationship. The underlying Trust Model must decide whether to trust Member A's original request and Member B's subsequent response. In this situation, overall trust is composed of the combination of business trust, based on direct/indirect business agreements, and authentication trust, which is based on the underlying direct/indirect authentication infrastructure. To put it simply, there is no direct business trust in a Liberty Alliance Brokered Trust model. Conversely, in the FIXS Trust Model all participating members have a formal relationship through acknowledgement and agreement to the "Terms of Use" for such credentials.

² Liberty Trust Model Guidelines: <http://www.oasis-open.org/committees/download.php/6158/ssct-saml-trustmodels-2.0-draft-01.pdf>

Note: For FiXs Definitions/Terminology, see [Master Glossary of Terms/Definitions](#)

References

Industry and Academia

- ITU-T Recommendation X.509, Public-Key and Attribute Certificate Frameworks, International Telecommunications Union -Telecommunications Standardization Sector, March 2000.
- Housley, R., eds. (April 2002). "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," RFC 3280, The Internet Engineering Task Force <http://www.rfceditor.org/rfc/rfc3280.txt>
- [X.509] "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks," ITU-T (2000). ITU-T Recommendation X.509 (2000) | ISO/IEC 9594-8:2000,
- FEGC Report by the DoD/Industry working Group for Strong Authentication and Secure Communications, "**An On-Going Assessment of Government Information Assurance, e-Business Policy, and Implementation in a Changing 'Trust' Environment**", 3 May 2002.
- FEGC Report prepared for DMDC and DoD, "**Developing an Interoperability Demonstration Pilot for the Defense Cross-credentialing Identification System (DCIS)**", version 4.1, dated 6 March 2003.
- Liberty Alliance Project, "**Liberty Alliance Trust Models**", draft version 1.0-14, 13 April 2003.

DoD Common Access Card (CAC) Program

- U.S. Department of Defense, Memorandum from Deputy Secretary of Defense – John J. Hamre, "**Smart Card Adoption and Implementation**", 10 November 1999.
- U.S. Department of Defense, Memorandum from DoD CIO and USD (P&R), "**Common Access Card (CAC)**", 16 January 2001
- U.S. Department of Defense, Department of Defense DIRECTIVE – ASD (C3I)/DoD CIO, "**Smart Card Technology**".
- U.S. Department of Defense, Memorandum from Connie K. DeWitte – Deputy Assistant Secretary of the Navy (Safety), **DODPUB Change- 5200.8R DOD Physical Security Program**", 2 June 2003.
- Memorandum of Understanding between The Federation for Identity and Cross Credentialing Systems and Defense Manpower Data Center signed January 10, 2006
- Letter from U.S. Department of Defense, Defense Manpower Data Center, acceptance of Card Holder Unique Identifier (CHUID) solution for assigning unique organizational codes to non-Federal government entities dated 6 December, 2007
- Defense Cross Credentialing Identification System (DCCIS) Initial Operating Capability (IOC) letter dated 16 July, 2007
- Memorandum of Understanding between The Federation for Identity and Cross Credentialing Systems and Defense Manpower Data Center signed February 12, 2009
- 2010 FiXs Notification on Credential Usage with US NORTHCOM (May, 2010)

- DTM 09-12

DoD PKI Program

- U.S. Department of Defense, "**Target Public Key Infrastructure User Requirements**", 29 February 2000.
- U.S. Department of Defense, "**Class 3 PKI Public Key-Enabled Application Requirements**", version 1.0, 13 July 2000.
- U.S. Department of Defense, "**Class 3 PKI Interface Specifications**", version 1.2, 10 August 2000.
- U.S. Department of Defense, "**PKI Implementation Plan**", version 3.1, 18 December 2000.
- U.S. Department of Defense, **Public Key Infrastructure (PKI) Policy Update**", 21 May 2002.
- U.S. Department of Defense, **Certificate Policy for External Certificate Authorities**", version 1.10, 14 November 2002.
- U.S. Department of Defense, "**Public Key Infrastructure Roadmap**", 13 June 2003.
- U.S. Department of Defense, "**X.509 Certificate Policy**", version 10, 2 Mar 2009

Federal Identity Management

- FIPS 201-1: Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006
- HSPD-12 Policy for a Common Identification Standard for Federal Employees and Contractors, 27 August 2004
- NIST SP 800-63: Electronic Authentication Guideline, April 2006
- NIST SP 800-76-1: Biometric Data Specification for Personal Identity Verification, January 2007
- NIST SP 800-79-1: Guidelines for the Accreditation of Personal Identity (PIV) Verification Card Issuers, June 2008
- NIST SP 800-116: A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS), November 2008
- NIST SP 800-73: Interfaces for Personal Identity Verification (4 Parts), February 2010



The Federation for Identity and
Cross-Credentialing Systems®

FiXS® IMPLEMENTATION GUIDELINES

VERSION 3.1
JANUARY 31, 2008

www.fixs.org

Copyright 2007 by the Federation for Identity and Cross-Credentialing Systems, Inc.

All Rights Reserved

Printed in the United States of America

10400 Eaton Place, Suite 500A

Fairfax, VA 22030

(703) 591-9255

Table of Contents

1 BACKGROUND	3
2 FIXS ASSURANCE LEVELS	6
2.1 OVERVIEW	6
2.2 IDENTITY MANAGEMENT METHODOLOGIES.....	6
2.3 IMPLEMENTING THE ASSURANCE LEVELS	7
2.4 ASSURANCE LEVEL OVERVIEW.....	7
2.4.1 <i>High Trust Level (Level 4).....</i>	7
2.4.2 <i>Medium High Trust Level (Level 3).....</i>	8
2.4.3 <i>Medium Trust Level (Level 2).....</i>	8
2.4.4 <i>Low Trust Level (level 1).....</i>	9
2.5 FiXs ASSURANCE LEVEL IMPLEMENTATIONS	10
3 FIXS IMPLEMENTATION GUIDELINES.....	13
3.1 HIGH LEVEL (4) -- HSPD-12 COMPATIBLE CREDENTIALS	13
3.1.1 <i>Users.....</i>	13
3.2 HIGH LEVEL (4) --DOD LOGICAL ACCESS CREDENTIALS (LACS)/PHYSICAL ACCESS CREDENTIALS (PACS) CREDENTIAL	15
3.2.1 <i>Users.....</i>	15
3.3 MEDIUM HIGH LEVEL (3)--DoD AND COMMERCIAL USE PACS/LACS CREDENTIAL.....	16
3.3.1 <i>Users.....</i>	16
3.4 MEDIUM HIGH LEVEL (3)--NON-SECURITY CLEARANCE CONTRACTOR AND COMMERCIAL USE CREDENTIAL.....	17
3.4.1 <i>Users.....</i>	18
3.5 MEDIUM HIGH LEVEL (3)--FIRST RESPONDER EMPLOYEES	20
3.5.1 <i>USERS</i>	20
3.6 MEDIUM LEVEL (2)--FIRST RESPONDER EMPLOYEES	22
3.6.1 <i>USERS</i>	22
4 ATTRIBUTE MANAGEMENT FOR MEDIUM HIGH LEVEL (3) ENHANCED FIRST RESPONDER CREDENTIALS.....	25
4.1 ATTRIBUTE MANAGEMENT FOR MEDIUM HIGH LEVEL (3) CLINICAL FIRST RESPONDER CREDENTIALS	25
4.1.1 <i>USERS</i>	25
<u>EXHIBITS & APPENDICES</u>	
TECHNICAL SPECIFICATION FOR CREATING A UNIQUE IDENTIFIER FOR A FIPS 201-ALIGNED FIXS™ CREDENTIAL	28
APPENDIX A - SMART CARD TOPOLOGY REQUIREMENTS	37
APPENDIX B - FIXS BARCODE REQUIREMENTS	43

1 BACKGROUND

The Federation for Identity and Cross-Credentialing Systems (FiXs™) is a not-for-profit 501 c (6) trade association comprised of a coalition of industry and public sector organizations whose objective is to support efforts to develop standards supporting the creation and deployment of a secure interoperable identity cross-credentialing network. These Operating Rules define the rights, responsibilities and liabilities of FiXs Member Organizations and are a part of a larger set of governance documents that lay the foundation for establishing trust in and the operations of the FiXs Network. The other documents, known as the FiXs Foundational Documents, include:

- The Trust Model;
- FiXs Policy;
- Implementation Guidelines;
- The Technical Architecture and Specifications; and
- Security Guidelines.

The FiXs Network provides a highly-scalable, secure, auditable solution set, whereby participating organizations can authenticate FiXs-Certified Credentials (also known as FiXs Credentials) issued to users from other participating organizations or “Subscribers” as well as authenticate the credentials issued by other related organizations (i.e. cross-credential). FiXs relies on a Federated Model of Trust, which is discussed more fully in the FiXs Trust Model. The federated identity model establishes trust between member organizations through the use of agreements, standards and technologies that make an “identity credential” portable across the organizations.

Initially, FiXs established a trusted relationship between certain FiXs Member Organizations and the DoD’s Defense Cross-Credentialing Identification System (DCCIS). The federation enabled participating Department of Defense (DoD) and industry facilities to achieve strong, and interoperable identity verification and authentication of participating contractor/private sector personnel who presented a company-issued trusted credential. Similarly, participating industry locations also recognized the DoD-issued Common Access Card (CAC) and the Defense Biometric Identity System (DBIDS) credential, which required no modifications in order to operate with FiXs and DCCIS. This initial proof-of-concept established the baseline for further expansion.

FiXs, which is the only organization authorized to inter-operate a cross-credentialing system with the U.S. Department of Defense, is deployed in a federated manner to enable other government agencies, first responders, and industry partners to authenticate the identity of individuals who seek access to their physical or logical assets in either the government or commercial environment.

In a federated system each sponsoring organization maintains its own database of enrolled members. Privacy and security are maintained because no identity information is held centrally or maintained in the infrastructure except in the employee’s host organization domain server.

At the present time the Federal Government has defined four recognized “security” levels of credentials and/or trust. It is generally accepted that each level is defined by two distinct processes; one that defines the vetting process that is accomplished prior to a credential being issued; and the second defines the standards for the data, and its placement on the credential, along with the standards and specifications for the credential/card itself. FiXs has chosen to use FIPS 201 compliant smart card specifications for all Levels of Trust. Thus, the main

differentiation between the levels is primarily the vetting process, documentation/verification, and biometric data collected, verified and maintained in the federated data model. FiXs- certified credentials also contain the appropriate data designating under which Level of Trust the credential was issued and classified accordingly.

The current Government sanctioned nomenclature for describing “Levels” is numerical (i.e. 4, 3, 2, 1) and described below. FiXs defines these levels with a non-numeric designation of Trust Level which provides a descriptive context associated by security level. Therefore, the remainder of this document and the accompanying Implementation Guidelines document will offer a corollary non-numeric description of levels to equate to the numerical levels used by the government:

“High Trust” = 4; “Medium High Trust” = 3; “Medium Trust” = 2”; and “Low Trust”= 1”

The highest trust level, Level 4, or FiXs equivalent “High” is aligned with Homeland Security Presidential Directive 12 (HSPD 12). HSPD 12, dated August 27, 2004, entitled “Policy for a Common Identification Standard for Federal Employees and Contractors” directed promulgation of a Federal standard for secure and reliable forms of identification for Federal employees and contractors. In March 2006 the National Institutes of Standards and Technology issued Federal Information Processing Standards 201 for Personal Identity Verification (PIV) of Federal Employees and Contractors. The PIV standards consist of two parts – PIV-I and PIV-II. PIV-I satisfies control objectives, including enrollment requirements of HSPD 12. PIV-II specifies implementation, including physical card characteristics, and use of identity credentials on integrated circuit cards for a federal personal identity verification system.

The next level, Level 3, or FiXs equivalent “Medium High” has not been defined at this time by a specific Federal Directive or Policy. FiXs members however have a requirement for this level of credential to meet their own use case situation(s), supporting constituencies such as: first responders, law enforcement, medical personnel, logistics personnel, maintenance and/or grounds personnel, etc. and others where the very highest level of background investigation is not warranted or practical. Accordingly, FiXs has promulgated Implementation Guidelines to accommodate these requirements and has presented these Implementation Guidelines to the Federal Government for consideration and adoption. FiXs-certified credential defined at the “medium high trust” level, or government Level 3, are aligned with PIV II, but differ from PIV I provisions in the enrollment process.

Level 2, or FiXs equivalent “Medium” is again aligned with PIV II, and differs somewhat from Level 3 in the enrollment process. The details for both the “medium high trust” and the “medium trust” levels are defined in detail in the FiXs Implementation Guidelines.

Level 1 or FiXs equivalent “Low”. is considered an un-acceptable level of trust for the Federal Government and for many use cases where a certain authoritative level of trust is needed or desired. FiXs “Certified Credentials” will at a future date assess the validity, requirements and resources required for this level. The level presently is not being used.

The FiXs Implementation Guidelines document provides the specific requirements for the vetting of sponsored individuals requesting credentials for “high”, medium high”, and “medium” trust levels”, and in specific market/functional venues. The accompanying CHUID section of the Implementation Guidelines deals with the specifics of the data and specifications of the card. Accordingly, these Operating Rules and the Implementation Guidelines must be read in tandem to implement FiXs cross-credentialing services.

Historically, FiXs has borrowed many of its operating concepts from the electronic payments industry. In the electronic payments industry, specific operating rules provide a uniform business and legal framework, as well as standard formats, for the exchange of financial payments. To rely on the principles already proven and established for the payments industry, NACHA – The Electronic Payments Association assisted with its knowledge and experience in development of the FiXs Operating Rules. This decades long experience and lessons learned allows FiXs to provide a proven and time-tested framework for inter-operable identity authentication similar to what has been achieved in the financial industry for financial transactions.

Since processing an employee's credentials is analogous to processing a payment, the FiXs Operating Rules for cross-credentialing encourage maximum participation among participating members that would otherwise use differing internal practices, standards, and platforms. The objective is to establish the standards and operational framework for a secure and interoperable “Chain of Trust” for all members regardless of industry or professional designation(s).

The FiXs Implementation Guidelines document provides detail on the requirements for issuing FiXs-Certified Credentials at different levels of confidence or assurance. The FiXs Operating Rules contain minimum requirements for issuing FiXs-Certified Credentials. All FiXs-Certified Credentials, regardless of their level of assurance, must comply with the FiXs Operating Rules and these Implementation Guidelines. The FiXs Implementation Guidelines provide additional requirements that must be followed by Member Organizations and Subscribers, depending upon the level and type of Credential issued. These processes deal with, but are not limited to, identity verification, enrollment, security and audit. These Guidelines only address provisions that are more detailed than the requirements in the FiXs Operating Rules.

All FiXs Certified credentials will have the ability to be distinguished according to the Level of Trust assurance under which they were issued. The following guidelines are not inclusive of the life cycle management controls and will be addressed at a later date.

2 FIXS ASSURANCE LEVELS

2.1 Overview

An underlying objective, whether explicit or not, of most identity management programs is to manage risk. In order to do that, a Credential Issuer first defines an acceptable level of risk and then identifies standards, criteria and procedures that, to the extent possible, support this level. Sometimes, the risk level and standards are defined by an external organization, such as a government Agency or client. When this is the case, a Credential Issuer must adopt the prescribed processes and requirements. However, another aspect of identity management programs is striking an appropriate balance between risk management, cost and feasibility considerations. This can be achieved through a Federated approach. For instance, it is possible to enact standards or criteria that are too stringent and that unnecessarily eliminate otherwise qualified personnel from being issued a credential. In addition to defining an acceptable level of risk, Credential Issuers should also consider the demographic of the population to be credentialed and the resources (physical and/or logical) to which the credential holders will have access. Thus, by “federating” the approach, it is possible to accommodate these requirements

In order to streamline this process for Credential Issuers, FiXs has identified and endorsed several Assurance Levels, targeted at different user communities. When developing these Assurance Levels, FiXs first identified “target populations” that would require credentials and then analyzed what types of resource access the credential holder might need. For instance, contractors working on US Federal government contracts might need access to US Federal government facilities or logical resources (a government LAN). In this case, the User would require a FiXs HSPD-12 Compatible Credential, which is based on FiXs Assurance Level 4. This particular credential is intentionally aligned with the government’s “Personal Identity Verification” (PIV) standard. In another example, Emergency Responders requiring access to an emergency scene might qualify for one of the Assurance Level 3 credentials. The Assurance Levels are defined in Section 1.1, while implementation guidelines for the specific user groups are provided in Section 2.

2.2 Identity Management Methodologies

Two methodologies support the risk management feature of identity management programs: identity verification and identity vetting. **Identity verification** uses manual and electronic methods to prove, to some level of certainty, that an applicant is who he says he is. Manual methods of verification include visual review of identity documents, such as birth certificates or drivers licenses, by trained personnel. Electronic methods include electronic authentication of documents using a document authenticator, or a “knowledge-based challenge quiz” that involves asking the applicant questions to which only the applicant should know the answers.

Identity vetting assumes that, from a risk assessment standpoint, a likely predictor of a person’s future behavior is their past behavior. Identity vetting, then, uses various methods and tools to establish a profile of a person’s behavior. In most cases, Identity vetting begins with an Applicant providing a detailed

background history including past residences, employment history, educational background and any criminal record. Even though much of this information will be returned by the actual background check, asking a person to self report this information provides an additional measure of trustworthiness. Depending on the Assurance Level, a background check may include an FBI Name and Fingerprint check, a local records (criminal database) check, manual verification of the Applicant's educational attainment, and/or a credit history report which may validate the Applicant's reported residence history. Once this historical information is compiled, a trained Adjudicator must make a trustworthiness assessment of the Applicant prior to the Applicant being enrolled into a FiXs Domain Server.

A strong identity management program often utilizes both identity verification and identity vetting elements.

2.3 Implementing the Assurance Levels

Specific implementation standards, as proposed by user industry experts and approved by the FiXs Board, are provided in Section 2 of this document. Members wishing to issue FiXs Credentials must first identify which standards they intend to follow and then meet the requirements of the specified standard(s).

2.4 Assurance Level Overview

The FiXs Assurance Levels described below are aligned to the National Institute of Standards and Technology's (NIST) Information Security guidelines [NIST SP 800-63].

2.4.1 HIGH TRUST LEVEL (LEVEL 4)

The High Level of Trust, (Level 4), is aligned with Homeland Security Presidential Directive 12 (HSPD 12). HSPD 12, dated August 27, 2004, entitled "Policy for a Common Identification Standard for Federal Employees and Contractors" directed promulgation of a Federal standard for secure and reliable forms of identification for Federal employees and contractors. In March 2006 the National Institutes of Standards and Technology issued Federal Information Processing Standards 201 for Personal Identity Verification (PIV) of Federal Employees and Contractors. The PIV standards consist of two parts – PIV-I and PIV-II. PIV-I satisfies control objectives, including enrollment requirements, of HSPD 12. PIV-II specifies implementation, including physical card characteristics, and use of identity credentials on integrated circuit cards for a Federal personal identity verification system.

Examples of persons needing a High Trust Level (Level 4) credential include contractors on US government contracts, employees of FiXs Member Companies that require a High Level assurance credential, and individuals that currently have a clearance or that will be processed for a clearance. In this last case, the background check involved in the

clearance process may be substituted for the High Level assurance background check.

2.4.2 MEDIUM HIGH TRUST LEVEL (LEVEL 3)

The Medium High Trust level (Level 3), has not been defined, at this time, by a Federal Directive or Policy. FiXs members, however, have a requirement for using this level of credential in both the government and commercial sectors, and thus FiXs has developed a set of Guidelines to accommodate that Medium High (Level 3) requirement. These Guidelines have been offered to the Federal government for consideration and adoption. FiXs Credentials certified at the Medium High Trust Level are aligned and compliant with FIPS 201, but will differ from PIV I provisions relating to the enrollment and vetting processes.

The Medium High Trust Level is designed to provide a medium high level of assurance for employees and includes both identity verification and in some cases additional identity vetting/verification attributes (i.e. First Responder and Health Care personnel Credentials). This level will require a background check, using commercially available sources of data, and fingerprints will be collected digitally at time of enrollment and **will be** sent to the FBI for a National Criminal History Fingerprint check.

Possible uses of a Medium High Trust Level include; employees of FiXs Member Companies/Organizations who do not need daily or frequent access to federal resources to support a government contracts; and credentialing a First Responder community, or service personnel who need access to federal or commercial facilities or environs. The Medium High Trust credential can also be used for Commercial applications.

2.4.3 MEDIUM TRUST LEVEL (LEVEL 2)

The FiXs Medium Trust Level (Level 2) applies to a level of assurance required by a specific implementation. This will require a background check, using commercially available sources of data, and fingerprints will be collected digitally at time of enrollment, solely for the purpose of linking to the issued credential. At this level the fingerprints **will not** be sent to the FBI for a National Criminal History Fingerprint Check.

The Medium Level may suit those commercial vendors who may require frequent access to facilities in order to provide deliveries; or stock shelves/vending machines; or provides maintenance services. This Medium Level may provide adequate acceptable risk for granting local privileges at lower threat levels, but may not be acceptable as threat levels rise. This level may also be used to accommodate persons who may temporarily work in positions of public trust, such as certain categories of first responders, health care workers or volunteers who help out at a disaster scene (i.e., Red Cross and other volunteers; public works employees; emergency technicians, etc.). The Medium Level credential can also be used for Commercial applications.

2.4.4 LOW TRUST LEVEL (LEVEL 1)

FiXs assigns the Low Level Trust (Level 1) the working definition of: a level of assurance that requires minimal proof of identity but no background check, and no document verification, therefore, it provides little or no level of trust assurance.

FiXs Credential Issuers are not permitted to enroll Users at a Low Trust Level (1); load any data into a FiXs Domain Server; nor attempt to authenticate such credentials across the FiXs Network.

Examples of a Low Level (1) credentials are shopper discount cards and public email accounts. Because these “credentials” may be granted by non-FiXs Members or Subscribers without any kind of identity verification, FiXs Members or Subscribers are cautioned against granting rights to a bearer.

2.5 FiXs Assurance Level Implementations

FiXs Credential Name	Assurance Level	Who
HSPD-12 Compatible Credentials	High (4)	<ul style="list-style-type: none"> • FiXs Member Company (or Subscriber) employees or contractors who perform work under a Federal government contract that includes the identity FAR clause. • Employees of a FiXs Member Company (or Subscriber) that requires an HSPD-12 Compatible Credential for some or all of their employees.
DoD Logical Access Credentials (LACS)/Physical Access Credentials (PACS) Credentials	High (4)	<ul style="list-style-type: none"> • FiXs Member Company (or Subscriber) employees or contractors on U.S. Department of Defense contracts who require long term (6 months or greater) access to DoD physical or logical resources. • FiXs Member Company (or Subscriber) employees who are required to authenticate to DoD resources at the highest level of assurance (Level 4).
DoD and Commercial use PACS/Short-term LACS Credentials	Medium High (3)	<ul style="list-style-type: none"> • FiXs Member Company (or Subscriber) employees or contractors who require physical access to a U.S. Department of Defense facility. • FiXs Member Company (or Subscriber) employees who are required to authenticate to DoD resources at a medium high level of assurance (3). • FiXs Member Company (or Subscriber) employees who do not have a requirement to authenticate to government facilities but do have a need for a medium high level of assurance for commercial use for physical/logical access.
Non-Security Clearance Contractor and Commercial use Credential	Medium High (3)	<ul style="list-style-type: none"> • Participants are those individuals needing physical access to Govt. facilities on a limited basis or for commercial uses not requiring access to government facilities. Examples of the would be: <ul style="list-style-type: none"> ○ Transportation Workers ○ Commercial Vendors <ul style="list-style-type: none"> ▪ Delivery Personnel ▪ Grounds personnel ▪ Repair Technicians ▪ Cleaning & Maintenance personnel ○ Facility Visitors for occasional official business ○ Leaders of tour groups, school personnel, on official tours ○ Health Care employees/patients ○ Financial/Insurance sector employees/customers

FiXs Credential Name	Assurance Level	Who
Enhanced First Responder	Medium High (3)	<ul style="list-style-type: none"> • Participants who may need a FiXs Medium High Level (3) Enhanced First Responder Credential may include first responders identified by the authority having jurisdiction as holding sensitive positions or requiring access to secure Federal, State, or local facilities. These individuals may include but are not limited to: <ul style="list-style-type: none"> ○ Police Officers ○ Sheriffs Officers ○ Corrections Officers ○ Municipal, County, State and Industrial Fire Fighters ○ Emergency Medical Technicians and Paramedics
Enhanced Clinical First Responder Credential	Medium High (3)	<ul style="list-style-type: none"> • Participants who may need a FiXs Medium High Level (3) Enhanced Clinical First Responder Credential may include first responders identified by the authority having jurisdiction as holding sensitive positions or requiring access to secure Federal, State, or local facilities. These individuals may include but are not limited to: <ul style="list-style-type: none"> ○ Physicians ○ Registered Nurses ○ Behavioral Health Professionals¹ ○ Advanced Practice Nurses² ○ Physicians Assistants ○ Dentists ○ Emergency Medical Technicians and Paramedics
Standard First Responder Credential	Medium (2)	<ul style="list-style-type: none"> • Participants who may need a FiXs Medium Level <ul style="list-style-type: none"> ○ (2) Standard First Responder Credential may include but are not limited to: <ul style="list-style-type: none"> ○ Municipal, County, State and Industrial Fire Fighters ○ Emergency Medical Technicians ○ Public Works Employees ○ Red Cross, Salvation Army and other humanitarian volunteers ○ National Citizen Corps Volunteers

¹ Marriage and Family Therapists, Medical and Public Health Social Workers, Mental Health and Substance abuse Social Workers, Psychologists, and Mental Health Counselors. ESAR-VHP Interim Technical and Policy Guidelines, Standards, and Definitions – Version 2 June 2005

² Nurse Practitioners, Nurse Anesthetists, Certified Nurse Midwives, Clinical Nurses Specialists. ESAR-VHP Interim Technical and Policy Guidelines, Standards, and Definitions – Version 2 June 2005

FiXs Credential Name	Assurance Level	Who
Standard Clinical First Responder Credential	Medium (2)	<ul style="list-style-type: none"> • Participants who may need a FiXs Medium Level (2) Standard Clinical First Responder Credential may include but are not limited to: <ul style="list-style-type: none"> ○ Pharmacists ○ Licensed Practical Nurses ○ Respiratory Therapists and Technicians ○ Cardiovascular Technologist and Technicians ○ Radiological Technologists & Technicians ○ Surgical Technologists ○ Medical and Clinical Laboratory Technologists

3 FIXS IMPLEMENTATION GUIDELINES

3.1 High Level (4) --- HSPD-12 Compatible Credentials

A FiXs HSPD-12 Compatible Credential is based on a High Level assurance (4), set of processes, and the highest assurance level achievable. The credential aligns with the Federal government’s “Personal Identity Verification” (PIV) standards. The FiXs HSPD-12 Compatible Credential requires two forms of government ID to verify the person’s identity and uses a background check to evaluate a person’s trustworthiness to have access to physical and logical resources.

3.1.1 USERS

Participants who may need a FiXs HSPD-12 Compatible Credential include:

- FiXs Member Company (or Subscriber) employees or contractors who perform work under a Federal government contract that includes the identity FAR clause.
- Employees of a FiXs Member Company (or Subscriber) that requires an HSPD-12 Compatible Credential for some or all of their employees.

High Level HSPD-12 Compatible Credentials	
System Requirements	<ul style="list-style-type: none"> Must adhere to the “FIPS PUB 201: Personal Identity Verification (PIV) of Federal Employees and Contractors” standards, including separation of system roles and revocation requirements.
Identity Verification Requirements:	<ul style="list-style-type: none"> Applicant must appear in person Applicant must present 2 forms of government ID, per the I-9 form, one of which must be a photo ID
Identity Vetting Requirements:	<ul style="list-style-type: none"> NAC: <ul style="list-style-type: none"> Security/Suitability Investigations Index (SII) Defense Clearance and Investigations Index (DCII) FBI Name Check FBI National Criminal History Fingerprint Check Written inquiries and searches of records: <ul style="list-style-type: none"> Employment, going back 5 years Education, going back 5 years and verifying highest degree Residence, going back 3 years References Law enforcement checks, going back 5 years
Adjudication Standards:	<p>The following criterion will be used to adjudicate the background investigations for persons requiring a FiXs HSPD-12 Compatible Credential. No person shall be granted such a credential if their background investigation reveals any of the following:</p> <ul style="list-style-type: none"> Is, or is suspected of being, a terrorist; Is the subject of an outstanding warrant; Has deliberately omitted, concealed, or falsified relevant and material facts from any official form used to collect biographic information for the purpose of initiating a background check; Has presented false or forged identity source documents; Has been barred from Federal employment; Is currently awaiting a hearing or trial or has been convicted of a crime punishable by imprisonment of six (6) months or longer; or Is awaiting or servicing a form of pre-prosecution probation, suspended or deferred sentencing, probation or parole in conjunction with an arrest or criminal charges against the individual for a crime that is punishable by imprisonment of six (6) months or longer.

3.2 High Level (4) --DoD Logical Access Credentials (LACS)/Physical Access Credentials (PACS) Credential

The FiXs DoD LACS/PACS Credential is based on assurance Level 4 and is intended for individuals who will have long-term physical and/or logical access to DoD resources.

3.2.1 USERS

Participants who may need a DoD LACS/PACS Compatible Credential include:

- FiXs Member Company (or Subscriber) employees or contractors on U.S. Department of Defense contracts who require long term (6 months or greater) access to DoD physical or logical resources.
- FiXs Member Company (or Subscriber) employees who are required to authenticate to DoD resources at the highest level of assurance (Level 4).

High Level DoD LACS/PACS Credential	
System Requirements	<ul style="list-style-type: none">• Must adhere to the “FIPS PUB 201: Personal Identity Verification (PIV) of Federal Employees and Contractors” standards, including separation of system roles and revocation requirements.• In addition, the System must also capture the following:<ul style="list-style-type: none">◦ Contract number under which the FiXs Member Company (or Subscriber) employee requires access to DoD resources, and◦ Reference to any existing security clearance an Applicant might have.
Identity Verification Requirements:	<ul style="list-style-type: none">• Applicant must appear in person• Applicant must present 2 forms of government ID, per the I-9 form, one of which must be a photo ID
Identity Vetting Requirements:	<ul style="list-style-type: none">• NAC:<ul style="list-style-type: none">◦ Security/Suitability Investigations Index (SII)◦ Defense Clearance and Investigations Index (DCII)◦ FBI Name Check◦ FBI National Criminal History Fingerprint Check• Written inquiries and searches of records:<ul style="list-style-type: none">◦ Employment, going back 5 years◦ Education, going back 5 years and verifying highest degree◦ Residence, going back 3 years◦ References◦ Law enforcement checks, going back 5 years

High Level DoD LACS/PACS Credential

Adjudication Standards:

The following criterion will be used to adjudicate the background investigations for persons requiring a FiXs DoD LACS/PACS Credential. No person shall be granted such a credential if their background investigation reveals any of the following:

- Is, or is suspected of being, a terrorist;
- Is the subject of an outstanding warrant;
- Has deliberately omitted, concealed, or falsified relevant and material facts from any official form used to collect biographic information for the purpose of initiating a background check;
- Has presented false or forged identity source documents;
- Has been barred from Federal employment;
- Is currently awaiting a hearing or trial or has been convicted of a crime punishable by imprisonment of six (6) months or longer; or
- Is awaiting or servicing a form of pre-prosecution probation, suspended or deferred sentencing, probation or parole in conjunction with an arrest or criminal charges against the individual for a crime that is punishable by imprisonment of six (6) months or longer.

3.3 Medium High Level (3)---DoD and Commercial Use PACS/LACS Credential

The FiXs DoD and Commercial Use PACS/Short-term LACS Credential, which is based on the Medium High assurance level, provides a medium high amount of assurance the credential holder is who they assert themselves to be and that they do not harbor any malicious or criminal intent.

3.3.1 USERS

Participants who may need a DoD and Commercial Use PACS/Medium High/ LACS Credential include:

- FiXs Member Company (or Subscriber) employees or contractors who, based on a contract with the DOD, require physical access to a DoD facility.
- An employee or contractor of a FiXs Member Company (or Subscriber) who, because of short term contractual terms, needs a credential for access.
- FiXs Member Company (or Subscriber) employees who are required to authenticate to DoD resources at a medium high level of assurance.
- FiXs Member Company (or Subscriber) employees who **do not** have a requirement to authenticate to DoD or other government entities but do have a commercial use requirement.

Medium High Level DoD and Commercial Use PACS/ LACS Credential
System Requirements
<ul style="list-style-type: none"> • Must adhere to the “FIPS PUB 201: Personal Identity Verification (PIV) of Federal Employees and Contractors” standards, including separation of system roles and revocation requirements. • In addition, the System must also capture the following: <ul style="list-style-type: none"> ◦ Contract number under which the FiXs Member Company (or Subscriber) employee requires access to DoD resources, and ◦ Reference to any existing security clearance an Applicant might have.
Identity Verification Requirements:
<ul style="list-style-type: none"> • Applicant must appear in person • Applicant must present 2 forms of government ID, per the I-9 form, one of which must be a photo ID
Background Check Components:
<ul style="list-style-type: none"> • Terrorist watch list check • Law Enforcement checks, going back five (5) years • FBI Name Check • FBI National Criminal History Fingerprint Check
Adjudication Standards:
<p>The following criterion will be used to adjudicate the background investigations for persons requiring a FiXs DoD PACS/Short-term LACS Credential. No person shall be granted such a credential if their background investigation reveals any of the following:</p> <ul style="list-style-type: none"> • Is, or is suspected of being, a terrorist; • Is the subject of an outstanding warrant; • Has deliberately omitted, concealed, or falsified relevant and material facts from any official form used to collect biographic information for the purpose of initiating a background check; • Has presented false or forged identity source documents; • Is currently awaiting a hearing or trial or has been convicted of a crime punishable by imprisonment of six (6) months or longer; or • Is awaiting or servicing a form of pre-prosecution probation, suspended or deferred sentencing, probation or parole in conjunction with an arrest or criminal charges against the individual for a crime that is punishable by imprisonment of six (6) months or longer.

3.4 Medium High Level (3)---Non-Security Clearance Contractor and Commercial Use Credential

The FiXs Non-Security Clearance and Commercial Use Credential, which is based on a Medium High Trust assurance level, provides a medium high amount of assurance that the credential holder is who he/she asserts themselves to be and that they do not harbor any malicious or criminal intent. Timely physical access is

imperative for the individual to be able to provide their service to the receiving Government office.

3.4.1 **USERS**

Participants who may need a Non-Security Clearance Contractor credentials include:

- Transportation Workers
- Commercial Vendors
- Maintenance Personnel
- Cleaning and Grounds Personnel
- Repair technicians
- Facility Visitors for occasional official business
- Leaders of tour groups, school personnel, etc who conduct tours
- Health Care Personnel
- Critical Infrastructure Supply Chain personnel

Medium High Level (3) – Non-Security Clearance and Commercial Use Credential for Commercial Vendors and Non-government employees and government contractors

System Requirements

Must adhere to the Fair Credit and Reporting Act (The FCRA) and other applicable laws. All identified job skills personnel/individuals must be informed, by the credential issuer, that by giving their approval under the “Identity Verification Requirement” and entering their personally identifiable data into the system, they consent and authorize FiXs and/or third party background screening provider(s) to perform background screenings checks for them that “requires physical or logical access to their job or agency-related activity but do not fall under the category of government employee or government contractor.

Identity Verification Requirements

- Applicants must have a sponsor (*authorizes the need for applicant to obtain physical and logical access to Federal facility*)
- Applicant must appear in person at Registration or Enrollment Station
- Applicant must present 2 forms of Government issued ID Per US Form I-9 or 6 CFR Part 37³, one of which must have a photo.
- Individual Information:
 - ✓ Date of birth;
 - ✓ Proof of SSN or ineligibility for an SSN;
 - ✓ The applicant’s address of principal residence; and
 - ✓ Lawful status in the United States.
 - ✓ Company-issued Employee Identification Number
 - ✓ Felony and Misdemeanor convictions
 - ✓ Outstanding warrant
 - ✓ Terrorist Watch List
- Applicants fingerprints will be collected electronically (ten flat or rolled)
- Applicants pin must be used to complete the transaction

³ A valid unexpired U.S. passport; A certified copy of a birth certificate; A consular report of birth abroad; An unexpired permanent resident card.; An unexpired employment authorization document (EAD); An unexpired foreign passport with valid U.S. visa affixed; A U.S. certificate of citizenship; A U.S. certificate of naturalization; or A REAL ID driver's license or identification card issued subsequent to the standards established by this regulation.

**Medium High Level (3) – Non-Security Clearance and Commercial Use Credential
for Commercial Vendors and Non-government employees and government
contractors**

Identity Vetting Requirements

- **NAC I Commercial Equivalent Check (CEC).**
 - FBI Name and FBI National Criminal History Fingerprint Check
 - Terrorist Watch List
 - Local Law Enforcement agency check
 - Residency verification
- **Written Inquires and Search of Records**
 - Employment going back 5 years
 - Education going back 5 years
 - Residences going back 3 years (*Note: Separately, all overseas addresses*)
 - References (*3 personal, non-relatives*)

Adjudication Standards:

The following criteria will be used to adjudicate the background checks for persons requiring a FiXs Non-Security Clearance Contractor Credential at the Medium High Level (3). No person shall be granted such as credential if the background check reveals any of the following:

- Is or is suspected of being a terrorist;
- Has been charged or convicted under any provision of the Patriot Act
- Is the subject of an outstanding warrant;
- Has deliberately omitted, concealed, or falsified relevant or material facts from any official form used to collect biographic information for the purpose of initiating a background check;
- Has presented false or forged identity documents;
- Has a current Criminal (not civil) restraining order, or has had a criminal restraining order within the last five years, issued due to threat of violence or sexual assault
- Is on the Sex Offenders List (level 2 or 3) (in the last ten years level 2, life level 3)
- Is currently awaiting a hearing or trial or has been convicted of a crime punishable by imprisonment of six (6) months or longer; or
- Is awaiting or servicing a form of pre-prosecution probation; suspended or deferred sentencing, probation or parole in conjunction with an arrest or criminal charges against the individual for a crime that is punishable by imprisonment of six (6) months or longer.

3.5 MEDIUM HIGH LEVEL (3)--First Responder Employees

Enhanced First Responder Credential – Medium High Level (3) The FiXs Enhanced First Responder Credential, which is based on a Medium High Trust assurance level, provides a medium high amount of assurance that the credential holder is who he/she asserts themselves to be and that he does not harbor any malicious or criminal intent.

3.5.1 USERS

Participants who may need a FiXs Medium High Level Enhanced First Responder Credential may include first responders identified by the authority having jurisdiction as holding knowledge sensitive positions or requiring unlimited access to secure Federal, State, or local facilities.

Medium High Level (3) – Non-Security Clearance Credential for Enhanced First Responder Designees

Identity Verification Requirements

- Applicants must have a sponsor (*authorizes the need for applicant to obtain physical and logical access to Federal facility*)
- Applicant must appear in person at Registration or Enrollment Station
- Applicant must present 2 forms of Government issued ID Per US Form I-9 or 6 CFR Part 37⁴, one of which must have a photo.
- Applicants fingerprints will be collected electronically (ten flat or rolled)
- Applicant must appear in person
- Applicant must present 2 forms of Government issued ID Per US Form I-9 or 6 CFR Part 37, one of which must have a photo. Documents must include information supporting the claim of
 - Date of birth;
 - Proof of SSN or ineligibility for an SSN;
 - The applicant's address of principal residence; and
 - Lawful status in the United States.
- Applicants fingerprints will be collected electronically (ten flat or rolled)
- Applicants pin must be used to complete the transaction

⁴ A valid unexpired U.S. passport; A certified copy of a birth certificate; A consular report of birth abroad; An unexpired permanent resident card.; An unexpired employment authorization document (EAD); An unexpired foreign passport with valid U.S. visa affixed; A U.S. certificate of citizenship; A U.S. certificate of naturalization; or A REAL ID driver's license or identification card issued subsequent to the standards established by this regulation.

Medium High Level (3) – Non-Security Clearance Credential for Enhanced First Responder Designees

Identity Vetting Requirements

- Establish validity of the identity - Identity proofing using electronic methods providing identity proofing criteria from public record and publicly available sources to include verification of enrollment information and breeder documents required in Federal form I-9, to verify the identity exists, the identity is active (not deceased) and the components are related at a high level of assurance.
- Establish ownership of the identity - vetting fraudulently obtained breeder documents using a third party interactive knowledge based query process presenting a minimum of five questions with successful response to at least 3.
- Biometric Cross Reference – Submit and check biometric against existing records for identity duplication and or criminal record history – to include but not limited to the Automated Fingerprint Identification System (AFIS)
- Criminal History Record Information (CHRI) / Risk Analysis (include a data quality score?) - to include Local, County, State, Federal Criminal History Checks; Department of Corrections Checks, Sex Offender Registry (SOR within NCIC), Patriot Act, Terrorist Watch List, Interstate Identification Index (triple I), NICS Index (firearms disqualifying records), National Crime Information Center (NCIC), National Protection Order File (within NCIC)
- **Written Inquires and Search of Records**
 - Employment going back 5 years
 - Education going back 5 years
 - Residences going back 3 years (*Note: Separately, all overseas addresses*)
 - References (3 personal, non-relatives)

Medium High Level (3) – Non-Security Clearance Credential for Enhanced First Responder Designees

Adjudication Standards:

The following criteria will be used to adjudicate the background checks for persons requiring a FiXs Standard First Responder Credential. No person shall be granted such a credential if the background check reveals any of the following:

- Is or is suspected of being a terrorist;
- Has been charged or convicted under any provision of the Patriot Act
- Is the subject of an outstanding warrant;
- Has deliberately omitted, concealed, or falsified relevant or material facts from any official form used to collect biographic information for the purpose of initiating a background check;
- Has presented false or forged identity documents;
- Has a current Criminal (not civil) restraining order, or has had a criminal restraining order within the last five years, issued due to threat of violence or sexual assault
- Is on the Sex Offenders List (level 2 or 3) (in the last ten years level 2, life level 3)
- Is currently awaiting a hearing or trial or has been convicted of a violent crime punishable by imprisonment of six (6) months or longer; or
- Is awaiting or servicing a form of pre-prosecution probation; suspended or deferred sentencing, probation or parole in conjunction with an arrest or criminal charges against the individual for a crime that is punishable by imprisonment of six (6) months or longer.

3.6 MEDIUM LEVEL (2)--First Responder Employees

Enhanced First Responder Credential – Medium Level (2)

The FiXs Standard First Responder Credential, which is based on Medium Trust assurance level, provides a medium amount of assurance that the credential holder is who he/she asserts themselves to be and that they do not harbor any malicious or criminal intent.

3.6.1 USERS

Participants who may need a FiXs Medium Level (2) Standard First Responder Credential may include first responders identified by the authority having jurisdiction as holding sensitive positions or requiring access to secure Federal, State, or local facilities.

Medium Level (2) – Non-Security Clearance Credential for Standard First Responder Designees

System Requirements

Must adhere to the Fair Credit and Reporting Act (The FCRA) and other applicable laws, this is to inform all identified job skills/individuals that by giving their approval under the “Identity Verification Requirement” and entering their personally identifiable data, they consent and authorize FIX’s and/or third party background screening provider(s) to perform background screenings checks for them that “requires physical or logical access to their job or agency-related activity but do not fall under the category of government employee or government contractor. Must adherer to the “FIPS PUB 201 Personal Identity Verification (PIV) I of Federal Employees and Contractors” only as it relates to;

- Control Objectives
- Privacy Requirements

Identity Verification Requirements

- Applicants must have a sponsor (*authorizes the need for applicant to obtain physical and logical access to Federal facility*)
- Applicant must appear in person at Registration or Enrollment Station
- Applicant must present 2 forms of Government issued ID Per US Form I-9 or 6 CFR Part 37⁵, one of which must have a photo.
- Applicants fingerprints will be collected electronically index fingers for the sole purpose of tying the identity to the credential.
- Applicant must appear in person
- Applicant must present 2 forms of Government issued ID Per US Form I-9 or 6 CFR Part 37 , one of which must have a photo. Documents must include information supporting the claim of
 - Date of birth;
 - Proof of SSN or ineligibility for an SSN;
 - The applicant’s address of principal residence; and
 - Lawful status in the United States.
- Applicants fingerprints will be collected electronically (ten flat or rolled) for identity and adjudication purposes
- Applicants pin must be used to complete the transaction

Identity Vetting Requirements

- Establish validity of the identity - Identity proofing using administrative/manual methods providing identity proofing criteria from breeder documents required in Federal form I-9, to verify the identity exists, the identity is active (not deceased) and the components are related at a moderate level of assurance.
- Criminal History Record Information (CHRI) / Risk Analysis (include a data quality score?) - to include Local, County, State as required by the laws governing the sponsoring authority

⁵ A valid unexpired U.S. passport; A certified copy of a birth certificate; A consular report of birth abroad; An unexpired permanent resident card.; An unexpired employment authorization document (EAD); An unexpired foreign passport with valid U.S. visa affixed; A U.S. certificate of citizenship; A U.S. certificate of naturalization; or A REAL ID driver’s license or identification card issued subsequent to the standards established by this regulation.

Medium Level (2) – Non-Security Clearance Credential for Standard First Responder Designees

Adjudication Standards:

The criteria to be used to adjudicate the background checks for persons requiring a FiXs Standard (level 2) First Responder Credential is determined by the State, County, and local, requirements and laws governing the sponsoring authority.

4 ATTRIBUTE MANAGEMENT FOR MEDIUM HIGH LEVEL (3) ENHANCED FIRST RESPONDER CREDENTIALS

The credentialing process for First Responders carry some unique characteristics due to program requirements of the Federal Emergency Management Agency recently clarified by verbiage in Public Law 110-53.

The terms “credentialed and credentialing”, for this community of users, carries the meaning of providing or having provided, respectively, documentation that identifies personnel and certifies the qualifications (**attributes**) of such personnel by ensuring that such personnel possess a minimum common level of training, experience, physical and medical fitness, and capability appropriate for a particular position in accordance with standards created under section 510;⁶

The FiXs Enhanced First Responder Credential, which is based on the FiXs Medium High assurance level (3), provides a medium high level of assurance that the credential holder is who he/she asserts themselves to be and meets the minimum qualifications required by the federal government sited above

4.1 Attribute Management for Medium High Level (3) Clinical First Responder Credentials

The clinical first responder credential must meet the requirements of Emergency System for Advanced Registration of Health Professions Volunteers. Title 42, Chapter 6A, Sub-Chapter II, Part B, § 247d-7b⁷

4.1.1 USERS

Participants who may need a FiXs Medium High Level (3) Enhanced Clinical First Responder Credential may include but are not limited to:

- Physicians
- Registered Nurses
- Behavioral Health Professionals⁸
- Advanced Practice Nurses⁹
- Physicians Assistants
- Dentists
- Emergency Medical Technicians (EMT's) and Paramedics
- Pharmacists
- Licensed Practical Nurses
- Respiratory Therapists and Technicians

⁶ PUBLIC LAW 110-53- IMPLEMENTING RECOMMENDATIONS OF THE 9/11 COMMISSION ACT OF 2007, TITLE IV, SEC. 401- DEFINITIONS, § (a) (3)

⁷ Retrieved September 4th, 2007 from
www4.law.cornell.edu/uscode/html/uscode42/usc_sec_42_00000247---d007b

⁸ Marriage and Family Therapists, Medical and Public Health Social Workers, Mental Health and Substance abuse Social Workers, Psychologists, and Mental Health Counselors. ESAR-VHP Interim Technical and Policy Guidelines, Standards, and Definitions – Version 2 June 2005

⁹ Nurse Practitioners, Nurse Anesthetists, Certified Nurse Midwives, Clinical Nurses Specialists. ESAR-VHP Interim Technical and Policy Guidelines, Standards, and Definitions – Version 2 June 2005

- Cardiovascular Technologist and Technicians
- Radiological Technologists & Technicians
- Surgical Technologists
- Medical and Clinical Laboratory Technologists
- Medical and Clinical Laboratory Technicians including Phlebotomists
- Diagnostic Medical Sonographers
- Veterinarians

Clinical Licensure Verification Requirements	
System Requirements	
	<ul style="list-style-type: none"> • Must adhere to the Fair Credit and Reporting Act (The FCRA) and other applicable laws, this is to inform all identified job skills/individuals that by giving their approval under the "Clinical Licensure Verification Requirement" and entering their personally identifiable data, they consent and authorize FIX's and/or third party background screening provider(s) to perform qualifications screenings checks for them that "requires physical or logical access to their job or agency-related activity but do not fall under the category of government employee or government contractor. Must adherer to the Department of Health and Human Services Standard for Early System for Advanced Registration of Volunteer Health Professionals, Standards of the Joint Commission (JAHCO), and any applicable local, County or State Requirements
Licensure Verification Requirements	
	<ul style="list-style-type: none"> • Applicant must appear in person • Applicant must present (dependent on profession); <ul style="list-style-type: none"> ○ Original copy of a state issued medical license with no restrictions, and or active and unrestricted state issued license to practice with the scope identified by the state ○ Original copy of MD. DO. PhD. MS. RN. Degree from an educational institution accredited by the authority having jurisdiction referenced under "evidence of credential – explanation of credential elements" from the emergency credentialing standard for that profession as defined in the HHS ESAR-VHP Standard. ○ Original copy of the DEA Registration Certificate for License Verification ○ Proof of Active Clinical practice through attestation or other documentation or peer reference from a credential holding peer (with ID reference), affirming that the individual is practicing medicine, or working within the scope of the profession being vetted, in a hospital or non hospital setting. ○ Proof of Active Clinical Hospital Privileges through attestation or other documentation or peer reference from a credential holding peer (with ID reference) , affirming that the individual is practicing medicine, or works within the scope of the profession being vetted and has privileges in a hospital setting. ○ Proof of State or National Certification to practice, under medical control, as a pre-hospital car provider • Applicants pin must be used to complete the transaction

Clinical Licensure Verification Requirements

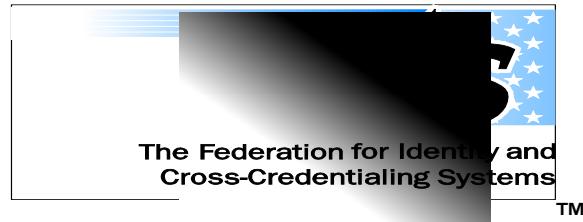
Licensure Vetting Requirements

- May include, dependent on professional, but not be limited to
- Primary Source Verification or delegation to a JCAHO accredited organization that has performed primary source verification of the individual's credentials.
- Degree, MD or DO through AAMC, AOA or ECFMG; for all others from an accredited institution
- Unencumbered Medical License from State of Issue
- Board Certification in recognized specialty or sub specialty from ABMS or AOA
- National Practitioner Databank Status
- Drug Enforcement Agency (DEA) License Verification with types
- Inspector General Status

Adjudication Standards:

The following criteria will be used to adjudicate the medical licensure and certifications for persons requiring a FiXs Clinical First Responder Credential. No person shall be granted such as credential if the licensure check reveals any of the following;

- Any failure to meet any of the credential elements for the profession as outlined in the Department of Health and Human Services Health resources Services Administrations "Standards and Guidelines for the Early System for the Advanced Registration of Volunteer Healthcare Professionals.
- Any Active Sanction on record with any State Inspector General
- Any Active disciplinary issue on file with the National Practitioner Databank



TECHNICAL SPECIFICATION FOR CREATING A UNIQUE IDENTIFIER FOR A FIPS 201-ALIGNED FIXS™ CREDENTIAL

**Version 1.0, rev. 02
January 10, 2007**

CHANGE HISTORY

Introduction

Homeland Security Presidential Directive -12 (HSPD-12) mandates the issuance of the Federal Information Processing Standard 201 (FIPS 201)-compliant Personal Identity Verification (PIV) card to all Federal employees and contractors starting October 27, 2006. The Department of Defense (DoD) Common Access Card (CAC) and the DoD Public Key Infrastructure (PKI) Programs are also being aligned to meet the additional set of requirements mandated by the Presidential Directive, HSPD-12. It is the objective of the Federation for Identity and Cross-Credentialing Systems™ (FiXs) organization to align any FiXs certified credential (also referred to as the FiXs credential) and the certified issuance process to meet, and “align” with, the requirements stated in FIPS 201.

The purpose of this Technical Specification is to define the FiXs certified credential’s unique identification number, which is consistent with the guidance provided by key documents such as NIST’s SP 800-73-1, *Interfaces for Personal Identity Verification*, published in March 2006 and the Technical Implementation Guidance for Smart Card Enabled Physical Access Control Systems (PACS), Version 2.3, dated December 20, 2005.

The topology of the FiXs certified card will follow the requirements of the FIPS 201 specification. These requirements are summarized in Appendix A Smart Card Topology Requirements and will not be discussed in detail in this specification. In addition, the FiXs smart card-based ID card topology will include a 3 of 9 barcode on the back of card that conforms to the FIPS 201 specification for an optional barcode. Details are included in Appendix B.

Background

Card Holder Unique Identifier (CHUID) Data Elements

NIST SP 800-73-1 specifies the PIV card application Card Holder Unique Identifier (CHUID) data object, which is further defined in PACS Version 2.3. Figure 1 “PACS V2.3 CHUID Data Model” shows the CHUID data model as it is defined in the PACS V2.3 specification. This data model is closely aligned with the PIV data model in SP 800-73-1. It includes both mandatory and optional data elements.

Data Element	Tag	Type	Max. Bytes	Mandatory/Optional
Buffer Length	EE	Fixed	2	M
FASC-N (SEIWG-012)	30	Fixed	25	M
Agency Code	31	Fixed	4	O
Organization Identifier	32	Fixed	4	O
DUNS	33	Fixed	9	O
GUID	34	Fixed	16	M
Expiration Date	35	Date (YYYYMMDD)	8	M
RFU	38- 3C			O
Authentication Key Map	3D	Variable	512	O
Asymmetric Signature	3E	Variable	2816	M
Error Detection Code	FE	LRC	1	M

Figure 1 PACS v2.3 CHUID Data Model

Federal Agency Smart Credential Number (FASC-N) Data Elements

The CHUID includes the Federal Agency Smart Credential Number (FASC-N), which uniquely identifies the card and cannot be modified post-issuance. Figure 2 "FASC-N" depicts the FASC-N data model as it is defined in NIST SP 800-73-1 and PACS V2.3 specifications.

Field name	Length (BCD digits)	Field description
AGENCY CODE	4	Identifies the government agency issuing the credential (9999 for FiXs)
SYSTEM CODE	4	Identifies the system the card is enrolled in and is unique for each site
CREDENTIAL NUMBER	6	Encoded by the issuing agency. For a given system no duplicate numbers are active
CS	1	CREDENTIAL SERIES (SERIES CODE) Field is available to reflect major system changes
ICI	1	INDIVIDUAL CREDENTIAL ISSUE (CREDENTIAL CODE) Recommend coding as a "1" always
PI	10	PERSON IDENTIFIER Numeric Code used by the identity source to uniquely identify the token carrier. (e.g. DoD EDI PN ID, TWIC credential number, NASA UUPIC)
OC	1	ORGANIZATION CATEGORY 1 - Federal Government Agency 2 - State Government Agency 3 - Commercial Enterprise 4 - Foreign Government (3 for FiXs)
OI	4	ORGANIZATION IDENTIFIER OC=1 – NIST SP800-87 Agency Code OC=2 – State Code OC=3 – Company Code OC=4 – Numeric Country Code (Used to Identify Companies for FiXs)

POA	1	PERSON/ORGANIZATION ASSOCIATION CATEGORY 1 – Employee 2 – Civil 3 – Executive Staff 4 – Uniformed Service 5 – Contractor 6 – Organizational Affiliate 7 – Organizational Beneficiary
SS	1	Start Sentinel. Leading character which is read first when card is swiped
FS	1	Field Separator
ES	1	End Sentinel
LRC	1	Longitudinal Redundancy Character

Figure 2 FASC-N Data Model

FiXs Implementation

Section 2.1 of the PACS Version 2.3 document explains how the CHUID could be used by non-federal issuers. The document states that Federal agencies shall only enroll CHUID credentials that are validated through the issuing agency or where the Agency Code is 9999 indicating the issuer is a non-federal entity.

Because FiXs is not a federal agency, FiXs plans to follow the specification and use the Code “9999” in the AGENCY CODE.

The FASC-N is not designed to insure uniqueness for non-federal issuers. When the FASC-N was originally developed, the entire FASC-N was set to binary coded decimal (all numeric) in order to be backward compatible with the SEIWG-012 number. The FASC-N encoding uses only BCD digits. Since alpha characters cannot be BCD encoded in the FASC-N, this limitation causes scalability issues. Another limitation in the FASC-N is that the OI field only accommodates 4-digits. This limits the number of organization identifiers to 9999 per Organization Category (OC). These limitations were recognized by the developers of the PACS Version 2.2 specification document and specification document that followed, i.e., PACS Version 2.3. This resulted in the addition of three optional fields to the CHUID. These fields have been included in the PIV CHUID described in FIPS 201 and NIST SP 800-73-1. The three optional fields are:

- **Agency Code** -Tag 31: For issuing agencies with alpha characters in their agency code
- **Organization Identifier** -Tag 32: An alphanumeric code that could be used as an extension to the numeric Organization ID (in the FASC-N) on the CHUID
- **Data Universal Numbering System (DUNS)** -Tag 33: For commercial organizations

For non-federal issuers, the optional data elements can extend the FASC-N to create a unique identifier when the Agency Code is encoded with 9999. If an Agency Code of

9999 is present in the FASC-N, then the Agency Code, DUNS, and/or Organization Code TLV records in the CHUID could indicate the identity of the credential issuer. It is anticipated that the FASC-N Tag 30 TLV record will always exist for industry compatibility for PACS that use the System Code and Credential Number as a credential identifier.

The PACS Version 2.3 document also states that for issuers not defined in SP 800-87, *Codes for the Identification of Federal and Federally Assisted Organizations*, the FASC-N can be constructed using an Agency Code of 9999; however this will not provide uniqueness of the FASC-N for federal agency applications. If a non-federal issuer has a requirement for federal interoperability, then a sponsoring agency could assign specific System Code(s) to the issuer. As mentioned above, when an Agency Code of 9999 is specified, a non-federal issuer must include an additional TLV record in the CHUID, such as the Organization Identifier number (Tag32) and/or DUNS number (Tag 33) to ensure uniqueness of the CHUID.

Conclusion

The FiXs system requires two data elements to operate properly. The first data element is the Organization Identifier. The Organization Identifier is used to route information between the FiXs/DCCIS Domain Servers in the FiXs and DCCIS systems. The Organization Identifier functions as a routing address and must be unique for each organization throughout the FiXs/DCCIS system. The second data element is the Person Identifier. The Person Identifier is used to identify a specific person's record within each of the organization's domains. The Person Identifier must be unique within each organization but does not have to be unique across the FiXs/DCCIS domain.

The NIST SP 800-73-1 and PACS Version 2.3 specifications both define a 10 digit Person Identifier in the FASC-N portion of the CHUID. This is more than sufficient to meet the needs of FiXs. FiXs plans to use the Person Identifier as defined in both specifications to uniquely identify persons within an organizational domain.

The FASC-N OI (4 BCD Digits) used to uniquely identify organizations has a size limitation, since it cannot accommodate more than 9999 FiXs credential issuing organizations. This limitation is not an immediate concern. It will become a problem as FiXs grows over the next few years. Therefore, a more robust numbering scheme will be needed once the number of FiXs member organizations exceeds 9999.

The FiXs infrastructure intends to use the FASC-N OI (4 BCD Digits-16 bits) combined with the CHUID OI (4 bytes alpha-numeric-32 bits). This will give FiXs a combined 48 bits from which to build a unique Organization Identification.

FiXs will implement these two data elements by combining them to create a unique 48 bit OI designator across FiXs for each FiXs member as follows:

1. The FASC-N OI will be used to represent the lower sixteen least significant bits (1-9999 BCD). *Note: The FASC-N OI (4 BCD Digits) will be restricted to the numeric digits only.*
2. The CHUID OI would be used to represent the upper thirty-two most significant bits (0000-ZZZZ). *Note: The CHUID OI could include both alpha and numeric characters, but for the initial 1-9999 FiXs members this would be all zeros.*

This method of implementation allows for short-term compatibility and implementation flexibility while providing the largest number of organizational identifier combinations long-term.

A subset of the CHUID information will also be used in the linear 1D barcode located on the rear of the smart card. The bar code specification is shown in Appendix B FiXs Barcode Requirements.

FiXs.org will generate the organizational identification number and ensure they are unique across FiXs on behalf of the DOD DMDC.

The unique FiXs credential identifier can be developed by assigning the following values to the following data elements within the FASC-N and CHUID:

1. Agency Code (within the FASC-N) will be assigned a value, 9999, to indicate that the card has been issued by a non-Federal issuer;
2. System Code (within the FASC-N) can be assigned a unique number ranging between 1 and 9999 to identify the FiXs enrollment and/or issuance system used by a FiXs member organization;
3. Credential Number (within the FASC-N) will be assigned a unique number ranging between 1 and 999,999 to identify the individual credential issued by a particular FiXs enrollment and/or issuance system used by a FiXs member organization;
4. Credential Series (Series Code) - within the FASC-N - can initially be assigned a value, 1, to indicate the first series and incremented up to 9 for additional series;
5. Individual Credential Issue (Credential Code) - within the FASC-N - should always be assigned a value, 1, as recommended by PACS Version 2.3;
6. Person Identifier (within the FASC-N) can be assigned a unique number ranging between 1 and 9,999,999,999 to uniquely identify the FiXs card holder within a specific FiXs member's Domain Server;
7. Organization Category (within the FASC-N) will be assigned a value, 3, to indicated that the card issuer is a commercial organization;
8. Organization Identifier (within the FASC-N) will be assigned a value between 1 and 9999 to identify the lower sixteen bits of the FiXs member's organization identifier;
- Note:** When the number exceeds 9999, the Organization Identifier (in the CHUID) will be combined to identify the FiXs member organization issuing the credential (as described in line item 10 below).
9. Person/Organization Association Category (within the FASC-N) can be assigned a value, 1, 3, 5, 6, or 7 to indicate that the cardholder's relationship with the FiXs member organization; and
10. The Organization Identifier (OI) in the CHUID, which is a 4-byte (32-bit) data element, will be assigned a value between 0000 and ZZZZ to identify the upper thirty-two bits of the FiXs member organization issuing the credential. Until the number of FiXs organizations exceeds 9999, the CHUID OI will be set to 0000 or omitted on systems that can not generate the optional field.

References

1. **Homeland Security Presidential Directive 12 (HSPD-12):** Policy for a Common Identification Standard for Federal Employees and Contractors (August 2004) Mandates the establishment of a standard for identification of Federal government employees and contractors and requires the use of a common identification credential for both logical and physical access to Federally controlled facilities and information systems.
<http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html>
2. **Federal Information Processing Standard (FIPS) 201-1:** Personal Identity Verification (PIV) of Federal Employees and Contractors (June 2006)
<http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf>
3. Government Smart Card Interagency Advisory Board - Physical Access Interagency Interoperability Working Group, "*Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems (PACS), Version 2.3*", December 20, 2005.
4. National Institute of Standards and Technology (NIST), Special Publication (SP) 800-73-1, "*Interfaces for Personal Identity Verification*", March 2006.
5. DMDC, Card Technologies & Identity Solutions Division (CTIS), "*DoD Implementation Guide for Transitional PIV II SP 800-73 v1, Version 1.01*", March 2006.
6. Framework for Inter-Agency Authentication of Federal Personal Identity Verification (PIV) cards, Version 1.0

APPENDIX A

SMART CARD TOPOLOGY REQUIREMENTS

Introduction

The FiXs smart card-based ID card is based upon the minimum standards set forth in the National Institute of Technology & Standards' (NIST) FIPS Pub 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*. The most current version of FIPS 201 was published by the NIST in March, 2006. FIPS 201 lays the groundwork for a commonly-recognized and interoperable federal ID that:

- Is based on sound criteria for verifying an individual's true identity
- Is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation
- Can be rapidly authenticated electronically
- Is issued only by providers whose reliability has been established by an official accreditation process.

Visual Card Topology Requirements

FIPS Pub 201 (4.1.4 Visual Card Topology) lists the requirements for creating a visual layout that meets the requirements of HSPD-12. The smart card's visual topology consists of "zones" that specify where particular information resides, such as the card holder's name, department/agency, the card's expiration date, etc.. Some areas of the card are labeled as "reserved" and should not be used for printing. These areas are off-limits so that printing does not interfere with a card's Integrated Circuit Chip (ICC).

Where the printed text on the PIV card is required to be in Arial font, the point size and style (bold, normal) will alter depending on the zone.

Some flexibility is given during card design to allow organizations to customize certain aspects. These options are explained in FIPS Pub 201 (4.1.4.3, Optional Items on the Front of the Card and 4.1.4.4, Optional Items on the Back of the Card).

Requirements for the Front of the Card

Zone 1 – Photograph

A color photograph (minimum of 300 dots per inch (dpi) resolution), presenting the individual from the top of the head to the shoulders, is to be placed in the upper left corner of the front of the card, vertically. The background (backdrop) color to be used behind the photographed individual is not specified in FIPS 201, but per the recommendation of the Internal Committee for Information Technology Standards (INCITS) 385, the background color should be uniform throughout an organization's issuance locations. Complete and specific technical requirements for facial image capturing should conform to NIST Special Publication (SP) 800-76, *Biometric Data Specification for Personal Identity Verification*.

Zone 2 – Name of Individual

The full legal name of the card holder's identity is to be printed under the photograph in capital letters. The minimum font size acceptable is 10 point.

Zone 8 – Affiliation

The card holder's affiliation shall be printed in Zone 8. Examples include: "CONTRACTOR," "ACTIVE DUTY," and "CIVILIAN." The required font for the card holder's affiliation is 6 point Bold.

Zone 10 – Organization Affiliation

The card holder's organization name shall be printed here. Two lines are available for use, with 6 point Bold being the font requirement.

Zone 14 – Expiration Date

The card expiration date is to be printed in a YYYYMMDD format (example: 2007MAR30). A PIV card may be valid for up to 5 years, depending on your status. The expiration date is to be printed in 6 point Bold.

Requirements for the Back of the Card***Zone 1 – Agency Card Serial Number***

Each card created will be assigned a unique serial number from the agency/organization. This serial number will be required to be printed in 6 point Bold, left-justified.

Zone 2 – Issuer Identification

Printed in 6 point Bold and right-justified will be the issuing facility's information. This identifier will consist of six characters for the department code, four characters for the agency code, and a five-digit number that uniquely identifies the issuing facility within the department or agency.

Durability Requirements

FIPS 201 includes special provisions regarding durability requirements of the smart card. The printed information on the PIV card shall be printed so that the print cannot be rubbed off the actual card material through printing, laminating, and during normal wear and tear throughout the card's life cycle. In addition to this, the print is not to be obscured by any images (example: agency seal should not obscure the agency title).

No decals or stickers of any type are to be affixed to the PIV card. Electronic contact points should also be considered off-limits for printing. Printing on areas designated as "unusable" by FIPS 201 could result in difficulties reading and writing data to the card. No manual markings or embossing (unless done during manufacture of the card itself by the manufacturer) are allowed.

The following standards should be referenced to ensure FIPS 201 compatibility for contactless cards:

- [ISO7810]
- [ISO10373]
- [ISO7816]
- [ISO14443]

In addition to the aforementioned ISO standards, the PIV card must also conform to test methods used in [ANSI322]:

- Card flexure
- Static stress
- Plasticizer exposure
- Impact resistance
- Card structural integrity
- Surface abrasion
- Temperature and humidity-induced dye migration
- Ultraviolet light exposure
- Laundry tests

Requirements set forth from [ISO10373] require that the PIV card be able to withstand up to 2000 hours of southwestern United States sunlight exposure (actual, concentrated, or artificial). Furthermore, the PIV card shall also meet testing requirements in [G90-98] for concentrated sunlight exposure and [G155-00] for accelerated exposure.

Regular cleaning, using a mild soap and water mixture should not cause the PIV card to malfunction, nor should it cause the laminate to peel. No visible cracks or failures should be experienced following dynamic bending per [ISO10373].

Physical Requirements

PIV cards must be 27 to 33-mil thick (prior to lamination). Consideration should be taken to ensure that the lamination itself does not interfere with the operation of the smart card reader. See [ISO7810] for specific details.

Punching holes in PIV cards should be done carefully, and only after consulting with the manufacturer. Printed text and photo areas are off-limits for hole punching, and any zones that feature machine-readable technology are also off-limits. Hole punching may void a card's warranty.

Security Requirements

There are many requirements built into FIPS 201 to ensure the security of a PIV card, from the beginning authorization to issue a PIV card through the end of the card's life cycle (termination). The following list is a minimum of security standards to be followed when implementing PIV:

Security Features

Any security features used on a PIV card must be in accordance with durability requirements in ISO7810. Security features also must be free of defects, such as fading, discoloring, or tampering. Printed information is to be legible and not obscured by any images whatsoever. Electronic contact points are to be free from printing zones, so that data can be read and written without impediment. A PIV card is required to have at least one of the following security features:

- Optical Varying Structures – A security feature that lays a pattern down across a holographic image or diffracted image, creating a surface relief pattern that appears semi-transparent.
- Optical Varying Inks – Known as OVI, optical varying ink utilizes metal luster in which colors actually appear as pairs of colors instead of individualized. The pairs of ink changes as the viewing angle of the object changes. This color angular effect cannot be duplicated by copying machines and scanners. OVI is the most complex anti-forgery ink available today.
- Laser Etching and Engraving – Laser etching/engraving involves marking the PIV card with a low-power laser or reduced-power engraving technique so that the cards can be uniquely marked without damaging or destroying them.
- Holograms – Holograms are three dimensional images that are created by utilizing two laser beams; one for illuminating the object for visibility, and the other directed to the film or background plate.
- Holographic Images – A holographic image is the result of the reconstruction of a wavefront that is identical to the reflection of light from the original object.
- Watermarks – A shaded watermark can be used onto the card, incorporating tonal depth, creating a grayscale image.
- Personal Identification Number - Each PIV card will be assigned a numerical Personal Identification Number (PIN), which will be used to access the data on the smart card. The PIN is to be a minimum of 6 digits, and should only be known by the owner of the card. PIN transactions should always be encrypted, never transmitted in clear text. FIPS 140-2 (Level 3) Operator requirements lists specific details.
- Card Holder Unique Identifier - The Card Holder Unique Identifier (CHUID) is a unique number on every PIV card, which includes an element and the FASC-N. [SP800-73] defines the CHUID, and the format of the CHUID signature element is found in Section 4.2.2 of FIPS 201.
- Biometrics – Two fingerprint samples of the card holder will be stored on the PIV card. These fingerprints can be used during authentication processes. Biometrics are only permitted to be accessed via the contact interface, after valid presentation of the associated PIN.
- Encryption – One asymmetric key pair and corresponding certificate will be included on each PIV card. This will also include the status of the NACI for the individual. Cryptographic operations may be performed with the PIV card, using RSA or elliptical curve key pair generation. These cryptographic transactions are to be performed on the PIV card itself. The PIV

authentication private key is never to be exported off the card, and should only be accessed via the contact interface. Additionally, the utilization of X.509 certificates (including the FASC-N) to support physical access) is included. PIV cryptographic keys must meet Level 2 (or above) of FIPS 140-2 and physical security requirements (to protect keys in storage) must meet Level 3.

APPENDIX B

FIXS BARCODE REQUIREMENTS

Introduction

As described in Appendix A, the FiXs smart card-based ID card is based upon the minimum standards set forth in the National Institute of Technology & Standards' (NIST) FIPS Pub 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*. This FiXs smart card will include a 3 of 9 barcode on the back of card that conforms to the FIPS 201 specification for an optional barcode in Zone 8 as depicted in Figure 4-7 below.

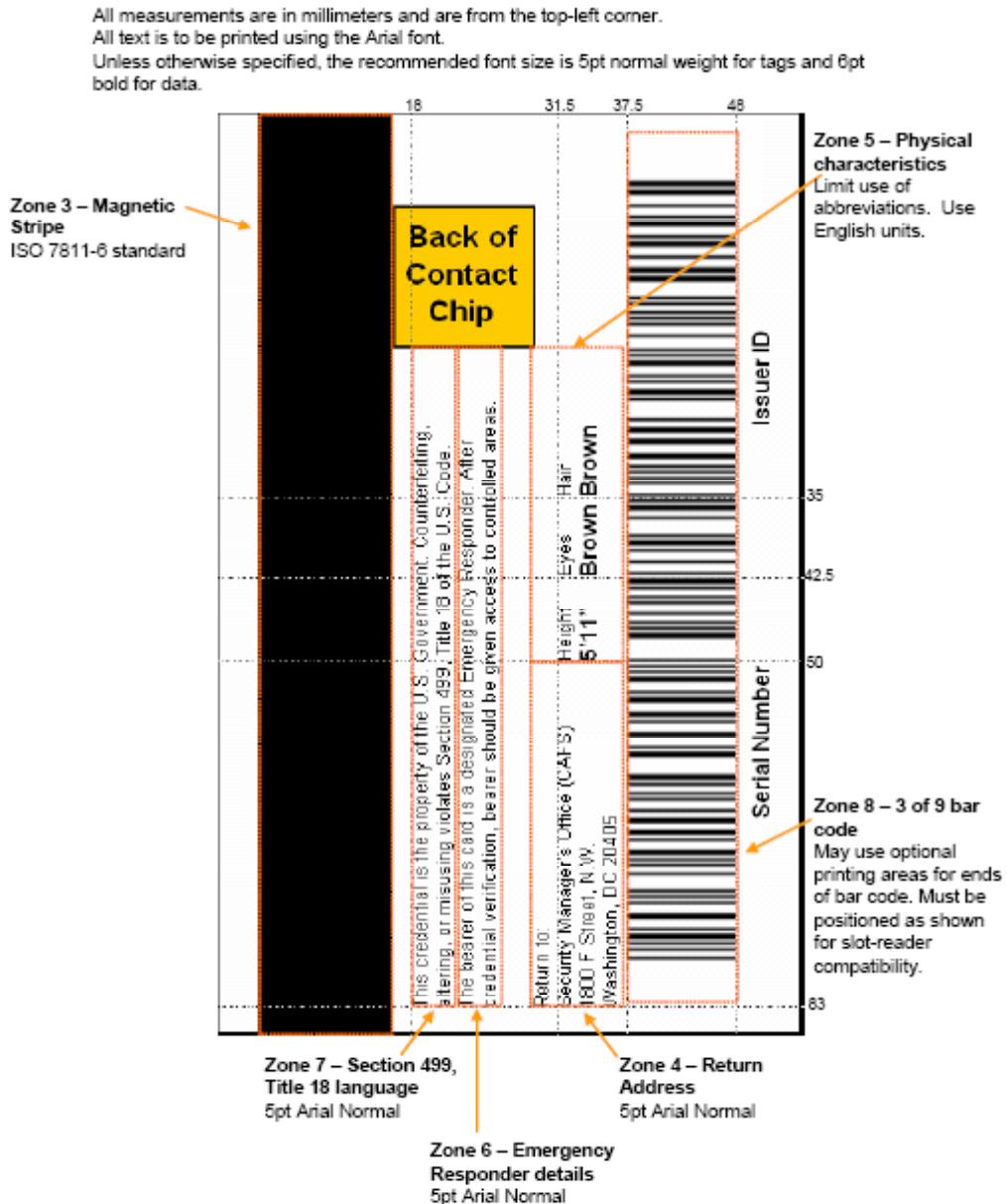


Figure 4-7. Card Back—Optional Data Placement—Example 1

FiXs Barcode Specification:

This FiXs barcode will consist of data elements selected from the CHUID. These data elements and the order in which they will be concatenated are described below:

1. Agency Code (within the FASC-N) will be assigned a value, 9999, to indicate that the card has been issued by a non-Federal issuer;
2. System Code (within the FASC-N) will be assigned a unique number ranging between 1 and 9999 to identify the FiXs enrollment and/or issuance system used by a FiXs member organization;
3. Credential Number (within the FASC-N) will be assigned a unique number ranging between 1 and 999,999 to identify the individual credential issued by a particular FiXs enrollment and/or issuance system used by a FiXs member organization;
4. Credential Series (Series Code) - within the FASC-N - will initially be assigned a value, 1, to indicate the first series and incremented up to 9 for additional series;
5. Individual Credential Issue (Credential Code) - within the FASC-N - should always be assigned a value, 1, as recommended by PACS Version 2.3;
6. Organization Category (within the FASC-N) will be assigned a value, 3, to indicated that the card issuer is a commercial organization;
7. Organization Identifier (within the FASC-N) will be assigned a value between 1 and 9999 to identify the lower sixteen bits of the FiXs member's organization identifier;

An example of a FiXs Barcode consisting of the following sample data is provided in Figure B-2 below:

- FASC-N Agency Code = 9999
- FASC-N System Code = 0001
- FASC-N CN = 123456
- FASC-N CS = 1
- FASC-N ICI = 1
- FASC-N OC = 3
- FASC-N OI = 0001



999900011234561130001

Figure B-2 Sample FiXs Barcode



The Federation for Identity and
Cross-Credentialing Systems®

Version 3.0
September 1, 2010

www.fixs.org

Copyright 2010 by the Federation for Identity and Cross-Credentialing Systems®, Inc.

All Rights Reserved

Printed in the United States of America

10400 Eaton Place, Suite 500A

Fairfax, VA 22030

(703) 591-9255

TABLE OF CONTENTS

1.0 INTRODUCTION	3
1.1 PURPOSE	3
1.2 APPLICABILITY AND SCOPE.....	3
1.3 DEFINITIONS	4
1.4 PROPONENT.....	4
1.5 GENERAL DESCRIPTION OF INFORMATION SENSITIVITY.....	4
2.0 MANAGEMENT CONTROLS	5
2.1 RISK ASSESSMENT AND MANAGEMENT	5
2.2 REVIEW OF SECURITY CONTROLS	6
2.3 RULES OF BEHAVIOR.....	8
2.4 PLANNING FOR SECURITY IN THE LIFE CYCLE.....	9
2.5 REQUIREMENTS TO AUTHORIZE PROCESSING.....	12
3.0 OPERATIONAL CONTROLS	13
3.1 PERSONNEL SECURITY	13
3.2 PHYSICAL AND ENVIRONMENTAL PROTECTION	14
3.3 PRODUCTION, INPUT/OUTPUT CONTROLS	19
3.4 CONTINGENCY PLANNING AND INCIDENT RESPONSE CAPABILITY	19
3.5 HARDWARE AND SYSTEM SOFTWARE MAINTENANCE CONTROLS	21
3.6 INTEGRITY CONTROLS.....	22
3.7 DOCUMENTATION	23
3.8 SECURITY AWARENESS & TRAINING.....	24
3.9 KEY MANAGEMENT BACKUP/RECOVERY	25
4.0 TECHNICAL CONTROLS FOR THE FIXS NETWORK	25
REFERENCES	25
FIXS SECURITY COMPLIANCE ASSESSMENT CHECKLIST	29

1.0 INTRODUCTION

1.1 Purpose

This Guideline:

1. Describes a set of security guidelines and assigns responsibilities to achieve information assurance for identity management to the Participants of FiXS. Policy is based upon and consistent with the amount of risk permitted within a given community and/or group of communities.
2. Designates the FiXS Executive Board responsible for overall management and integration of guidance, operating, and technical documents.

1.2 Applicability and Scope

This Guideline applies to:

1. All Participants of FiXS (hereafter referred to as "Participants"). Participants consist of three major communities, national security, all other government entities, and the commercial sector. This policy does not supersede US Government policies or regulations.
2. All Participant-owned or -controlled information systems that receive, process, store, display or transmit FiXS identity management information, regardless of mission assurance category, classification or sensitivity.
3. Information systems that support special environments, e.g., Special Access Programs (SAP) and Special Access Requirements (SAR), as supplemented by the special needs of the program.
 - Platform IT interconnections, e.g., weapons systems, sensors, medical technologies or utility distribution systems, to external networks.
 - Information systems under contract to the federal government.
 - Outsourced information-based processes such as those supporting e-Business or e-Commerce processes.
 - Stand-alone information systems.
 - Mobile computing devices such as laptops, handhelds, and personal digital assistants operating in either wired or wireless mode, and other information technologies as may be developed.

Nothing in this Guideline shall alter or supersede the existing authorities and policies of the Director of Central Intelligence (DCI) regarding the protection of Sensitive Compartmented Information (SCI) and special access programs for intelligence as directed by Executive Order 12333 (reference Executive Order 12333, *SUBJECT: Information Assurance (IA)*, October 24, 2002) and other laws and regulations. This Guideline does not apply to weapons systems as defined by DoD Directive 5137.1 or other IT components, both hardware and software, that are physically part

of, dedicated to, or essential in real time to a platform's mission performance where there is no platform IT interconnection.

1.3 Definitions

Terms used in this Guideline are defined in National Security Telecommunications and Information Systems Security Instruction Number 4009 or enclosure 2 of Department of Defense Directive 8500.1, Information Assurance and in the FiXs Operating Rules.

The FiXs Network is defined as all of the FiXs compliant systems that operate together as a unit to exchange identification information.

1.4 Proponent

The FiXs Security Committee has overall responsibility for the maintenance of this document and shall:

- Monitor, evaluate and provide advice to the Executive Board regarding all IA activities.
- Oversee appropriations earmarked for the IA program and manage supporting activities.
- Develop and promulgate additional IA policy guidance consistent with these Guidelines.
- Establish metrics and annually validate the IA readiness of all Participants.
- Develop and provide IA training and awareness products.
- Develop and provide security configuration guidance for IA and IA-enabled IT products.
- Develop and implement IA personnel management and skill tracking procedures and processes to ensure adequate personnel resources are available to meet critical IA requirements.
- Monitor information system security practices and conduct regular inspections of Participants processes.

1.5 General Description of Information Sensitivity

1. Information handled within the system includes that contained in Immigration Form I-9, biometrics, photographs, personal identification numbers, employer name, employee number, etc. Much of these data require protection as described in the Privacy Act of 1974.
2. The loss, misuse, or unauthorized access to, or modification of, information within the system ranges from temporary loss of access privileges, to identity theft resulting in financial, property, and/or intellectual property fraud and abuse, to personal harm and/or death, to catastrophic endangerment of national security. These levels of security vary depending on a given environment, nature of use, and local access requirements. Therefore, they do not map, nor should be confused with, OMB's 4 Levels of Assurance.

3. FiXs systems are generally classified as a Mission Assurance Category (MAC) "3", Confidentiality Level "Sensitive" system for the purposes of assigning Information Assurance (IA) Controls to implement. These IA Controls are based on the Department of Defense Instruction 8500.2, "Information Assurance (IA) Implementation", dated February 6, 2003 (DoDI 8500.2).

2.0 MANAGEMENT CONTROLS

2.1 Risk Assessment and Management

2.1.1 Pre-Operation

Prior to becoming an operational Participant in the FiXs Network; a Participant shall have a risk assessment conducted by an independent third-party Assessor. The Participant shall select the Assessor from the list of FiXs authorized and approved certification agents. The Assessor produces the risk assessment based on the results of security controls tested as part of the Certification Phase. In addition, any findings listed as "to be mitigated prior to becoming operational" shall be mitigated, and a Plan of Actions and Milestones (POA&M) shall be completed. The mitigation of the "to be mitigated prior to becoming operational" findings and the plan will be verified by the organization that performed the risk assessment, and that organization will submit the system risk assessment along with the assessment report and POA&M.

2.1.2 Methodology

The risk assessment will be done in accordance with the methodology defined in NIST SP 800-30¹. The risk assessment will include checking for items included as requirements or recommendations in NIST SP 800-26², the FiXs Operating Rules³, and Trust Statement⁴ documents, OMB Circular No. A-130⁵, DoD 5220.22-M⁶, and other items found in current Information Assurance best practices. The result of the risk assessment will be a risk assessment report submitted to the FiXs C&A Committee for review, evaluation, and in preparing a recommendation to the DAA.

The completed report will be considered sensitive and will not be shared with other FiXs Participants without written permission from the assessed organization. It shall be marked "Sensitive but Unclassified" and "The FiXs Executive Board may share the information contained in this document with

¹ NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*

² NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*

³ *FiXs Operating Rules*

⁴ *FiXs Trust Model*

⁵ OMB Circular No. A-130, Appendix III, *Security of Federal Automated Information Resource*

⁶ DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*

the site analyzed for purposes of review and program planning; under no circumstances may any information in this document be shared with the public, other government offices or agencies, other FiXs Participants, or anyone not approved by the assessed organization.”

2.1.3 During Operation

During operation the systems (processes, equipment, facilities, and personnel) shall be reassessed every 3 years or when ever there is a significant change in the systems. In addition, the operating organization shall perform self-assessments using the methodology described above.

2.2 Review of Security Controls

An assessment of an organization’s security controls shall be conducted prior to the initiation of operation within the FiXs Network and every three years thereafter or when there is a significant change in hardware, software, or physical protection. This may be done as a part of the FiXs Certification and Accreditation Process (CAP) or as a separate activity (at the discretion of the FiXs Executive Board). The security control assessment shall be conducted by a FiXs authorized and approved certification agent. In addition, any findings listed as “to be corrected prior to becoming operational” shall be corrected, and a plan for the correction of any other findings shall be completed.

The purpose of the security control assessment is ensure that FiXs member-deployed systems and components meet federal security standards and protection guidelines for identity management information. FiXs requires a standard set of Information Assurance (IA) controls for use in evaluating the security posture of existing and prospective “Member Service Providers” (MSP) and “Credential Issuers”, hereinafter collectively referred to as “Issuers”. These IA controls provide a baseline to evaluate a prospective Issuer for Certification and Accreditation (C&A) purposes. The objective of the C&A process review is the issuance of an Authority to Operate (ATO), or Interim Authority to Operate (IATO) as applicable, with the FiXs Network.

This process will generally follow the DoD 8500.2 IA Controls for a Mission Assurance Category (MAC) III Sensitive System as the basis for IA controls and requirements for a FiXs Issuer. The DoD 8500.2 MAC III Sensitive IA controls cover all of the areas found in the FIPS 200 and the NIST SP800-53A for systems with similar criticality and sensitivity.

There are two sets of controls – the FiXs Information Systems Security Controls Checklist and the PIV Security Controls Checklist. The FiXs Information Systems Security Controls Checklist is based on NIST 800-53A controls, as well as the FiXs Operating Rules and Implementation Guidelines. The PIV Security Controls will be used for systems which contain PIV information and support the issuance of PIV

Cards. It is based on the controls in NIST 800-79-1 and FiXs Operating Rules and Implementation Guidelines.

Guidance for how systems must be configured will be derived from the Defense Information System Agency (DISA) published Security Technical Implementation Guides (STIGs) that are available on the DISA Information Assurance Support Environment website <http://iase.disa.mil/stigs/stig/index.html>. The Issuer and the C&A assessor will also use the compliance checklist for the STIG found at <http://iase.disa.mil/stigs/checklist/index.html> to validate that the IA Controls have been implemented. Examples of the STIGs and checklists are the Windows 2003 Server STIG; Database STIG/checklist; Network STIG/checklist; and Traditional Basic Checklist.

To check operating system security settings, the Issuer and the C&A assessor will use the DISA FSO Gold disk in the scan only mode, and for Microsoft products, the Microsoft Baseline Security Analyzer. The Gold Disk can also be found at the DISA IASE website <http://iase.disa.mil/stigs/SRR/index.html> and the Microsoft Baseline Security Analyzer is found at <http://www.microsoft.com/technet/security/tools/mbsahome.Issuerx>.

The actual STIGs or Checklist(s) used are dependent upon the proposed architecture the prospective Issuer is using; their operating system(s); databases, applications; and overall solution set and architecture.

The rationale for choosing the aforementioned baselines and tools is that they are proven to be effective, commonly applied and available, as well as kept current while providing the broadest coverage for ensuring systems security. An additional benefit of applying these standards is the increased level of trust between organizations such as FiXs and the DoD/DMDC, other government agencies, as well as many commercial concerns because they are well understood by the broader community of interest.

It is recognized that some of the IA controls may prove to be difficult for a commercial entity to implement, such as using the DoD Vulnerability Management system to register their system and manage vulnerabilities. With this in mind FiXs must approach any implementation of IA controls and security guidelines with a common sense approach that takes into account the risk and the cost of compliance. Many of these issues will be based on sound business decisions. Such determinations will need to be made on a situational basis taking into account the overall security risks and business requirements inherent in the specific solution architecture.

The results of the assessment will be considered sensitive and will not be shared with other FiXs Participants without written permission from the assessed organization. It shall be marked "Sensitive but Unclassified" and "The FiXs Executive Board may share the information contained in this document with the site

analyzed for purposes of review and program planning; under no circumstances may any information in this document be shared with the public, other government offices or agencies, other FiXs Participants, or anyone not approved by the assessed organization.”

Following the completion of assessment activities, a security control assessment report will be produced and formatted similar to the assessment report described above. The assessment report will document the findings and provide the results of each assessed security control. Based on the assessment results, the system owner with the assistance of the Assessor will update the System Risk Assessment Report and the POA&M.

Periodic announced and unannounced security audits shall be conducted based on the FICC Recommendations⁷ to ensure that the FiXs Network Participants remain in compliance with the security requirements. These audits may be combined with other types of audits. The type and frequency will be determined by the FiXs Executive Board.

The methodology to be followed for the audits and auditor selection shall include:

- Require all FiXs Participants to have and maintain compliance audits.
- Evaluate and approve independent entities that have the expertise to conduct compliance audits.
- Ensure the independence of the compliance auditor.
- Standardize on a specific compliance audit standard that creates uniform expectations, and enhances the ability to assess the community in a uniform manner.
- All prior audit reports shall be reviewed while conducting any new audits.
- Establish timelines for compliance audits and determine how frequently a compliance audit is required after commencement of services.
-

2.3 Rules of Behavior

The system's rules of behavior located within the FiXs Operating Rules⁸, Implementation Guidelines, and Trust Model.

The rules of behavior are made available to every user prior to receiving access to the system. Each user shall use this set of rules of behavior or develop their own set of rules of behavior (based on the FiXs set) and have it approved by the FiXs Executive Board prior to commencing operation as a part of the FiXs Network.

⁷ Federal Identity Credentialing Committee, Shared Service Provider Subcommittee, *FICC Audit Standards for PKI Shared Service Provider Entities: An Analysis of Requirements and Alternatives*, January 16, 2004

⁸ *FiXs Operating Rules*

The rules of behavior:

- Clearly delineate the responsibilities and expected behavior of all individuals with access to the system;
- State the consequences of inconsistent behavior or noncompliance;
- Include appropriate limits on interconnections to other systems; and
- Are an appendix to the system's security plan.

2.4 Planning for Security in the Life Cycle

FiXs Participants will wish to plan to accomplish specific security requirements during each phase of the security life cycle of their FiXs systems in order to enhance the security of the system. While all Participants may not perform all of the tasks described below, this is provided as a guide of possible security activities during the system's life cycle. The section below was taken from NIST SP 800-64⁹, which describes the tasks in more detail.

2.4.1 Initiation Phase

2.4.1.1 Security Categorization

An organization shall define which of the three levels (i.e., low, moderate, or high) of potential impact will exist on FiXs, their organization, or individuals should there be a breach of security (a loss of confidentiality, integrity, or availability). Security categorization standards assist organizations in making the appropriate selection of security controls for their information systems. FIPS 199¹⁰ and NIST SP 800-60¹¹ provide a guide for this action.

2.4.1.2 Preliminary Risk Assessment

Based on the results in an initial description of the basic security needs of the system, a preliminary risk assessment shall be done to define the threat environment in which the system will operate. NIST SP 800-26 provides a guide for this action.

2.4.2 Development/Acquisition Phase

2.4.2.1 Risk Assessment

Analysis that identifies the protection requirements for the system through a formal risk assessment process. This analysis builds on the initial risk assessment performed during the Initiation Phase, but will be more in-depth and specific.

2.4.2.2 Security Functional Requirements Analysis

⁹ NIST Special Publication 800-64, *Security Considerations in the Information System Development Life Cycle*

¹⁰ Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (DRAFT)

¹¹ NIST Special Publication 800-60, *Guide for Mapping Information and Information Types to Security Objectives and Risk Levels* (DRAFT)

Analysis of organizational specific requirements and any requirement to interface FiXs with internal, organizational systems. This may include the following components:

- System security environment, (i.e., enterprise information security policy and enterprise security architecture)
- Security functional requirements

2.4.2.3 Security Assurance Requirements Analysis

Analysis of requirements that address the activities required and assurance evidence needed to produce the desired level of confidence that the information security within the Participants organizational structure while meeting all FiXs rules and policies, and enable the system to work correctly and effectively. The analysis, based on legal and functional security requirements, will be used as the basis for determining how much and what kinds of assurance are required.

2.4.2.4 Cost Considerations and Reporting

Determines how much of the development, implementation, and operation costs can be attributed to information security over the life cycle of the system. These costs include hardware, software, facilities, personnel, and training.

2.4.2.5 Security Planning

The development of a System Security Plan (SSP) that ensures that, planned or in place, agreed upon security controls is fully documented. The security plan also provides a complete characterization or description of the information system as well as attachments or references to key documents supporting the organization's information security program (e.g., configuration management plan, contingency plan, incident response plan, security awareness and training plan, rules of behavior, risk assessment, security test and evaluation results, system interconnection agreements, security authorizations/accreditations, and plan of action and milestones).

2.4.2.6 Security Control Development

This activity ensures that security controls described in the respective security plans are designed, developed, and implemented. For information systems currently in operation, the security plans may call for the development of additional security controls to supplement the controls already in place or the modification of selected controls that are deemed to be less than effective.

2.4.2.7 Developmental Security Test and Evaluation

Ensures that security controls developed to supplement FiXs are working properly and are effective. Some types of security controls (primarily those controls of a non-technical nature) cannot be tested and evaluated until the

information system is deployed—these controls are typically management and operational controls.

2.4.2.8 Other Planning Components

This activity ensures that all necessary components of the development process are considered when incorporating security into the life cycle. These components include selection of the appropriate contract type (if implementation, maintenance, operation, etc. are selected for the organization's FiXs), participation by all necessary functional groups within an organization, and development and execution of the necessary contracting plans and processes.

2.4.3 Implementation Phase

2.4.3.1 Inspection and Acceptance

This activity ensures that the organization validates and verifies that the functionality described in the specification is included in the implemented system. This also ensures that the deployed system meets applicable federal laws, regulations, policies, guidelines, and standards.

2.4.3.2 Security Control Integration

Ensuring that security controls are integrated at the operational site where the information system is to be deployed for operation. Security control settings and switches are enabled in accordance with vendor instructions and available security implementation guidance.

2.4.3.3 Security Certification

Ensures that the controls are effectively implemented through established verification techniques and procedures and gives organization officials confidence that the appropriate safeguards and countermeasures are in place to protect the organization's information and systems. Security certification also uncovers and describes any known vulnerabilities in the system.

2.4.3.4 Security Accreditation

Provides the necessary authorization for the organization's system to process, store, or transmit information that is required to become a part of the FiXs Network. This authorization is granted by the FiXs Executive Board and is based on the verified effectiveness of security controls to some agreed upon level of assurance and an identified residual risk to organizational assets or operations and the FiXs community.

2.4.3.5 Data Protection Requirements

Determine the requirement for the protection of sensitive data (such as encryption). Ensure the implementation of data protection requirements.

2.4.4 Operation/Maintenance Phase

2.4.4.1 Configuration Management and Control

These activities ensure adequate consideration of the potential security impacts due to specific changes to a system or its surrounding environment. Configuration management and configuration control procedures are critical to establishing an initial baseline of hardware, software, firmware, environment, and personnel components for the system and subsequently controlling and maintaining an accurate inventory of any changes to the system.

2.4.4.2 Continuous Monitoring

This will ensure that controls continue to be effective in their application through periodic testing and evaluation. Security control monitoring (i.e., verifying the continued effectiveness of those controls over time) and reporting the security status of the system to the appropriate organizational and FiXs officials is an essential activity of a comprehensive security program.

2.4.4.3 System Security Plan Updates

If a SSP was developed, it shall be updated whenever there is a change to the system that is documented in the plan. The SSP shall be considered a “living document” that is continually updated as changes occur.

2.4.5 Disposal Phase

2.4.5.1 Information Preservation

This activity ensures that information is retained, as necessary, to conform to current legal requirements and to accommodate future technology changes that may render the current retrieval method obsolete.

2.4.5.2 Hardware and Software Disposal

Ensure that hardware and software is disposed of as directed by organizational and federal policies and laws, the organizational security and information system security officers.

2.4.5.3 Media Sanitization

Ensure that all sensitive data, software, and firmware is deleted, erased, and/or written over as necessary.

2.4.5.4 Data Transfer

Ensure that all organizational and federal policies, laws, regulations, etc. are followed when moving data or programs to another system as well as during archiving, discarding, purging, clearing, overwriting, degaussing, or destroying (memory or media) activities. Ensure that only those with the proper need-to-know and authorization are permitted access to sensitive data even during these activities.

2.5 Requirements to Authorize Processing

Before a new system can become an operational part of the FiXs Network it shall be assessed by a FiXs authorized certifier and approved by the FiXs DAA. The FiXs DAA shall accredit a system (authorize it to process as a part of the FiXs Network) if:

- The operating organization has been accepted as a FiXs Participant.
- The system (equipment, processes, and personnel) has successfully passed a risk assessment (all significant findings mitigated and a plan to mitigate non-significant findings is approved).
- The system (equipment, processes, and personnel) has successfully passed a security controls assessment (all significant findings corrected and a plan to correct non-significant findings is approved). The security controls review may be combined with the risk assessment.
- There is a compliant System Security Plan in place that contains the security policies of the system
- The operating organization has agreed to announced and unannounced audits of their FiXs system (equipment, processes, and personnel).
- The operating organization must pass any audit that is performed or suspend processing until any significant finding from an audit are mitigated or corrected, and a plan to mitigate or correct any non-significant findings is presented to and approved by the FiXs Executive Board or their designated representative.

3.0 OPERATIONAL CONTROLS

3.1 Personnel Security

3.1.1 Definitions and Requirements

Participants of the FiXs organization must designate access permissions and responsibilities to their personnel based on their need for such access in order to fulfill their functional responsibilities as outlined in the FiXs Operating Rules, Section 1.1.

This guideline classifies personnel as Level 4, Level 3 and above, and Level 2.

The following Personnel are considered *Level 4* and shall be subject to additional screening due to their overall control and access to the FiXs system.

- *Program Manager*
- *Domain Technical Administrator*
- *Domain Functional Administrator*

The following personnel are considered *Level 3 and above*, due to their access to enrollment processes and procedures.

- *Facility Domain Administrator*
- *Facility Administrative Enroller*

The following personnel are considered *Level 2* in the FiXs system, due to their low level of access to systems beyond their local Participant facility.

- *Facility Enroller*
- *Facility Verifier*
- *Authentication Station Operator*

Note: The Facility Enroller and Facility Verifier cannot process FiXs card requests at a level higher than the level FiXs card they possess.

3.1.2 Screening

All personnel shall be required to have FiXs compliant background checks of criminal, employment, and financial information. Sensitive personnel shall be subject to routine criminal background checks. Least sensitive personnel shall be subject to screening at the Participants discretion.

1. 3.1.3 Audit Requirements

Each participating organization is responsible for maintaining complete and up-to-date records of events related to their participation in FiXs. It is a requirement that all FiXs transactions have the ability to be re-created from start to finish including records of the personnel performing the transaction. Event logs and transaction audit data will be held for 7 years by each participating organization.

2. Separation of Duties

The identity proofing, registration and issuance process shall adhere to the principle of separation of duties to ensure that no single individual has the capability to issue a credential without the cooperation of another authorized person.

3. Access Controls

Each class of sensitive and least sensitive personnel may access FiXs systems using Role Based Access Control methods. The Program Manager shall be responsible for ensuring the appropriate issuance and revocation of access credentials for Participant personnel, including the immediate revocation of credentials for terminated employees, and the audit of terminated employees FiXs activities where appropriate.

3.2 Physical and Environmental Protection

The requirements for physical protection for the systems (e.g., locks on terminals, physical barriers around the building and processing area, etc.) are presented below.

4. 3.2.1 FiXs Domain Server (FDS)

3.2.1.1 Physical Access:

The FDS shall be:

- Within a building that is protected from unauthorized access by a guard and/or receptionist or an access control system.
- Within a room that has access controlled by a locking mechanism.

3.2.1.2 Fire Safety:

- The building shall be equipped with a fire alarm system, both manual and smoke/heat detectors.
- The room shall be equipped with a fire extinguishing system, wet or dry pipe sprinklers, halon, or equivalent.
- The room shall be equipped with a manual fire extinguisher and instructions for its use.

3.2.1.3 Failure of Supporting Utilities:

The equipment shall be equipped with an Uninterruptible Power Supply for the FDS (may be supplied by the building) that allows the system to operate for a sufficient period for the FDS to be gracefully shut down.

3.2.1.4 Structural Collapse:

There shall be no structural damage or decay to the building.

3.2.1.4.1 Plumbing Leaks:

- There shall be no signs of plumbing leaks in the vicinity of the equipment (ceiling, above the ceiling, walls, floor, or under the floor).
- There shall be no plumbing lines running over, adjacent to, or under the FDS.

.A.4..1.

.A.4..2.3.2.1.4.2 Rings of Security Requirements:

- Definition: A ring of security is a physical or electronic barrier that must be circumvented or passed to get to the operational system and its data.
- The FDS shall have at least 4 rings of security in total (at least 2 physical and 2 electronic). Note: If there is only 1 electronic security barrier, there shall be 3 physical barriers.
- The FDS shall have at least 2 physical rings of security (as described above in “Physical Access.”
- The FDS shall have at least 2 electronic rings of security.

3.2.1.5 Enrollment Workstation

A.4..3.3.2.1.5.1 Physical Access:

The Enrollment Workstation shall be:

- Within a building that is protected from unauthorized access by a guard and/or receptionist or a lock system.
- Within a room that has access controlled by a locking mechanism.

.A.4.4.

.A.4.5.3.2.1.5.2 Fire Safety:

- The building shall be equipped with a fire alarm system, both manual and smoke/heat detectors.
- The room shall be equipped with a fire extinguishing system, wet or dry pipe sprinklers, halon, or equivalent.

.A.4.6.

.A.4.7.3.2.1.5.3 Failure of Supporting Utilities:

It is desirable, but not required that the office be equipped with an UPS for the Enrollment Workstation (may be supplied by the building) that allows the system to operate for a sufficient period for the workstation to be gracefully shut down.

3.2.1.5.4 Structural Collapse:

There shall be no signs of structural damage or decay to the building.

3.2.1.5.5 Plumbing Leaks:

- There shall be no signs of plumbing leaks in the vicinity of the equipment (ceiling, above the ceiling, walls, floor, or under the floor).
- There shall be no plumbing lines running over, adjacent to, or under the Enrollment Workstation.

3.2.1.5.6 Interception of Data:

Any circuits used to transmit unencrypted data shall be secured (in conduit) and checked for tampering on a regular basis.

3.2.1.5.7 Local Authentication:

- Boot or EPROM password that is changed at least every 90 days.
- Username/Password for the local domain that is changed at least every 90 days
- A Trusted Platform Module must be present in compliance with Trusted Computing Group standards, and used for local or PKI authentication where appropriate for the local domain (ref 49).
-

3.2.1.5.8 Rings of Security Requirements:

- Definition: A ring of security is a physical or electronic barrier that must be circumvented or passed to get to the operational system and its data.
- The Enrollment Workstation shall have at least 4 rings of security (at least 2 physical and 2 electronic) in total. Note: If there is only 1 electronic security barrier, there shall be 3 physical barriers.

- The Enrollment Workstation shall have at least 2 physical rings of security (as described above in “Physical Access,” more is always better).
- The Enrollment Workstation shall have at least 1 electronic ring of security.

3.2.1.6 Authentication Workstation

3.2.1.6.1 Physical Access:

The Authentication Workstation shall be:

- Within a building that is protected from unauthorized access by a guard and/or receptionist or a lock system.
- In an area that is under the observation of a guard and/or receptionist during normal working hours.

.A.4..8.

.A.4..9.3.2.1.6.2 Fire Safety:

- The building shall be equipped with a fire alarm system, both manual and smoke/heat detectors.
- The area shall be equipped with a fire extinguishing system, wet or dry pipe sprinklers, or equivalent.

3.2.1.6.3 Failure of Supporting Utilities:

It is desirable, but not required to have an UPS for the Authentication Workstation (may be supplied by the building) that allows the system to operate for a sufficient period for the workstation to be gracefully shut down.

.A.4..10.

.A.4..11. 3.2.1.6.4 Structural Collapse:

There shall be no signs of structural damage or decay to the building.

3.2.1.6.5 Plumbing Leaks:

- There shall be no signs of plumbing leaks in the vicinity of the equipment (ceiling, above the ceiling, walls, floor, or under the floor).
- There shall be no plumbing lines running over, adjacent to, or under the Authentication Workstation.

3.2.1.6.6 Interception of Data:

Any circuits used to transmit unencrypted data shall be secured (in conduit) and checked for tampering on a regular basis.

3.2.1.6.7 Local Authentication:

- Boot or EPROM password that is changed at least every 90 days.
- Username/Password for the local domain that is changed at least every 90 days

- A Trusted Platform Module must be present in compliance with Trusted Computing Group standards, and used for local or PKI authentication where appropriate for the local domain (ref 49).
- .A.4..12.
- .A.4..13. 3.2.1.6.8 Rings of Security Requirements:
- Definition: A ring of security is a physical or electronic barrier that must be circumvented or passed to get to the operational system and its data.
 - The Authentication Workstation shall have at least 3 rings of security (at least 1 physical and 1 electronic) in total. Note: If there is only 1 physical security barrier, there shall be 2 electronic barriers.
 - The Authentication Workstation shall have at least 1 physical rings of security (as described above in “Physical Access.”)
 - The Authentication Workstation shall have at least 1, but preferably 2, electronic rings of security.

5. 3.2.2 FiXs Trust Broker

3.2.2.1 Physical Access:

The FiXs Trust Broker shall be:

- Within a building that is protected from unauthorized access by a guard and/or receptionist or a lock system.
- Within a room that has access controlled by a locking mechanism.

3.2.2.2 Fire Safety:

- The building shall be equipped with a fire alarm system, both manual and smoke/heat detectors.
- The room shall be equipped with a fire extinguishing system, wet or dry pipe sprinklers, halon, or equivalent.
- The room shall be equipped with a manual fire extinguisher and instructions for its use.

3.2.2.3 Failure of Supporting Utilities:

The room shall be equipped with an UPS for the FiXs Trust Broker (may be supplied by the building) that allows the system to operate for at least 2 hours following a power failure.

3.2.2.4 Structural Collapse:

There shall be no signs of structural damage or decay to the building.

3.2.2.5 Plumbing Leaks:

- There shall be no signs of plumbing leaks in the vicinity of the equipment (ceiling, above the ceiling, walls, floor, or under the floor).

- There shall be no plumbing lines running over, adjacent to, or under the FiXs Trust Broker.

3.2.2.6 Interception of Data:

Any circuits used to transmit unencrypted data shall be secured (in conduit) and checked for tampering on a regular basis.

3.2.2.7 Rings of Security Requirements:

- Definition: A ring of security is a physical or electronic barrier that must be circumvented or passed to get to the operational system and its data.
- The FiXs Trust Broker shall have at least 4 rings of security (at least 2 physical and 2 electronic) in total.
- The FDS shall have at least 2 physical rings of security (as described above in "Physical Access.")
- The FDS shall have at least 2 electronic rings of security.

3.3 Production, Input/Output Controls

All input and output from FiXs systems shall involve transactions subject to audit trails.

All FiXs Participants shall establish controls used for the marking, handling, processing, storage, and disposal of input and output information and media, as well as labeling and distribution procedures for the information and media. Such controls shall be consistent, at minimum, with the Privacy Act of 1974, and shall cover the following:

1. Storage/handling of I-9, privacy and release forms.
2. Physical protection of printed or electronic information.
3. Policy and process for ensuring that only authorized users pick up, receive, or deliver input and output information and media.
4. Restricting access to output (reports, back-up media, external storage devices, etc.).
5. Procedures for transporting or mailing media or printed output.
6. Labeling based on sensitivity (e.g., Privacy Act, Proprietary).
7. Media storage vaults and physical document libraries, including environmental protection controls/procedures.
8. Sanitization procedures preparing electronic media for reuse (e.g., overwriting or degaussing).
9. Policies for shredding or other destructive measures for hardcopy media when no longer required or electronic media not intended for reuse.

3.4 Contingency Planning and Incident Response Capability

In the occurrence of a disaster or other situation that interrupts the ability of FiXs' ability to function, it may be necessary to have a recovery/back-up plan and process.

There are two types of recovery/back-up plans: both a Disaster Recovery Plan (DRP) and Continuity of Operations Plan (COOP). It is required that there be both a DRP and a COOP for the FiXs Trust Broker. It is desired, but not required, that FiXs Participants have a DRP and a COOP for their FDS. Having a COOP or DRP for the Authentication or Enrollment Workstation is up to the individual organizations. NIST SP 800-34¹² shall be used as a guide for the development of COOPs and DRPs.

1. Continuity of Operations Plan (COOP) – this is a plan with associated procedures that describes how to continue operations during the period of time that a system is down (for up to 30 days) until recovery of operation is accomplished.
2. Disaster Recovery Plan (DRP) – this is a plan and associated procedures that describes how to recover operation capability at an alternate site (it may also include recovery of capability at the damaged site).
3. Any requirements within COOP or DRP for backup processing that relies on support from another organization (or department within an organization) shall be documented with a formal agreement (Memorandum of Understanding) between the organizations (departments).
4. The COOP or DRP shall include the requirements for documented backup and the backup procedures including frequency (daily, weekly, and monthly) and scope (full, incremental, and differential backup). It is suggested that backup be:
 - a. Daily incremental
 - b. Weekly full
 - c. Monthly full
 - d. With off-site storage of the weekly and monthly backups
 - e. Tapes are rotated so that there are:
 - 2 weeks of daily tapes
 - 2 months of weekly tapes
 - 12 months of monthly tapes
5. Off-site storage of backups and generations of backups shall be kept at a secure facility in a different building than the systems, and preferably a sufficient distance from the systems to avoid a single disaster from damaging both the system and the backups. (But not so far away that it takes an inordinate amount of time to obtain a backup tape when it is needed.)
6. COOPs and DRPs shall be tested on a regular basis. The frequency of testing shall be defined in the plan. The minimum recommended testing frequency is:
 - Annual test that includes actually switching the system to and bringing up the systems at the support facility.

¹² NIST Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems*

- Quarterly desk top tests where the responsible parties talk through the actions required to accomplish the COOP or DRP.
 - It may be possible to combine the tests. In the event of an actual disaster, both plans may have to be implemented.
7. All employees that may be involved in the execution of a COOP or DRP shall be trained in their roles and responsibilities relative to the plans. These same employees shall execute their roles and responsibilities relative to the plans when the plans are tested. New employees with plan responsibilities or roles shall receive plan training as soon as possible.
8. All incidents that affect a FiXs component shall be reported immediately to the Organizational FiXs Program Manager. If the incident has the potential to affect other FiXs components (outside the organization) or the integrity or reliability of the FiXs Network or data, the Organizational FiXs Program Manager shall report the incident to the other FiXs Participants and the Executive Board.
9. Every FiXs Participant shall have an incident handling policy. This policy shall include the recognition and handling of incidents (e.g., what files and logs shall be kept, who to contact, and when). NIST SP 800-61¹³ provides a guide for the development of incident handling policies.
10. Every FiXs Participant shall have policies concerning who receives and responds to alerts/advisories (e.g., vendor patches, exploited vulnerabilities).
11. Every FiXs Participant shall have policies concerning preventative measures that shall be in place (e.g., intrusion detection tools, automated audit logs, periodic penetration testing). As a minimum, every FiXs Participant shall have policies requiring the installation and constant updating/monitoring of Virus Protection software and TripWire (or equivalent) software on the FDS, Authentication Workstation, and Enrollment Workstation.
12. Every FiXs Participant shall notify the other FiXs Participants when ever their FDS will be or is out of service:
 - For more than 30 minutes during normal business hours.
 - For more than 2 hours during non-business hours.

3.5 Hardware and System Software Maintenance Controls

6. 3.5.1 Personnel

The Domain Technical Administrator has direct responsibility for the ongoing maintenance and installation of FiXs System hardware and software. They may perform this work unsupervised, or may delegate such maintenances provided such personnel are directly supervised at all times.

¹³ NIST Special Publication 800-61, *Computer Security Incident Handling Guide*

3.5.2 Emergency Repair and Maintenance

The Domain Technical Administrator may direct that emergency repair or maintenance necessary to meet the uptime requirements outlined in the FiXs Operating Rules. The Domain Technical Administrator is then required to audit the work done within 30 days to ensure system integrity.

3.5.3 Outside Service

Should outside contractors, vendor technicians, or similar personnel be required to perform or assist in hardware or software maintenance, such personnel shall be escorted by Participant personnel at all times, and shall be directly supervised during the actual performance of work. Under no circumstances shall media containing either FiXs software or FiXs data leave their installed locations except under direct and continuous control of the Domain Technical Administrator.

3.5.4 Introduction of New Components

All software or hardware added to an extant FiXs system shall first be tested in a mock environment for 24 hours. During this period, hardware or software components shall be directly tested with their desired functions (bandwidth loading, sample transactions, failure modes, etc.).

3.5.5 Training and Documentation

Any changes to an extant FiXs system, either hardware or software, shall be documented with specific and objective rational for the changes, including cost/benefit analysis and affidavits by the Domain Technical Administrator that such changes will not compromise or degrade the performance of the system. All changes shall be communicated to downstream Participant personnel, preferably with sufficient time to engage in retraining where necessary.

3.6 Integrity Controls

7. 3.6.1 General Requirements

- All systems shall be continuously monitored by FiXs Participant personnel to ensure adequate performance of FiXs tasks.
- All core networks relevant to FiXs operations shall employ commercially reasonable intrusion detection systems.
- All systems shall use commercially reasonable verification systems to detect tampering, errors, and omissions in FiXs processes.
- All systems shall be subject to penetration testing on at least an annual basis, and ideally performed by a third party.
- All clear text transmission protocols (e.g., FTP, Telnet) shall be disabled on any platforms containing FiXs software and supporting applications.

8. 3.6.2 Antivirus/Spyware/Malware

All computers (servers and workstations) connected to the network will have available up to date virus/spyware/malware scanning software for the scanning and removal of suspected viruses. Specifically:

- All computers shall be automatically scanned on a regular basis where possible.
- Scanning software shall be capable of detecting and regularly updating profiles for:
 - Traditional .exe and .com viruses
 - Automated hidden software installations (spyware)
 - The presence, regardless of source, of password compromising systems
- All anti-virus software shall be subscribed to that software vendor's automatic virus signature system.
- No disk that is brought in from outside the FiXs Participant shall be used until it has been scanned on a standalone machine that is used for no other purpose and not connected to the network. The scanning software on this machine shall be manually checked and updated regularly.
- All systems shall be built from original, clean master copies whose write protection has always been in place. Only original master copies shall be used until virus scanning has taken place.
- All diskettes containing executable software (software with .EXE and .COM extensions) shall be write protected wherever possible.
- Shareware shall not to be used; shareware on disk or downloaded from a bulletin board is one of the most common infection sources. If it is absolutely necessary to use shareware it shall be thoroughly scanned before use.
- New commercial software shall be scanned before it is installed as it occasionally contains viruses.
- To enable data to be recovered in the event of a virus outbreak, regular backups will be taken by FiXs Participants.
- Users will be kept informed of current procedures and policies.
- Users will be notified of virus incidents.
- FiXs Participant employees will be held directly accountable for any breaches of the Company's anti-virus policies.
- Anti-virus policies, procedures and software will be reviewed regularly (at least annually).

3.7 Documentation

9. 3.7.1 Initial Documentation

At the time of installation, the Domain Technical Administrator shall document the hardware and software, with specifications, version numbers, and integration notes. Additionally, all policies and procedures with regards to the implementation of the FiXs Operating Rules, approval and access procedures, emergency/contingency plans, and other relevant procedures shall be included.

10. 3.7.2 Access

All security policies and procedures shall be documented in a single location (e.g., binders, a commonly accessible share). All new employees shall be briefed by senior IT personnel on security policies and procedures before accessing any portion of the FiXs system. Any changes to the FiXs Security Guidelines shall be distributed through normal corporate communications channels, and retraining shall occur where needed.

11. 3.7.3 Review

All documentation shall be reviewed at least annually, or in response to any structural or environmental changes to the system. Further, the Program Administrator is responsible for providing any changes in the FiXs Operating Rules, this security policy, or any other relevant FiXs initiated communication to the Domain Technical Administrator so that they may review and update policies and procedures.

3.8 Security Awareness & Training

12. 3.8.1 Preliminary Employment Training

All employees shall undergo thorough training for their designated role in the FiXs system. Such training shall include a detailed briefing on the security procedures in place to ensure the integrity of both the Participant's facilities, and the data used and collected by the system. Employees shall undergo formal testing of their understanding of these procedures before assuming the responsibilities for which they have been trained.

13. 3.8.2 Hands-on training

Before operating any component of the FiXs system unsupervised, each employee shall be paired with an existing employee, where possible, or under direct supervision from their superior, for a minimum of 8 hours. Part of hands-on training shall be the simulation of various system failures and unusual circumstances designed to test the trainee's knowledge of security procedures.

14. 3.8.3 Currency

All FiXs system personnel shall be required to attend at least one retraining session (in-house, industry seminar, or additional on-the job training). Such sessions, their content, and their frequency are at the discretion of the Program Manager

15. 3.8.4 Ongoing Education

The Program Manager is responsible for implementing an ongoing program to reinforce the messages of Security Awareness and Training. Traditional employee training methods (posters, brown bag lunches, seminars, events, etc.) shall be employed on a periodic basis and the Program Manager's discretion.

16. 3.8.5 Help Desk

FiXs Participants shall establish a help desk for employee questions, reporting of technical problems, and general issues.

17. 3.8.6 Content

While the primary focus of FiXs security training should be those areas that impact FiXs systems directly, these requirements shall be part of the Participant's overall security training program. Such programs shall include:

- Password policies
- Date encryption and key management
- Privacy policies
- Data preservation and destruction policies
- Social engineering prevention
- Antivirus policies and procedures
- Laptop security
- Security event communication protocols

3.9 Key Management Backup/Recovery

18. 3.9.1 Architecture

FiXs architecture should make use of a FiXs approved Security Solution, using Hardware Security Modules (HSMs) and Trusted Platform Modules (TPMs) for key storage or better, ensuring that strong hardware based authentication of the platforms is used to the greatest extent possible.

19. 3.9.2 Affected Platforms

Relevant platforms include, but are not limited to:

Enrollment stations
Authentication stations
FiXs Domain Servers
FiXs Trust Broker

20. 3.9.3 Use of Keys and Backup

All data generated and stored on these platforms shall be encrypted, with corresponding keys stored in compliance with DCCIS Software Specification 2.0. Keys shall be backed up to external servers securely using secure SSL. The servers shall have access to a domain management system (e.g., active directory) and keys stored on HSMs. (See IV D.) Keys shall be recoverable with minimal disruption and effort. Keys shall be migratable to replacement hardware with approval and key authorization of the Domain Technical Administrator.

4.0 TECHNICAL CONTROLS FOR THE FiXs NETWORK

FiXs-based identities and credentials shall be used exclusively for the purposes of FiXs-based systems and applications. Any identities and/or credentials that are presented, displayed and/or transmitted shall not be used, copied, duplicated or deleted for any other purposes. Such use is considered a misuse and violation of the terms of the FiXs agreements.

No FiXs-based identities and/or credentials shall be transmitted unless explicitly solicited by a valid authentication client, FDS server, and/or FiXs Trust Broker and DoD Trust Gateway Broker (TGB) router.

The technical controls for the FiXs Network have been developed from NIST SP 800-26, NIST SP 800-53, NIST SP 800-64, NIST SP 800-73, DOD 8500.1, DODI 8500.2, FiXs Operating Rules, FiXs Trust Model, FiXs Certification and Accreditation Process Document, and FiXs Security Guidelines.

REFERENCES

The policies, laws, regulations, directives, etc. that affect this system include, but are not limited to:

- NIST Special Publications.
 1. NIST Special Publication 800-12, *An Introduction to Computer Security - The NIST Handbook*
 2. NIST Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*
 3. NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*

4. NIST Special Publication 800-26, *Security Self -Assessment Guide for Information Technology Systems*
 5. NIST Special Publication 800-27, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*
 6. NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*
 7. NIST Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems*
 8. NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information System*
 9. NIST Special Publication 800-41, *Guidelines for Firewalls and Firewall Policy*, January, 2002
 10. NIST Special Publication 800-42, *Guideline on Network Security Testing*
 11. NIST Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*
 12. NIST Special Publication 800-53 (Final Public Draft), *Recommended Security Controls for Federal Information Systems*, January 26, 2005
 13. NIST Special Publication 800-53A, *Techniques and Procedures for Verifying the Effectiveness of Security Controls in Federal Information Systems* (DRAFT)
 14. NIST Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*
 15. NIST Special Publication 800-60, Initial Public Draft, Version 1.0, *Guide for Mapping Types of Information and Information Systems to Security Categories*, December, 2003
 16. NIST Special Publication 800-61, *Computer Security Incident Handling Guide*
 17. NIST Special Publication 800-64, *Security Considerations in the Information System Development Life Cycle*
 18. NIST Special Publication 800-73, *Interfaces for Personal Identity Verification (PIV)* (DRAFT)
 19. NIST Special Publication 800-76, *Biometric Data Specification for Personal Identity Verification (PIV)* (DRAFT)
 20. NIST Special Publication 80-68, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals*
- FIPS Documents
 21. Federal Information Processing Standards (FIPS) PUB 73, *Guidelines for Security of Computer Applications*
 22. FIPS Pub 112, *Password Usage and*
 23. FIPS Pub 180-1, *Secure Hash Standard*
 24. *FIPS 181, Automated Password Generator*
 25. FIPS Pub 186, *Digital Signature Standard*
 26. FIPS Pub 199, *Standards for Security Categorization of Federal Information and Information Systems*

27. Federal Information Processing Standards (FIPS) Publication 201

- DoD Documents
 - 28. DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOL)*
 - 29. DoD 8500.1, *Information Assurance*
 - 30. DoD 8510.1-M, *Information Technology Security Certification and Accreditation Process (DITSCAP)*
- DISA Documents
 - 31. DISA Instruction 630-230-19, *Information Systems Security Program*
 - 32. DISA, *Security Technical Implementation Guides (STIGs) and Checklists*, <http://csrc.nist.gov/pcig/cig.html>
- OMB Documents
 - 33. OMB Circular No. A-130, Appendix III, *Security of Federal Automated Information Resources*
- DCCIS Documents
 - 34. *FiXs/DCIS Operating Rules, Version 5.4*
 - 35. *FiXs/DCIS Policy Document, Version 2.0*
 - 36. *FiXs/DCIS Trust Statement, Version 1.0*
 - 37. *FiXs/DCIS Technical Architecture and Specifications, Version 1.1*
- Other Documents
 - 38. Federal Identity Credentialing Committee, Shared Service Provider Subcommittee, *FICC Audit Standards for PKI Shared Service Provider Entities: An Analysis of Requirements and Alternatives*, January 16, 2004
 - 39. Executive Order 12333, SUBJECT: *Information Assurance (IA)*, October 24, 2002
 - 40. National Security Telecommunications and Information Systems Security Instruction Number 4009
 - 41. NSA, Security Recommendation Guides
 - 42. Computer Fraud and Abuse Act
 - 43. Computer Security Act of 1987
 - 44. Information Technology Management Reform Act of 1996
 - 45. Government Information Security Reform Act
 - 46. Federal Information Security Management Act
 - 47. Privacy Act of 1974, amended
 - 48. Electronic Communications Privacy Act, Public Law 99-508, 1986
 - 49. Trusted Computing Group Architecture Overview
 - 50. Windows 2003/XP/2000 Addendum Version 5, Release 1 Developed by DISA for the DOD

FiXs SECURITY COMPLIANCE ASSESSMENT CHECKLIST

The checklist in this section is a compilation of information assurance controls and risk and vulnerability assessment statement that have been developed from NIST SP 800-26, NIST SP 800-53, DOD 8500.1, DODI 8500.2, FiXs Operating Rules, FiXs Trust Model, FiXs Certification and Accreditation Process, and FiXs Security Guidelines. The table below provides a crosswalk between the DoDI 8500.2 IA controls and the FIPS 200 guidance. This has been done to provide assurances to the FiXs members, service providers, issuers and relying parties that FiXs systems have been assessed to meet both DoD, Federal, and commercial best practices in the area of security and information assurance.

This checklist is included for convenience only and is subject to change at the discretion of FiXs. Members and potential members should contact the FiXs executive board for updated Assessment procedures.

The FiXs Baseline Security Assessment Checklist is located in Appendix D of the FiXs Certification and Accreditation Process document:

http://www.fixs.org/Websites/fixs/Images/FiXs%20CAP%20V.%201.1%2015%20Sept%202008_ALL.pdf



The Federation for Identity and
Cross-Credentialing Systems®

FiXS Trusted Broker (FTB) Gateway: Operating and Interface Specification and Statement of Objectives

August 22, 2008

Final 1.0

Copyright 2008© by the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXS®)

All Rights Reserved

10400 Eaton Place, Suite 500A

Fairfax, VA 22030

(703) 591-9255

Preface

The charter of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs) is to promulgate the necessary technical and operational standards; implement the governance and trust models; provide an open communications forum; and maintain non-attributable, objective oversight of the operations of a network “switch” whereby the commercial sector and public sector organizations can securely authenticate identity credentials among and between themselves (cross-credential).

FiXs provides a trusted mechanism for federated identity infrastructure within and between public and private sector organizations with accuracy and trust through the application of a Federated Trust Model. The network capabilities can be accessed worldwide, in remote or fixed environments, wired or wirelessly, and in real-time. A key component to the network integrity is its strong credential authentication and revocation processes, as governed by the FiXs operating rules.

The FiXs Trusted Broker (FTB) has an interface to the Department of Defense’s Defense Cross-Credentialing Identification System (DCCIS) and its’ related Trusted Gateway Broker (TGB) as well as potential interface connections to other Trust Broker’s that may be established in conjunction with the FiXs Network. The FiXs Trust Broker also has interfaces with the FiXs Domain Server(s) (FDS) and authentication systems.

The purpose of the network is to route and process authentication inquiries from networked authentication devices across the FiXs Network, and where applicable to the DCCIS, to the authoritative data store, or domain server, and return an authentication response.

Modeled after the financial industry’s highly-secure and widely-accepted ATM (Automated Teller Machine) approach, the FiXs network is a secure, scalable system that provides trusted, interoperable identity verification and credential authentication for network users accessing a range of government and commercial facilities. The FiXs network meets federally-mandated requirements, supports physical and logical access applications and integrates with an organization’s existing personnel system, while leveraging the network’s economies of scale.

Revision History

This guide will be upgraded periodically as needed. Please make sure you have the latest version of this guide and that the guide is compatible with the version of software being used. Updated versions of this guide are available from FiXs.

Version	Release Date	Description
0.3	2-22-08	Initial Draft Release (compatible with the DoD TGB release 0.3)
0.4	3-17-08	CCB Revision 1
1.0	3-20-08	Board of Directors Version CCB Revision 2 - Draft for Comment
2.0	5-15-08	Board of Directors Approved Version CCB Revision 3 - Posted for Comment
3.0	8-22-08	FiXs Officers Approved Version Final 1.0

Contents

1.0	About This Specification	1
2.0	Statement of Objectives.....	1
3.0	FiXs Overview – Key Components and Architecture.....	2
3.1	FiXs SECURITY	2
3.2	COMPLIANCE WITH FiXs POLICIES, STANDARDS, AND GOVERNANCE.....	2
3.3	ARCHITECTURAL OVERVIEW.....	2
4.0	Requirements	4
4.1	TRUST GATEWAY BROKER (TGB) REQUIREMENTS.....	4
4.2	SECURITY REQUIREMENTS	5
4.3	IMPLEMENTATION REQUIREMENTS	5
4.4	DATA REQUIREMENTS.....	5
4.5	REFERENCE STANDARDS.....	6
5.0	FTB Service Level Requirements.....	7
6.0	Schemas.....	9
6.1	CONTROL DATA SCHEMA DEFINITION	9
6.2	ENVELOPE SCHEMA DEFINITION	14
6.3	PAYLOAD SCHEMA DEFINITION	16
7.0	Glossary	19

1.0 About This Specification

The FiXs Trusted Broker (FTB) and Interface Specification is designed as an aid for FiXs users, developers and service providers by providing specifications that will allow operation of the FTB and integration of FiXs Domain Servers with the FTB. This guide also supports the on-going configuration baseline and requirements/specifications for operating the FTB. This guide is updated by the FiXs CCB under the auspices of the FiXs Executive Committee and the FiXs Board of Directors as specified in the FiXs By-Laws.

The information in this guide is effective at the time it was written and may change under the direction of the CCB with minimum notice. By providing the requirements and interface specifications for the FTB along with the Service Level Agreements required by FiXs, this document will serve as a Statement of Work for any organization seeking to contract for operation of the FTB and the associated network.

2.0 Statement of Objectives

This guide will also be used to serve as a statement of objectives for the solicitation for a service provider to operate and maintain the FTB. As a statement of objectives this document has two functions – to provide those specifications required for the operation of the FTB within the FiXs operating environment as well as those minimum requirements that must be met to ensure that FiXs members receive a high level of service and one that can be relied upon commensurate with the importance of function the FiXs Federation was set up to perform – real time Federated credential authentication. However, as a statement of objectives these specifications and requirements are meant to be at a higher level as may be necessary to totally instantiate the network. This is done for two reasons – first to encourage innovation and efficiency by our service provider and second to allow the service provider to specify the operating system and operating environment most efficient for their bid. Since this specification is a statement of objectives, the winning service provider is expected to provide to the FiXs Board of Directors very specific information on how the service provider intends to meet the requirements stated in Section 4 of this document and the service levels they will provide in each of the areas called out in Section 5 of this document.

In addition, service providers responding to the solicitation to operate the FTB will have to follow the acquisition process specified by the FiXs Board of Directors. The details of the acquisition process to be followed, the make up of the evaluation team and the evaluation criteria are detailed in the FiXs® Trust Broker (FTB) Acquisition Plan which is posted on the FiXs® website and meant to be used in conjunction with this statement of objectives.

3.0 FiXs Overview – Key Components and Architecture

The FiXs Trusted Broker (FTB) and the FiXs Domain Server (FDS) are the key components in the implementation of the FiXs network. The FDS provides access to different FiXs member organization databases, making it possible for them to authenticate visitors carrying authorized FiXs Certified credentials issued by fellow FiXs member organizations or the exchange of such information with FiXs authorized partner organizations such as the Department of Defense (DoD) through the FTB.

FiXs members communicate with other members or other FTBs using XML. The XML message is passed from the source FiXs partner through a FTB to other connected applications. The receiving applications are responsible for deciphering and acting on the information contained in the XML message. This XML message and its schema represent the interface between each member in the FiXs network. It is the responsibility of these applications to encrypt and decrypt the information before passing the data to other partners.

3.1 FiXs Security

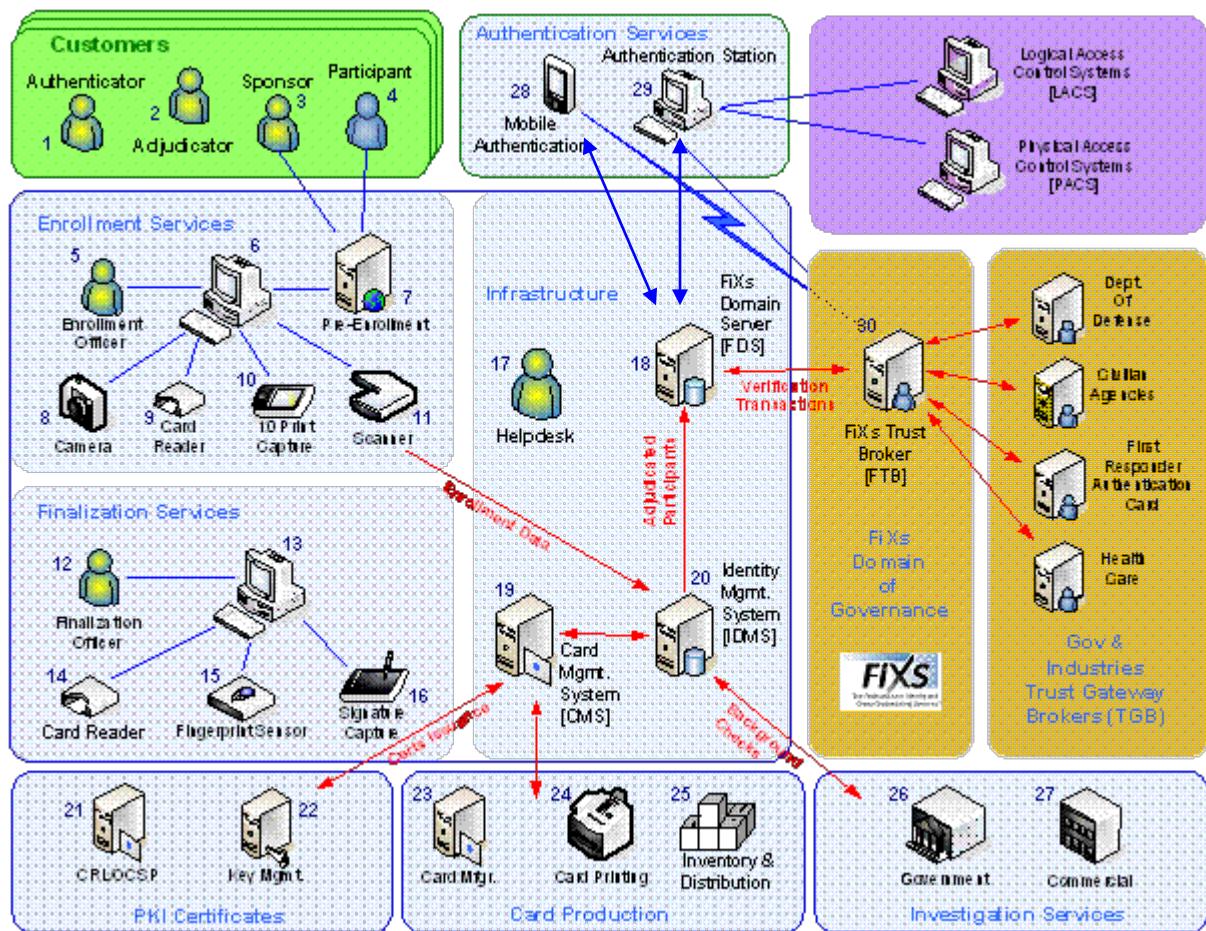
FiXs adheres to its own security principles published in the “FiXs Security Guidelines v2.0 3.29.07” for the transmission of private information over open networks. This includes the need to maintain confidentiality, the need to ensure data integrity, the need to guarantee that information to be sent cannot be repudiated, and that all entities involved in communications, either human agent or machine, are authenticated.

3.2 Compliance with FiXs Policies, Standards, and Governance

All services provided hereunder shall at all times comply with all FiXs Policies, Standards, specifications, governance requirements, and management directives. Should there be any real or apparent conflicts between any of those requirements and the requirements under this SOW, the former shall take precedence.

3.3 Architectural Overview

This section provides a high-level overview of the FiXs Network and its related components and interfaces. The diagram below facilitates the understanding of the workflows in the FiXs network and the technical architecture that drives the requirements in this document for the FTB.



The basic key components of the architecture are:

Enrollment and Issuance Workstation(s): An Enrollment and Issuance Workstation consists of a PC with a standard web browser which is used to access the web-based enrollment application. An enrollment and issuance workstation also includes peripheral devices such as a fingerprint reader, camera, barcode reader, card production equipment.

Authentication Station: The desktop authentication station allows credential holders to be authenticated across the FiXs Network and to the DOD DEERS database for government employees.

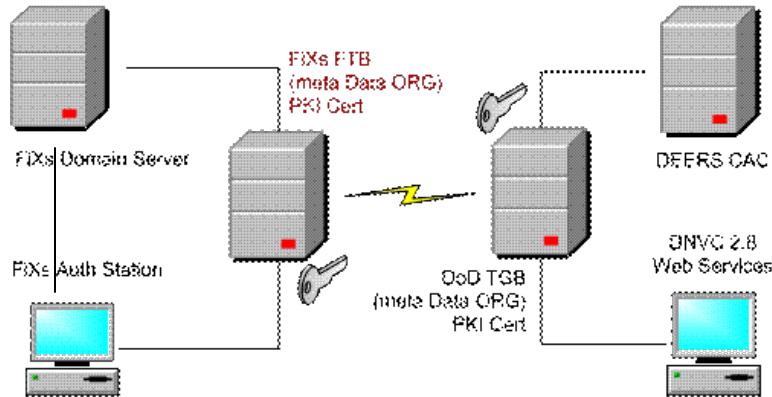
Handheld Authentication Device/Authentication Workstation: Enrolled contractors credentials may also be authenticated via a FiXs-certified handheld device or FiXs-certified mobile authentication device.

Wireless Hubs: At locations where handheld devices are used, a wireless hub will be installed so that the handheld authentication devices can communicate to the backend devices.

FiXs Domain Server (FDS): A FiXs Domain Server is maintained for each unique organization whose employees are enrolled. A single FDS may be properly partitioned to maintain enrollment

data on multiple organizations in a secure logical manner. The FDS maintains a repository of contractors' enrollees' information associated with each organization.

Trusted Gateway Broker (TGB): The Trusted Gateway Broker, or FiXs Trust Broker (FTB) facilitates communication between FDS servers and authentication stations and routes validation and authentication requests to the appropriate FiXs Domain Server or DCCIS domain server and FiXs and DoD National Visitors Center (DNVC) authentication stations as well as interfaces with the DoD's Trusted Gateway Broker.



4.0 Requirements

4.1 FiXs Trust Broker (FTB) Requirements

- 1) The FTB sends out system control data to domain servers that submit a control data request.
- 2) The FTB pushes out system control data to domain servers when the FTB re-starts.
- 3) The system control data contains information in two sections: the FiXs organization, and the Government partners. It includes the public keys of each organization on the list.
- 4) Every time the FiXs FTB re-starts, it generates an updated control data file by updating the FiXs section of the system control data, and merges it with the existing Government partners' control data. It does not modify the Government partners' information.
- 5) The FTB periodically checks the heart beat of domain servers. The FTB will give up on contacting a domain server after three failed attempts.
- 6) The FTB acts like a router, by passing but not deciphering data.
- 7) The FiXs FTB has the ability to communicate with multiple TGBs and domain servers within the government community or commercial networks.
- 8) The FiXs FTB is the central point of contact in communications with the DoD TGB.
- 9) The FiXs FTB runs on an RDBMS server such as Oracle.
- 10) The FTB will support both https and http (internal only) connections.
- 11) The FTB maintains and uses a metadata table for organization codes for commercial and government organizations.

-
- 12) The application shall be based on a single code base upon which advancements, modifications, and additions may more easily be executed.
 - 13) The FTB documentation will be provided as part of the baseline configuration. Any changes shall conform the policies of the FiXs Configuration Control Board and be fully documented as a modification to the baseline configuration documentation.
 - 14) The FTB shall be supplied with “Web Logs” to monitor system performance
 - 15) The FTB shall be supplied with “sniffer” capability to isolate transaction protocols.
 - 16) The FTB shall be equipped with appropriate load-generating capability for usage planning purposes.
 - 17) The FTB shall be equipped with an automated error (alarm) and email generation system and email alerts must be generated to system administrators for any event that impairs the full functionality of the FiXs network.
 - 18) The FTB shall be programmable using a standard web interface with appropriate tools designed to make the application flexible and user friendly.

4.2 Security Requirements

- 1) FTB in the system uses secure communication channels to ensure confidentiality.
- 2) The source domain servers encrypt the message payload in such a way that it can only be read by the destination domain servers.
- 3) The destination domain servers validate the integrity of the message payload received from the source domain servers.
- 4) The destination domain servers ensure non-repudiation of the message payload received from the source domain servers. The domain servers validate the integrity of the overall message sent by the FTB, and the FTB validates the overall messages sent by the domain servers.
- 5) The domain servers ensure non-repudiation of the overall message sent by the FTB, and the FTB ensures non-repudiation of the overall messages sent by the domain servers.
- 6) The domain server and FTB each have their own digital certificates (public keys) and private keys used for SSL, digital signatures, and encryption.
- 7) All digital certificates used for SSL, digital signatures, and encryption must be issued by a single authorized Certificate Authority (CA).
- 8) The FiXs FTB has two digital certificates, one for SSL, and the other for digital signatures and encryption.
- 9) Each domain server that connects to the FiXs FTB has a signature certificate for digital signatures. It will not require the SSL certificate if it is in the CA trust chain.

4.3 Implementation Requirements

- 1) The main system interface is a web based application accessible through a web browser.

4.4 Data Requirements

- 1) The FTB stores a copy of every domain server’s public key certificate, its own private key, and its own X.509 certificate.

-
- 2) Each domain server stores a copy of the FTBs public key certificate, its own private key, and its own X.509 certificate.

4.5 Reference Standards

Consistent with FiXs Security Guidelines, Version 2.0, dated 29 March 2007, the FTB must be flexible enough to incorporate the standards and policies of:

- 3.5.1 The General Services Administration eAuthentication
- 3.5.2 The Liberty Alliance
- 3.5.3 The Standards, Regulations and Policies of State and Local Governments who utilize the FiXs Network
- 3.5.4 The Standards, Regulations and Policies of Commercial Interests who utilize the FiXs Network
- 3.5.5 The Standards, Regulations and Policies of Foreign Entities, Government and Commercial, who utilize the FiXs Network

5.0 FTB Service Level Requirements

The general level of service, Standard, and Acceptable Level of Quality shall be established for each FTB service level requirement. When a Requirement is listed as mandatory, there is no specific Acceptable Level of Quality other than compliance.

FTB Service Metrics

Requirement	Standard	Metric
FTB Service Availability	99.99%	$Availability = \frac{Uptime}{Uptime + Unplanned\ Downtime}$
Time to Restore	Less than 2 hours	Time to restore shall be calculated based on the initial log discovery of the outage plus the actual time evolved until system restoration. An exact representation of measures taken and critical obstacles (incorrect information from an adjoined FiXs Domain) shall be maintained as a matter of record.
FTB Routing Accuracy	99.99%	$Accuracy = \frac{Total\ Transactions}{Total\ Transactions + Erroneous\ Routing\ Attempts}$ An automated feature shall record as an error any attempt to misroute control data. Problem Identification and remediation must be recorded as a matter of record.
FTB Throughput and Response	2 Sec for Authentication 5 Sec for Biometric	The FTB must be capable of timely response even with a high level of network activity. The FTB configuration must be capable of transparently adding routing capability. A minimum capability of 50 transactions per second must be present at IOC. The standard applies to the time from authentication station entry to full response at the authentication station.
FTB Network Monitoring	99.9%	$Monitoring = \frac{Restarts}{Restarts + Failed\ Control\ Data\ Exchange}$ On restart, the FTB shall generate control data to connected Domain Servers and the Brokers of other Connected Federations. Failures of this exchange must generate an alarm and email notification to the Network Manager.
FTB Domain Connections	99.99%	After three failed attempts to contact any FiXs Domain Server, the FTB must alarm and generate an email

		notification to the network manager.
FTB COOP capability	99.9%	FTB Coop capability will be supplied by FiXs for disaster recovery. Contractor responsible for meeting availability requirement and throughput and response requirement
Planned Downtime	Mandatory	Planned downtime for system maintenance may not exceed 2 hours in any week.

6.0 Schemas

6.1 Control Data Schema Definition

Element	Attribute	Type	Description
ControlDataDateTime		dateTime	The timestamp of the current Control Data Table
Category			The grouping of DDSs into Federal, State, Commercial, or Foreign Government categories. There are a maximum of four categories.
	CategoryName	String	Valid Values: <ul style="list-style-type: none">• Federal Government Agency• State Government Agency• Commercial Enterprise• Foreign Government
	CategoryCode	String	Valid Values: <ul style="list-style-type: none">• 01 (Federal Government Agency)• 02 (State Government Agency)• 03 (Commercial Enterprise)• 04 (Foreign Government)
TGB			The list of TGBs under a category.
	TGBName	String	The Trust Gateway Broker name.
	TGBCode	String	The Trust Gateway Broker code.
Attributes (TGB)			
	EnableEncryption	Boolean	True if this TGB can process encrypted data.

Element	Attribute	Type	Description
	PrimeInCategory	Boolean	True if this TGB is the prime repository for the meta data in its category (this TGB is responsible for maintaining all data for the Commercial Enterprise).
	EnableAdvancedCompression	Boolean	True if this TGB can use advanced compression techniques.
PublicKey (TGB)			The public key of the Digital Certificate that was issued to this TGB.
	Algorithm	String	The standard algorithm name for this (Public) key. (RSA, DSA, etc.)
	Format	String	The name of the primary encoding format of this key. (e.g. RAW, SunX509
DDS			The list of DDSs that belong to a TGB.
	DDSSName	String	The DCCIS Domain Server name.
	DDSCode	String	The Unique DCCIS Domain Server code.
Attributes (DDS)			
	EnableEncryption	Boolean	True if this DDS can process encrypted data.
	UseMinutiae	Boolean	True if this DDS can accept fingerprint templates in the industry standard format.
	EnableAdvancedCompression	Boolean	True if this DDS can use advanced compression techniques.
PublicKey (DDS)			The public key of the Digital Certificate that was issued to this DDS.

Element	Attribute	Type	Description
	Algorithm	String	The standard algorithm name for this (Public) key. (RSA, DSA, etc.)
	Format	String	The name of the primary encoding format of this key. (e.g. RAW, SunX509)
Organizations			A list of organizations that belong to this DDS.
	OrganizationName	String	The Organization Name. Must be unique across the entire DCCIS Domain.
	OrganizationCode	String	The Organization Code. Must be unique within the DDS Domain.
Associations			

Element	Attribute	Type	Description
	AssociationName	String	<p>The person's association to the organization.</p> <p>Valid Values:</p> <ul style="list-style-type: none"> • Employee (e.g., hourly or salaried employee) • Government Civil (state or federal government workers, appropriated and non-appropriated fund) • Government Executive Staff or Appointee (includes (SES)) • Uniformed Service (includes active duty, guard and reserve) • Contractor (i.e., contracting to identifying organization) • Organizational Affiliate (those affiliated based on work environment or location, for DoD includes Foreign National, Foreign Military and members of other government agencies working at DoD sites) • Organizational Beneficiary (those whose association only involves receiving benefits from the organization, for DoD this would be family members, retirees, DAV, etc.)

Element	Attribute	Type	Description
Associations (Continued)			<p>Valid Values</p> <ul style="list-style-type: none"> • Employee • Civil • Political Appointee/SES • Uniform Service • Contractor • Affiliate • Beneficiary
	AssociationCode	String	<p>The person's association (code) to the organization.</p> <p>Valid Values:</p> <ul style="list-style-type: none"> • 00 - Employee • 01 - Civil • 02 - Political Appointee/SES • 03 - Uniform Service • 04 - Contractor • 05 – Affiliate • 06 - Beneficiary
Tokens			
	TokenName	String	<p>The name of the token accepted by an Organization.</p> <p>Valid values:</p> <ul style="list-style-type: none"> • Employee Identifier • Bar Code • CAC Card
	TokenCode	String	<p>The token code accepted by an Organization. Valid values:</p> <ul style="list-style-type: none"> • 00 (Employee Identifier) • 01 (Bar Code) • 02 (CAC Card)

6.2 Envelope Schema Definition

Element	Attribute	Type	Description
SourceDDSCode		String	The originator of this Message.
DestinationDDSCode		String	The destination of this Message.
DCCISMsgTypeCode		String	<p>The message type.</p> <p>Valid Values:</p> <ul style="list-style-type: none"> • 01 – Authentication Request • 02 – Authentication Response • 03 – Control Table Request • 04 – Control Table • 05 – Remote Domain Server is not available • 06 – XML Schema Version is out of date • 07 – Control Data Table is out of date • 08 – Heart Beat • 09 – Remote Trust Gateway is not available • 10 – Remote Authentication Request Not Processed • 98 – Trust Gateway shutdown message • 99 – Fatal Service Exception
DCCISXMLSchemaVersion		String	The XML schema version for both the payload and control data table.
DCCISTransactionIdentifier		String	A unique identifier assigned to this DCCIS transaction. The message originator is responsible for assigning a unique identifier to each message.
ControlDataDateTime		dateTime	The timestamp of the current Control Data Table
Payload		hexBinary	The encrypted message payload. This can be either the Control Data XML or the Payload XML. The message type is used to determine which xml schema to expect.

Element	Attribute	Type	Description
PayloadKey		hexBinary	This is the symmetric key that was used encrypt the payload. The PayloadKey has been encrypted using asymmetric encryption and can only be decrypted using the Destination DDS's private key.
EnvelopeSignature		hexBinary	The digital signature of this envelope. It includes all fields with the exception of the Payload and PayloadKey.

6.3 Payload Schema Definition

Element	Attribute	Type	Description
TokenString		String	The unique code that was obtained from the DCCIS Member. It may have been obtained from a CAC, Bar Code, or entered by the member.
OrganizationCode		String	The DCCIS Member's organization.
TokenCode		String	The token code that was presented by the member at the authentication station.
FingerImage		hexBinary	The fingerprint image.
FingerImageType		String	The fingerprint image type <ul style="list-style-type: none"> • 01 – Bit Map • 02 – JPEG • 03 – TIFF • 04 – GIF • 05 – Raw image • 06 – Pattern Template • 07 – Minutiae Template
FingerCaptureCode		String	The finger capture code. Indicates the fingerprint the Image represents.
FingerImageHeight		int	The image height. Only needed for raw '05' finger print images.
FingerImageWidth		int	The image width. Only needed for raw '05' finger print images.
FingerImageResolution		int	The image resolution in Dots Per Inch (DPI)

Element	Attribute	Type	Description
ReturnCode		String	The result of the request. Valid Values: <ul style="list-style-type: none">• 00 - Success• 01 – Member Not Found• 02 – Member not in specified organization• 03 – Poor fingerprint quality• 04 – Fingerprint match successful• 05 – Fingerprint match failed
SecurityClassificationIdentifier		String	Reserved for future use.
LastName		String	A member's last name.
FirstName		String	A member's first name.
MiddleName		String	A member's middle name.
Cadency		String	The cadency name (Sr, Jr, III) of a member.
Nationality		String	The citizenship of the DCCIS member.
Association		String	Used to describe the association that the member has with the organization. For commercial DCCIS, this will generally be employee. For DoD, the associations: <ul style="list-style-type: none">• 00 - Employee• 01 - Civil• 02 - Political Appointee/SES• 03 - Uniform Service• 04 - Contractor• 05 – Affiliate• 06 - Beneficiary
PhotoImage		hexBinary	The Member's photograph.
ImageType		String	The image type (JPEG, GIF, TIFF)
CaptureCode		String	Finger Sequence Number that is available for the DCCIS Member.

Element	Attribute	Type	Description
VetType		String	The vetting type or level for the DCCIS Member. (Reserved for future use.)
VetDate		dateTime	The vetting date. (Reserved for future use.)

7.0 Glossary

DCCIS – Defense Cross Credentialing Identification System

The DCCIS application provides web access to different DCCIS member organization databases, making it possible for them to authenticate visitors carrying authorized ID cards issued by fellow DCCIS member organizations. To compensate for differences in identification systems and credentials used, DCCIS can read a range of media and accept a range of credentials.

DMDC – Defense Manpower Data Center

A Defense Support Activity which is the most comprehensive repository of personnel, manpower, training, and financial data in the DoD. DMDC owns and manages DEERS, including AWS.

DoD (DOD) – Department of Defense

The collection of federal agencies responsible for safeguarding national security.

FiXs: The Federation for Identity and Cross-Credentialing Systems

FTB: FiXs Trusted Broker

HTTP – HyperText Transport Protocol

The underlying protocol used by the Internet which defines how messages are formatted and transmitted, as well as what actions web servers and browsers should take in response to various commands.

PKI – Public Key Infrastructure

Public-key infrastructure (PKI) is the combination of software, encryption technologies, and services that enables DoD to protect the security of their communications and business transactions. PKI integrates the Common Access Card (CAC), digital certificates, public-key cryptography, and certificate authorities into total, enterprise-wide network security architecture.

PO – Project Officer: An individual representing DMDC and assigned to a customer for the purposes of implementing AWS.

XML – eXtensible Markup Language: A simple, very flexible text format derived from SGML (ISO 8879). Originally designed to meet the challenges of large-scale electronic publishing, XML is also playing an increasingly important role in the exchange of a wide variety of data on the Web. For more information about XML, refer to

<http://www.w3.org/XML/>



The Federation for Identity and
Cross-Credentialing Systems®

FiXS® Configuration Control Board Procedures

***Version 3.0
September 1, 2010***

www.fixs.org

Copyright 2010 by the Federation for Identity and Cross-Credentialing Systems, Inc.®

All Rights Reserved

Printed in the United States of America

10400 Eaton Place, Suite 500A

Fairfax, VA 22030

(703) 591-9255

Table of Contents

1.0	GENERAL REQUIREMENTS AND DEFINITIONS.....	3
2.0	APPLICABILITY	3
3.0	SCOPE.....	3
4.0	REFERENCES AND STANDARDS	4
5.0	CCB INPUTS AND OUTPUTS	4
6.0	ACTIVITIES.....	4
7.0	ROLES AND RESPONSIBILITIES.....	5
7.1	MEMBERSHIP	5
7.2	DECISIONS.....	6
7.3	MEETING LOGISTICS	7
8.0	CCB ACTIVITIES ASSOCIATED WITH THE CONFIGURATION CHANGE MANAGEMENT PROCESS	7
8.1	EMERGENCY MEETINGS.....	7
8.2	CLOSURE OF PROPOSED CHANGES.....	8
8.3	ACTION ITEM MANAGEMENT	8
8.4	TEST AND EVALUATION ACTIVITIES	9
9.0	AMENDMENTS TO THE CCB PROCEDURES	9
10.0	REVISION HISTORY.....	10
	APPENDIX – ACRONYM LIST	1

1.0 General Requirements and Definitions

The CCB reports directly to the Executive Committee for recommendations on necessary implementation of changes that affect the day-to-day operations of these Network, products, or services. This document defines the role of the FiXs Configuration Control Board (CCB) in configuration and change management processes as it applies to FiXS; the FiXs Network; any service providers providing products or services related to FiXs or using FiXs-branded products or services, or otherwise utilizing the FiXs Network. It defines the details of CCB operations, including the scope, membership, responsibilities, and operating procedures.

The CCB is responsible for recommending changes to the FiXs Technical Architecture and Specifications document and is responsible for the advising on the technical development and modification of FiXs products and services, to include development and maintenance of FiXs software, site certification requirements, security, and the interface specifications to be used in the FiXs Trust Broker (FTB) configuration(s).

2.0 Applicability

This document defines development, change and configuration management (CM) processes used to manage the FiXs baseline, including but not limited to hardware, software, commercial off-the-shelf (COTS), licenses, documentation, schedule, processes and procedures along with any interfaces, as applicable. The configuration of the FiXs baseline shall not be changed without CCB recommendation to the Executive Committee and subsequent approval. Such configuration changes include changes to the software, hardware, COTS products, and the documentation defining the program configuration and operation.

3.0 Scope

The FiXs CCB is the single point of coordination for change management recommendations and requirements related to the configuration and evolutionary development of FiXs.

4.0 References and Standards

The following standards will be used for reference in the CM process outlined in this procedure.

- CMMI for Systems Engineering/Software Engineering/Integrated Product and Process Development/Supplier Sourcing, Version 1.1, Carnegie Mellon Software Engineering Institute, March 2002 (*as updated*).
- National Consensus Standard for Configuration Management, Electronic Industries Alliance, EIA 649-A, 01-Oct-2004 (*as updated*).

5.0 CCB Inputs and Outputs

Any change to the configuration baseline must be managed using the configuration change management process (see Figure 1), and must be accepted by the FiXs CCB and forwarded to the Executive Committee for approval. The FiXs CCB manages changes to the configuration baselines by using Request for Changes (RFCs) or Engineering Change Proposals (ECPs). To perform its review, the CCB requires input from the members of the FiXs CCB.

The output of the FiXs CCB review is a decision on whether or not to recommend initiation of the change. For those changes which are approved, the CCB will also prioritize the changes to indicate a preferred or desired sequence in which the changes should be implemented.

6.0 Activities

A typical CCB meeting may include, but is not limited to, the following activities:

- Review/approval of minutes from the previous meeting (if any)
- Review and status reporting of open CCB action items
- Review of RFC's and ECP's presented for CCB consideration. This review may address the following considerations:
 - Strategic plan impacts
 - Schedule impacts
 - Cost and budget impacts

- Documentation requirements
 - Security accreditation impacts
 - Interface impacts
- Closure of completed RFC's and ECP's
- Status of other open RFC's or ECP's, including status of ongoing development, testing, or deployment activities
- Report of ongoing test and evaluation activities by Testing and Evaluation
- Consideration of the total impact of each proposed change followed by a decision by the CCB membership whether to forward a recommendation
- Review of any new action items created and assigned by the CCB Chairperson

7.0 Roles and Responsibilities

7.1 Membership

In accordance with the Bylaws, the FiXs CCB is limited to members of the Board of Directors. By approval of the Board, the Chair is the FiXs Vice President. There shall be no more than seven (7) voting members of the CCB. In addition to the voting members, other personnel may be assigned to support the deliberations of the CCB, as needed, from each of the following areas of specialization:

- Configuration Management (CM) – including but not limited to equipment, software, licenses
- Systems Engineering
- Software Development
- Installation and Deployment
- Integration & Test
- Logistics (documentation, support, training, spares)
- Quality Assurance
- Budget

The CCB will meet periodically, as determined by the Chairperson (or designated alternate) or directed by the Executive Committee. A quorum consisting of at least 50% of the CCB Board members plus the Chairperson (or designated alternate) is required for a meeting to

proceed. With proper advance notice, these meetings may be attended by non-voting members, to assist in clarifying specific change requests. All CCB members are encouraged to attend these meetings in person. However, meetings *may* be conducted by means of telephone conference or similar communication equipment by means of which all persons participating in the meeting hear each other, and participation in a meeting by such means shall constitute presence in person at such meeting.

Emergency meetings may be called by the Chairperson or as directed by the Executive Committee to handle unexpected developments, situations or circumstances requiring more urgent response. CCB members may attend these emergency meetings in person, or dial in via telephone. Further, members who are unable to attend emergency sessions may submit their inputs via e-mail in advance of the emergency meeting to the Chairperson or to a designated representative/alternate.

7.2 Recommendations

CCB recommendations are determined by the CCB Board members with additional input being considered from non-voting attendees. Non-voting members may be excused from the meeting, in order for the CCB Board members to discuss and deliberate the issues and to reach a decision.

Typically, one of the following recommendations is rendered by the CCB, for each proposed change:

- “Approve As-Is”
- “Approve with Noted Change/s”
- “Disapprove” (reason will be stipulated)
- “Hold” or “Defer” (reason will be stipulated)

A simple majority of votes cast by “members present” (see Paragraph 7.1 above for definition) carries any action except where provided otherwise by law or by the FiXS governance requirements and subject to any coordination necessary with other committees, as applicable (i.e. Legal and Privacy Committee, Security Committee, etc. Further, voting may take place in person or by proxy with advance written notice. All votes shall be recorded in the meeting minutes. Votes may also be cast orally via conference call or via email either during or after a conference call. In each instance, the voting records will be recorded and reported in the meeting minutes.

The results of all recommendations, along with the assigned priorities, shall be presented to the Executive Committee, at their next regular meeting for final adjudication.

7.3 Meeting Logistics

FiXs CCB meetings are held as directed by the CCB Chairperson. If the CCB Chairperson or a designated alternate is not available to chair a scheduled meeting, the meeting will be re-scheduled.

8.0 CCB Activities Associated with the Configuration Change Management Process

Any change to the configuration of the FiXs baseline must be approved through the CCB. During the development of a configuration change, the CCB must recommend continuation of work following each test phase.

All engineering work products identified as required CM artifacts are placed under CM control. The members of the CCB perform a technical evaluation of the recommendation and the supporting artifacts. Work products are analyzed for completeness and accuracy. Once required artifacts have been provided and accepted, the ECP is then ready for CCB consideration. The CCB makes a programmatic decision whether to authorize continuation of work on the changes.

The CCB considers:

- Analysis and recommendation of Subject Matter Experts (SMEs)
- Whether expected interface, schedule, cost, infrastructure, documentation, migration, and other impacts are acceptable (risk management)
- Whether CM documentation requirements have been met

8.1 Emergency Meetings

In addition to the routine CCB meeting(s), there may be occasions where an emergency meeting is required. Conditions which warrant these added meetings include configuration change recommendations required to either continue system functionality; to meet schedule; or to preclude extensive delay in meeting deadlines.

When an emergency or urgent action is required by the CCB, the Chairperson (or designated alternate) is notified by the requesting member and provided with suitable justification. If the Chairperson agrees with the emergency session request, the Chairperson or a CM representative will:

- Arrange a schedule and location for the meeting,
- Contact all CCB members or alternates and communicate the nature of the problem and the schedule for the meeting.
- Make copies of the agenda package and distribute at the earliest opportunity.

The minimum quorum for an emergency CCB meeting is 3 members plus the Chairperson for a total of 4 standing CCB members.

The requesting member will present the issue or requested change. Each participating member will estimate the impact to their functional area. After considering the problem and impact assessment, the members of the CCB will render an appropriate decision, assign an appropriate priority (if approved), assigns the appropriate action item(s) (if necessary), or provides other direction as required to resolve the issue.

Any proposed CCB changes to address an urgent matter must be approved, by the FiXs President and at least one other officer of the Federation.

After the meeting, the CCB will complete the post-meeting actions.

At the next formal meeting, the CCB will officially address all emergency CCB issues for closure of paperwork as needed.

8.2 Closure of Proposed Changes

All changes proposed to the CCB (such as ECP's and RFC's) can only be closed by the CCB. Generally, the CCB closes an ECP or RFC when all development, CM, and deployment activities have been completed and an acceptable after-action report has been provided. Some of the other reasons for closing ECP's include:

- An ECP or RFC was superseded by a related ECP or RFC
- Development of a change was cancelled after initiation of work

8.3 Action Item Management

The CCB uses "action items" to record and track the resolution of all actions assigned to CCB members and others at CCB meetings by the Chairperson. A review of open action items takes place at each CCB meeting, and each meeting concludes with a reiteration of new action items assigned at the meeting.

The following information is recorded for each CCB action item:

- Date action initiated
- Title of action

- Description of action
- Priority (1-5; 1 is most urgent priority)
- Originator
- Assignee
- Due date

The following additional information may be recorded for CCB action items:

- Meeting at which the action was assigned
- ECP or RFC with which the action is associated

Each time an action is reviewed by the CCB, the review date and a description of actions taken by the CCB and/or the assignee are recorded. When the assigned action is complete, the action is closed by recording the closure date, the individual who closed the action (usually the Chairperson), and a summary description of what was done to complete the action.

The CCB Chair is responsible for recording and updating CCB action items in the Action Item Database following each meeting. The CCB Chair is also responsible for preparing a list of open CCB action items for review at each CCB meeting.

8.4 Test and Evaluation Activities

At each CCB meeting, a Testing and Evaluation representative may provide a summary status of developmental and operational test activities in progress. The Testing and Evaluation representative may also summarize the current status of test activities being performed and provide a schedule of planned test activities.

9.0 Amendments to the CCB Procedures

The FiXs Executive Committee shall provide the overall guidance in the framework and operating procedures for the CCB. Any changes resulting from this guidance shall be incorporated into these procedures.

Administrative changes to these procedures shall be incorporated into the Procedures by the CCB Chairperson or a designated alternate. Such changes shall constitute a “minor” revision change in the numbering of this document. All proposed changes shall be reviewed by the members of the CCB Board. The CCB Board members shall vote on the proposed changes, either individually, or taken as a whole. All such changes are to

be provided to the Executive Committee for final approval and/or submission to the Board of Directors as required.

10.0 REVISION HISTORY

Version	Date	Comments
0.1	Nov 10, 2005	Initial release
0.2	Nov 15, 2005	Clarified Membership, Added section on Changes & Revisions to these Procedures
0.9	Nov 16, 2005	Minor changes based on CCB meeting review & comments – Applicability, Membership, Decisions, and Figure 1.
2.0	March 29, 2007	Changed version number for FiXs documents consistency
2.1	Jan. 31, 2008	Modified to add language regarding the CCB responsibilities, to Section 1.0, General Requirements and Definitions; update Section 7.1 Membership, to be in accordance with the Bylaws; minor editorial changes
3.0	Sept. 2010	Minor changes and edits made in preparation of baseline with DMDC and based on latest Board review/recommendations (Board Meeting 8.14.10)

Appendix – Acronym List

CCB	Configuration Control Board
CM	Configuration Management
CMMI	Capability Maturity Model – Integration
COTS	Commercial Off-the-Shelf
DW	Deviation/Waiver
ECP	Engineering Change Proposal
FiXs	Federation for Identity and Cross-credentialing Systems
I&T	Integration and Test
QA	Quality Assurance
PM	Program Manager
RFC	Request for Change
SD	Software Development
SE	Systems Engineering
SME	Subject Matter Expert

Process Flowchart

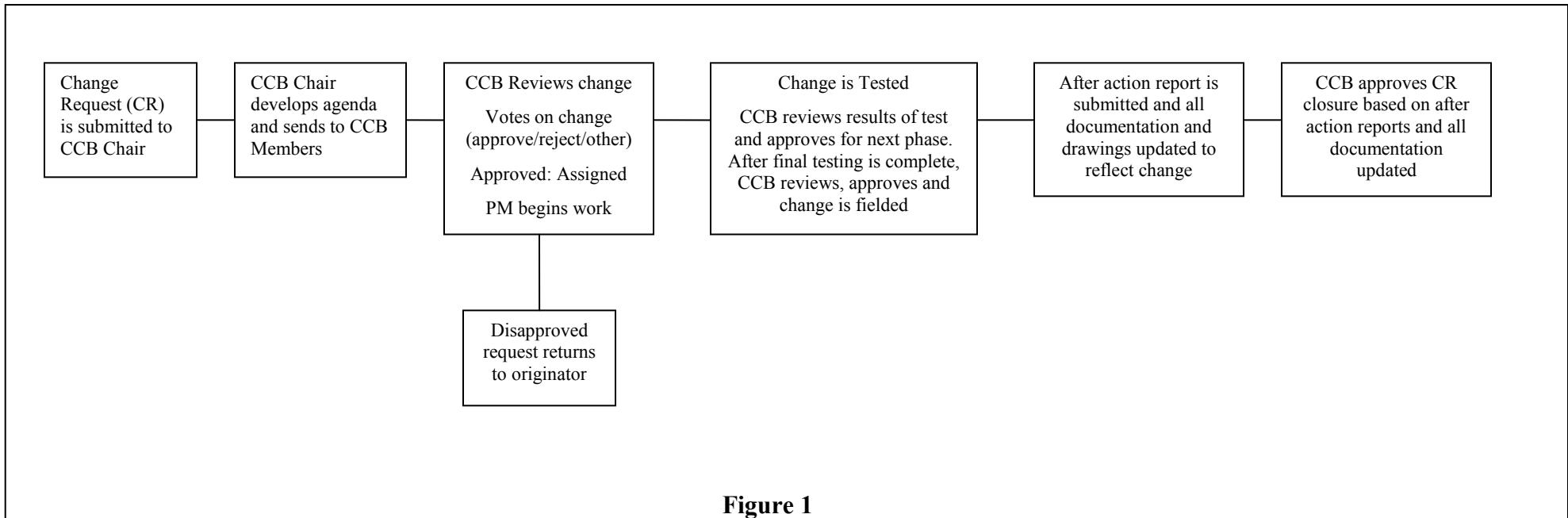


Figure 1



The Federation for Identity and
Cross-Credentialing Systems®

FiXS Certification and Accreditation Process

V 1.1

September 15, 2008

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXS®)
Page 1284 of 1794

TABLE OF CONTENTS

1	FIXS CERTIFICATION AND ACCREDITATION PROCESS	5
1.1	Background.....	5
1.2	FiXs C&A Process Overview.....	6
2	FIXS C&A INITIATION PHASE	8
3	FIXS SECURITY CERTIFICATION PHASE.....	10
3.1	FiXs General Information System Certification Assessment.....	11
3.2	FiXs PIV Certification Assessment	12
3.3	FiXs Compliance Assessment Report.....	12
4	FIXS ACCREDITATION PHASE	13
4.1	ATO Decision	13
4.2	FiXs ATO Decision Appeals Process	13
5	FIXS CONTINUOUS MONITORING PHASE	14
5.1	Reassessment and Audit	14
5.2	Random-compliance Assessments	14
5.3	Government-compliance Assessment	14
6	ACRONYMS AND ABBREVIATIONS.....	15
7	REVISION HISTORY	16

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

TABLE OF FIGURES

FIGURE 1: FIXS C&A PROCESS	7
FIGURE 2: SYSTEM BASELINE DOCUMENTATION ANALYSIS PROCESS.....	9
FIGURE 3: FIXS SYSTEM CERTIFICATION PROCESS	10

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

TABLE OF APPENDICES

Appendix A: FiXs Information Systems Security Controls Checklist.....	A-1
Appendix B: FiXs PIV Security Controls Checklist.....	B-1
Appendix C: FiXs Approval to Operate (ATO) Application	C-1
Appendix D: FiXs Baseline Security Assessment Checklist	D-1
Appendix E: Risk Assessment Template	E-1
Appendix F: System Security Plan Template.....	F-1
Appendix G: Plan of Action and Milestones (POA&M) Template	G-1
Appendix H: Security Requirements Traceability Matrix Template	H-1
Appendix I: PIV Card Issuer (PCI) Operations Plan Template	I-1

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

1 FIXS CERTIFICATION AND ACCREDITATION PROCESS

1.1 Background

The Federation for Identity and Cross-Credentialing Systems (FiXs™) is a not-for-profit 501 c (6) trade association comprised of a coalition of industry and public sector organizations whose objective is to support efforts to develop standards supporting the creation and deployment of a secure interoperable identity cross-credentialing network. These Certification and Accreditation (C&A) processes are based on requirements and security guidance contained in numerous government directives and policies as well as industry standards and best practices and define the rights, responsibilities and liabilities of FiXs Member Organizations and are a part of a larger set of governance documents that lay the foundation for establishing trust in and the operations of the FiXs Network. The other documents, known as the FiXs Foundational Documents, include:

- The Trust Model;
- FiXs Policy;
- Implementation Guidelines;
- The Technical Architecture and Specifications; and
- Security Guidelines.

The FiXs Network provides a highly-scalable, secure, auditable solution set, whereby participating organizations can authenticate FiXs-Certified Credentials (also known as FiXs Credentials) issued to users from other participating organizations or “Subscribers” as well as authenticate the credentials issued by other related organizations (i.e. cross-credential). FiXs relies on a Federated Model of Trust, which is discussed more fully in the FiXs Trust Model. The federated identity model establishes trust between member organizations through the use of agreements, standards and technologies that make an “identity credential” portable across the organizations.

Initially, FiXs established a trusted relationship between certain FiXs Member Organizations and the DoD’s Defense Cross-Credentialing Identification System (DCCIS). The federation enabled participating Department of Defense (DoD) and industry facilities to achieve strong, and interoperable identity verification and authentication of participating contractor/private sector personnel who presented a company-issued trusted credential. Similarly, participating industry locations also recognized the DoD-issued Common Access Card (CAC) and the Defense Biometric Identity System (DBIDS) credential, which required no modifications in order to operate with FiXs and DCCIS. This initial proof-of-concept established the baseline for further expansion.

FiXs, which is the only organization authorized to inter-operate a cross-credentialing system with the U.S. Department of Defense, is deployed in a federated manner to enable other government agencies, first responders, and industry partners to authenticate the identity of individuals who seek access to their physical or logical assets in either the government or commercial environment.

In a federated system each sponsoring organization maintains its own database of enrolled members. Privacy and security are maintained because no identity information is held

centrally or maintained in the infrastructure except in the employee's host organization domain server.

In order to implement and achieve security standards outlined in Homeland Security Presidential Directive 12, FiXs has developed a certification and accreditation (C&A) process which is based on requirements and security guidance outlined in OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources. The FiXs C&A process incorporates both national security policy guidance outlined OMB Circular A-130 and C&A process definitions and implementation guidelines which are defined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, NIST 800-53, NIST 800-79-1, and other NIST information security and PIV publications. The NIST documents, along with FiXs Operating Rules, Implementation Guidelines, and other policy and procedural documents collectively define the policy and procedural baseline for the FiXs C&A process. The FiXs C&A process is based on the following NIST and FiXs documents:

- a. NIST SP 800-37, May 2004
- b. NIST SP 800-53, Revision 1, Dec 2006
- c. NIST SP 800-53A, Jul 2008
- d. NIST SP 800-79-1, Jun 2008
- e. National Information Assurance Certification and Accreditation Process (NIACAP) [NSTISSI No. 1000] , April 2000
- f. FiXs By-Laws, Version 2.2, 26 Nov 2007
- g. FiXs Security Guidelines, Version 2.0, 29 Mar 07
- h. FiXs Implementation Guidelines, Version 3.0, 29 Mar 2007
- i. FiXs Policy Document , Version 2.0, 29 Mar 2007
- j. FiXS Operating Rules, Version 2.0, 29 Mar 2007
- k. FiXS Operating Rules, Addendum
- l. FiXS Trust Model, Version 2.0, 29 Mar 2007

1.2 FiXs C&A Process Overview

The FiXs C&A process provides the policies, procedures, and guidelines for ensuring that FiXs member-deployed systems and components meet federal security standards and protection guidelines for identity management information. As the guidelines established in NIST 800-37, NIST 800-53, and NIST 800-79-1, the FiXs C&A process is designed to provide a set of standard procedures and policies for security certification and accreditation which will enable a governing authority and its Designated Approval Authority (DAA) to review and analyze the security posture and assess security risks associated with nominated information systems and/or components. In the context of the FiXs C&A process, the FiXs Board of Directors has designated the President of FiXs as its DAA. The FiXs DAA is empowered to authorize operation of a nominated FiXs-related system or

component under the framework of the FiXs C&A process. The FiXs DAA will keep the Board updated on the C&A nominations and successful completion of C&A activities along with IATO's and ATO's granted. Currently, the FiXs Board of Directors has delegated C&A review authority and accreditation decision recommendation authority to the organization's selected C&A Committee. The C&A committee works under the auspices of the FiXs CCB which governs its processes and procedures and this document. The standing chair of the C&A committee is the FiXs Corporate Secretary. The FiXs C&A Committee is selected from the general membership of the FiXs organization on a case-by-case basis when an application for C&A has been accepted and nominated for C&A. The selected members are selected based upon the type and nature of review contemplated and their area of expertise at it relates to the review and they are vetted to insure objectivity and no vested interest in the outcome of the C&A being performed.

Following the completion of the certification phase of the C&A process, the FiXs C&A Committee provides an accreditation recommendation to the FiXs DAA. The FiXs DAA analyzes the recommendations from the C&A committee and makes the accreditation decision on behalf of the FiXs organization. .

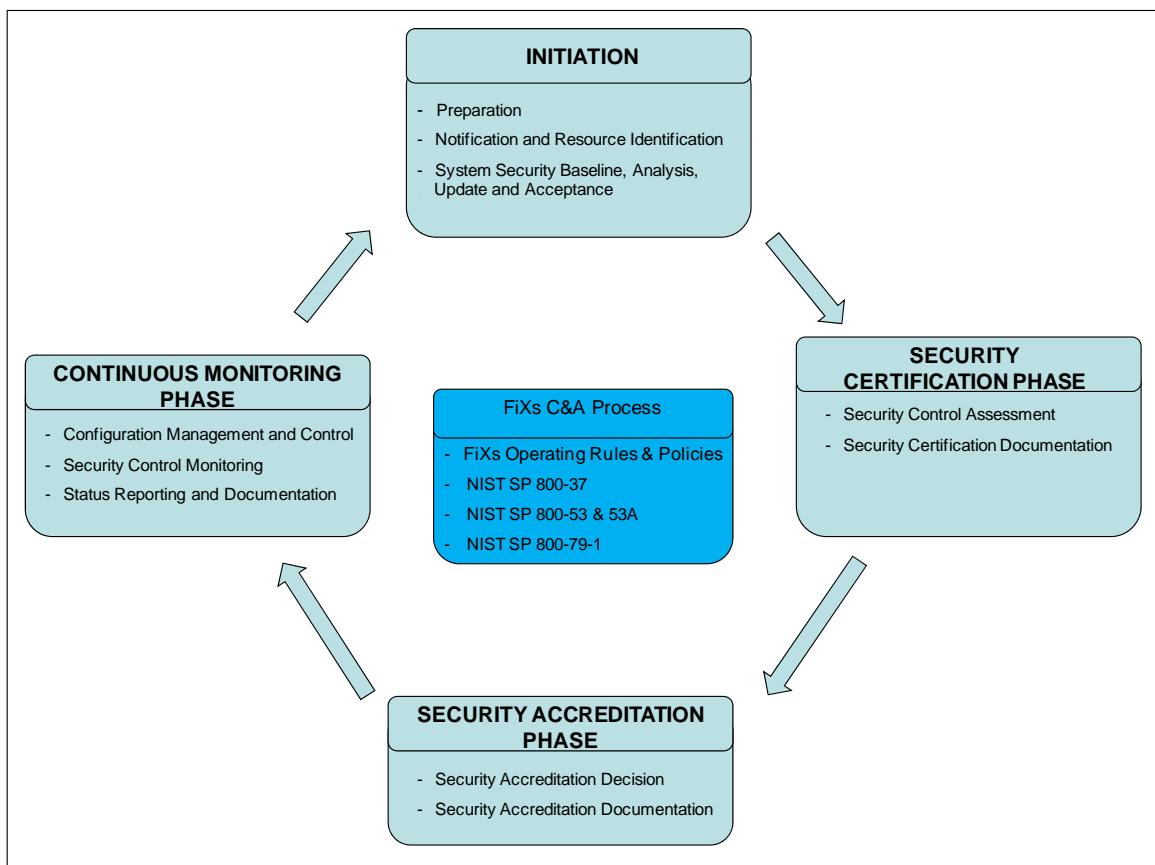


Figure 1: FiXs C&A Process

The FiXs C&A process, similar to the C&A process of the U. S. Federal Government, consists of four distinct phases:

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

- Initiation
- Security Certification
- Security Accreditation
- Continuous Monitoring

Upon the completion of the certification phase of the FiXs C&A process, the FiXs DAA will review the certification package and issue an accreditation decision on the nominated system or component. The accreditation decision, which is based on the DAA's determination of whether the nominated system or component meets the processes and criteria set forth in this document, to include OMB Circular A-130 NIST 800-37, NIST 800-53, and NIST 800-79-1 mandated information protection and security requirements, results in an "Authorization to Operate," "Interim Authorization to Operate," or "Denial of Authorization to Operate" decision.

2 FIXS C&A INITIATION PHASE

The Initiation Phase consists of three tasks: (i) preparation; (ii) notification and resource identification; and (iii) system security baseline documentation analysis, update, and acceptance. The primary focus during this phase is the establishment of the system's security baseline and the development of the system's supporting security documentation.

The initiation phase of the C&A process begins during the design, implementation, and testing of the proposed information system. Security system certification and accreditation must be factored into these initial phases of the system's lifecycle. Development of the system's security certification and accreditation package should be considered during the early phases of the systems lifecycle. The system's baseline security baseline documentation should be developed prior to the deployment phase. The security baseline assessment as a minimum includes the following actions:

- a. Conducting an initial security assessment of the nominated system using the FiXs Baseline Security Assessment Checklist,
- b. Preparing a draft System Security Plan (SSP),
- c. Conducting an initial System Risk Assessment and preparing a Risk Assessment Report,
- d. Developing an initial Plan of Action and Milestones (POA&M)

When the system is nearing the deployment phase, the baseline documentation along with the FiXs ATO application should be submitted to the FiXs C&A Committee.

A key focus of this phase of the C&A process is to ensure that the FiXs DAA and the organization's C&A Committee are in agreement with the contents of the system baseline before the assignment of a certification agent and initiation of the certification phase of the process.

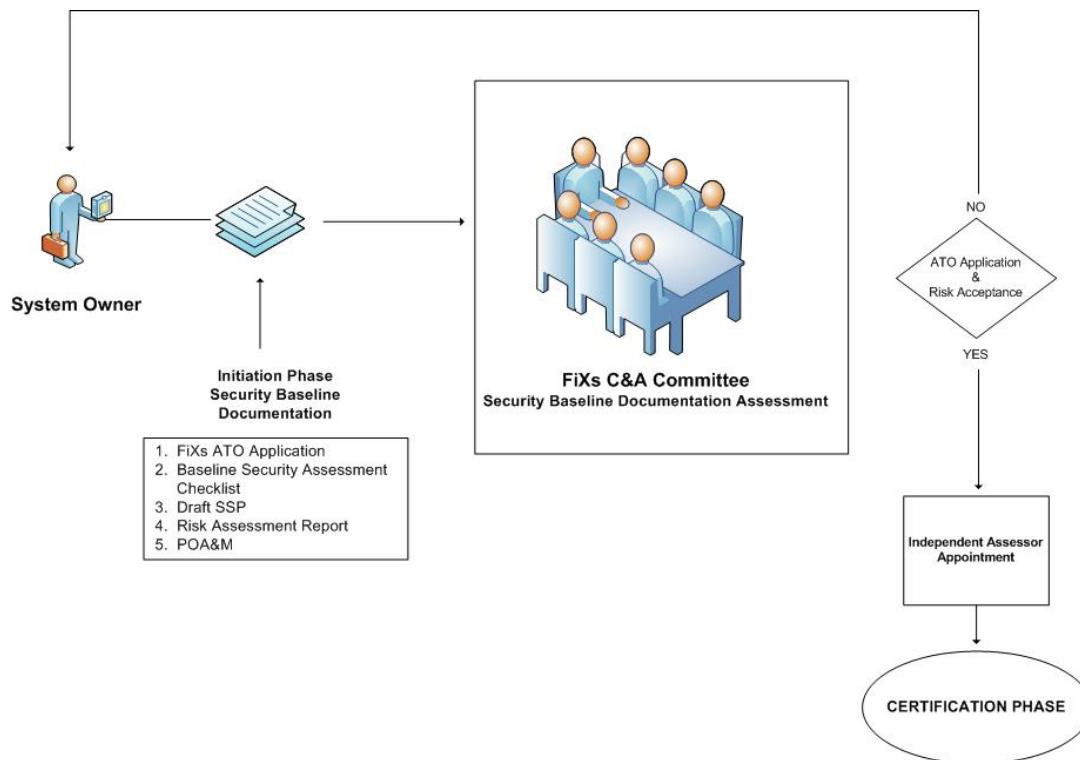


Figure 2: System Baseline Documentation Analysis Process

The C&A Committee will review the submitted security baseline documentation and advise the DAA on the completeness of the submitted documentation and acceptability of the identified risks. After coordination and negotiation on these issues, the system owner is given approval to move into the certification phase of the process. Once activities of the initiation phase have been completed, the FiXs system of records notice (SORN) is updated by the FiXs C&A Committee and the FiXs-approved independent Third-Party Assessor (s) are notified. The system owner negotiates a contract with the independent Third-Party Assessor for conducting an independent system certification and developing a security assessment report and accreditation recommendations.

The FiXs SORN is used to uniquely identify FiXs operating systems and components which are involved in the retrieval and or storage of information which contain personal identity information, e.g., the name of an individual, or some identifying number, symbol, or other identifier assigned to the individual. In compliance with this federal mandate, the FiXs organization will maintain and update the SORN to reflect systems descriptions and a list of identity attributes utilized by each FiXs system or component. The FiXs SORN will be made available to federal authorities for inspection.

3 FIXS SECURITY CERTIFICATION PHASE

All systems nominated for connection and approval to operate over the FiXs Network must be assessed by an independent third-party Assessor. The Applicant must select the Assessor from the list of FiXs authorized and approved certification agents. Once the appropriate support agreements are in place, the Applicant and the Assessor are responsible for gathering appropriate supporting materials which are necessary to support the assessment effort. Typically, all documents and supporting materials included or referenced in the SSP and the FiXs C&A checklist are required to support the assessment effort. Additionally, the results from previous audits, security certifications, security reviews, self-assessments, security test, and privacy impact assessments should be made available to the Assessor.

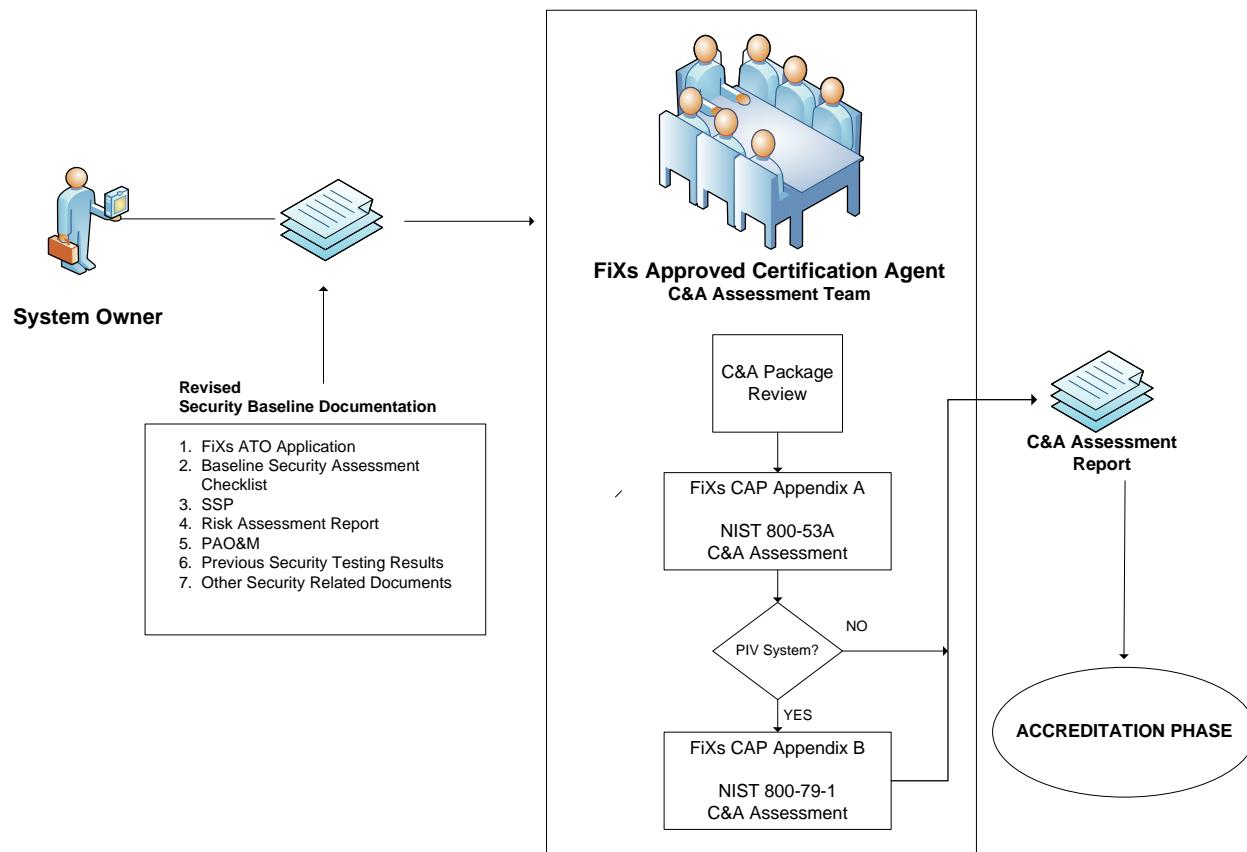


Figure 3: FiXs System Certification Process

The FiXs certification security assessment process outlines assessment criteria for the general information technology system functionality as well as functionality provided in Personal Identity Verification (PIV) systems. General information system assessment criteria and procedures are outlined in the FiXs Security Requirements Checklist, Appendix A. The assessment criteria and procedures for systems that include PIV information are contained in Appendix B, the FiXs PIV Security Requirements Checklist. Depending on the proposed role of the nominated system indicated in the FiXs connection application, one or both of the above checklists may be used to assess the security controls of a nominated system.

When the nominated system or component includes PIV functionality, the NIST 800-53A based IT security controls must be assessed first. Following the completion of the NIST SP 800-53A based security controls assessment, the NIST 800-79-1 based PIV assessment is conducted.

3.1 FiXs General Information System Certification Assessment

Once the security baseline documentation submitted during the initiation phase is assessed and validated by the FiXs C&A Committee, a FiXs-approved Independent Assessor must be selected. Based on guidance resulting from the FiXs C&A Committee review of the submitted security baseline documentation, the Assessor and system owner must select, or develop when needed, appropriate methods and procedures to assess the management, operational, and technical security controls of the nominated information system. The Assessor and system owner will apply the security control tailoring process outlined in NIST SP 800-100 to select the recommended set of security controls from the FiXs Security Requirements Checklist which are applicable to the nominated system. The recommended security controls list for the nominated system should be based on the tailoring guidance contained in NIST SP 800-100, FiXs C&A Committee's comments from system's baseline documentation review, and risks identified in the nominated system's security baseline Risk Assessment Report.

After the recommended security controls have been selected, the Assessor and system owner will designate the recommended assessment method for each selected security control. The list of recommended security controls will be listed in a Systems Requirements Test Matrix (SRTM). The prepared SRTM will indicate one of the following proposed methods for assessing each identified security control:

- a. Interview
- b. Demonstrate
- c. Test
- d. Observe

The Assessor will submit the SRTM to the FiXs C&A committee for review and ratification. The validated SRTM will define the scope of the information system's security controls assessment effort. The Assessor will conduct the assessment in accordance with the criteria outlined in the validated SRTM.

Once a validated SRTM is established for a common FiXs infrastructure component, the SRTM will generally be used as the baseline for future implementations of components with similar risk characteristics which perform the same functionality. When a pre-existing SRTM is available for a nominated system or component, tailoring recommendations for a nominated system should be based on the established SRTM baseline. A sample SRTM template is provided at Appendix H.

3.2 FiXs PIV Certification Assessment

The FiXs PIV Security Requirements Checklist, Appendix B outlines certification assessment criteria for systems which contain PIV information and support the issuance of PIV Cards. Nominated systems which contain PIV information and support PIV related functionality must undergo assessments under both the FiXs Security Requirements Checklist and the FiXs PIV Security Requirements Checklist. The PIV assessment effort is usually conducted in conjunction with the information systems security assessment. The Assessor will conduct the PIV portion of the assessment in accordance with the criteria outlined in Appendix B. The results of both elements of the assessment effort must be forwarded to the FiXs C&A Committee as part of the forwarded certification and accreditation package.

In addition to undergoing an assessment conducted under the security controls outlined in Appendix B, the nominated PIV system must be completely described in a PIV Card Issuer (PCI) operations plan. This comprehensive document incorporates all the information about the nominated system that is needed for the Assessor to review and assess the capability and reliability of the nominated system's operations. The PCI operations plan includes a description of the structure of the nominated PIV system, its facilities, any external service providers, and the roles and responsibilities within the system owner's PCI facility. A template for a PCI operations plan is provided in Appendix I.

3.3 FiXs Compliance Assessment Report

Following the completion of assessment activities, the Assessor must prepare and submit an assessment report. The assessment report will document the findings found during each phase of the assessment and provide the results of each assessed security control. Based on the assessment results, the system owner with the assistance of the Assessor will update the system's Risk Assessment Report and POA&M. The updates to these documents must also be included with the submitted assessment report.

The assessment report along with the accompanying system risk assessment and POA&M will be submitted to the FiXs C&A Committee for review, evaluation, and in preparing a recommendation to the DAA.

4 FIXS ACCREDITATION PHASE

Upon receipt of the detailed report from the certified Assessor, the FiXs C&A Committee Chairperson will convene a meeting of the C&A committee to review the submitted findings. This committee will be assembled with a minimum of three members. The FiXs C&A Committee Chairman will select impartial committee members, which have an understanding of the process involved and are capable in rendering an objective recommendation. Upon the completion of a detailed review of the assessment report, the C&A Committee may submit follow-up questions and seek clarification of findings supplied in the assessment report.

Once questions and any issues relating the assessment report are resolved, the C&A Committee will make a written recommendation to the FiXs DAA to either grant or deny ATO Certification or provide a conditional interim ATO (IATO) pending completion of open, low-risk requirements and open items identified on the submitted POA&M.

4.1 ATO Decision

The FiXs DAA will analyze recommendations from the C&A committee and make the accreditation decision on behalf FiXs.

If an IATO is granted, the interim period of operations will not to exceed 90 days. It is incumbent upon the Applicant to remedy open issues and to come in full compliance with ATO requirements within the designated period to include having any identified follow-up or incremental assessments completed.

An approval of an ATO or IATO Certification will grant the Applicant the authority to officially operate.

4.2 FiXs ATO Decision Appeals Process

Any applicant whose ATO is denied by the DAA may appeal the decision to a review panel comprised of members of the FiXs Board of Directors.

Upon receipt of an Appeal Request from an applicant, FiXs will appoint a three-member review panel from among the FiXs Board of Directors to hear the appeal request. The panel may request any additional information from the applicant or schedule a hearing to permit the Applicant to further clarify and present his/her position(s). The panel may also make its determination solely upon the information presented in the appeal request. The appointed panel will consider the evidence submitted during the appeal process and make a final determination on the accreditation status of the system.

5 FIXS CONTINUOUS MONITORING PHASE

The Applicant will be required to submit an Annual Renewal Compliance Statement for an ATO Certification to remain in effect. The Applicant must warrant continued compliance with the requirements set forth in the assessment process and shall agree to provide annual audit results. FiXs reserves the right to perform a follow-up compliance assessment or a random compliance assessment at any time. This follow-up assessment will be done with advance notice and coordination with the party being reviewed; however, it will be accomplished without undue delay. The party being reviewed may be required to bear the costs of such reassessment if the conditions are such that the standards then required for being granted an ATO are not being complied with. If such conditions are warranted, any ATO may be cancelled effective immediately.

5.1 Reassessment and Audit

The Applicant must notify the Assessor and the FiXs C&A Committee of any organizational or material changes at least 60 days before the change is performed or immediately upon the occurrence of any unplanned change. FiXs will determine if a reassessment is required for the changes.

The Applicant must also agree to the following conditions to maintain ATO Certification:

- A FiXs-designated Assessor may conduct an on-site reassessment or POA&M review of an Applicant within one year after certification.
- A FiXs-designated Assessor must audit any certified Applicant at least every three years or as needed.
- The Applicant may be required to submit other internal audits, as deemed necessary.
- Additional maintenance activities may be stipulated between FiXs and the Applicant.

5.2 Random-compliance Assessments

Accredited Applicants will be assessed on a random, periodic basis for compliance with FiXs policies and procedures and security compliance. Such random compliance assessments will be performed by independent Assessors, which shall be conducted using the matrix of compliance factors relevant to the system(s) being audited.

5.3 Government-compliance Assessment

Under the terms of the FiXs Memoranda of Understanding (MOU) with the Department of Defense and the flowdown MOU with the Applicant, federal agencies may assess the entire FiXs Network or any of its components to ensure compliance with its regulations and conformance with the requirements and intent of agreed-to policies. These assessments are random, with or without notice, prompted by indicators from the network or other forms of inspection.

6 ACRONYMS AND ABBREVIATIONS

Term	Definition
Assessor	The individual or organization responsible for conducting assessment activities under the guidance and direction of a Designated Accreditation Authority.
ATO	Authorization to Operate; one of three possible decisions concerning a nominated system made by a Designated Accreditation Authority after all assessment activities have been performed stating that the reliability of the system is accredited and the system is authorized to perform specific PIV of information system functions.
C&A	Certification and Accreditation
DAA	Designated Approval Authority
FiXs	Federation for Identity and Cross-Credentialing Systems
IATO	Interim Approval to Operate
MOU	Memoranda of Understanding
NIACAP	National Information Assurance Certification and Accreditation Process
NIST SP	National Institute of Standards and Technology Special Publication
PCI	PIV Card Issuer
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestones
SRTM	Security Requirements Traceability Matrix
SSP	System Security Plan
TGB	Trusted Gateway Broker

7 REVISION HISTORY

Version	Date	Comments
1.0	September 11, 2008	FiXs Board of Directors approved version 1.0 as baseline.
1.1	September 15, 2008	FiXs Board of Directors on September 11, 2008 approved Change Control Board (CCB) oversight of the Certification and Accreditation Subcommittee (C&A) <u>after</u> they voted approval of version 1.0. The CAP document was then edited to reflect these CCB and C&A subcommittee changes and reviewed/updated for consistency based on this set of changes. The CAP document version was then updated to Version 1.1. These changes were completed on 9/15/2008.

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)



The Federation for Identity and
Cross-Credentialing Systems®

Appendix A

FiXS Information Systems Security Controls Checklist

NIST 800-53 Compliance

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXS®)

This FiXs IT Systems Certification and Accreditation Checklist contains requirements from NIST 800-53. Applicants are assessed based on these requirements.

The Checklist is divided into workbook sections by NIST 800-53 family. In the checklist, each requirement has sub-requirements. These sub-requirements are deemed as low, medium, or high impact. Assessment methods for each of these sub-requirements are provided in the checklist. These methods include document review and interviews. Each requirement receives a result of Fully Satisfied, Partially Satisfied, or Not Satisfied. These results are tabulated at the bottom of each section.

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

CHANGE CONTROL RECORD SHEET

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

Control Family	Control ID	Original Content	Revised Content
N/A	N/A	N/A	Inserted First Page with FiXs Crossmap to NIST 800-53. This will provide a Vehicle to define FiXs Specific Guidelines and instructions and this change page. Primary contents should be from FiXs Implementation guidelines. Changes for applying 800-53A to FiXs have two considerations first being longevity of the Certification and Testing process, second the system being tested may have to meet Federal requirements (such as personnel vetting) as well as FiXs requirements. The assumption is made if a system is meeting the Federal Requirements it will meet the FiXs requirement for the same control.
All	All	L M H	FiXs Provides for 3 levels of Credential Assurance High, Medium-High, and Medium. Medium-High and Medium Assurance Credentials required be hosted on systems with a comparable Medium FIPS 199 Categorization. Low Assurance Credentials and Low Assurance System/System Implementation are strictly forbidden.
CP CM	2.1 2.1	Federal Enterprise Architecture	FiXs Federated Architecture
PE	3.3	(i) the access control system is consistent with FIPS 201 and NIST Special Publication 800-73 (where the federal Personal Identity Verification (PIV) credential is used as an identification token and token-based access control is employed); (ii) the access control system is consistent with NIST Special Publication 800-78 (where the token-based access control function employs cryptographic verification); and (iii) the access control system is consistent with NIST Special Publication 800-76 (where the token-based access control function	(i) the access control system is consistent with, FiXs Rules and Guidance, applicable FIPS 201 and NIST Special Publication 800-73 (where the FiXs Certified Credential is used as an identification token and token-based access control is employed); (ii) the access control system is consistent with FiXs Rules and Guidance, applicable NIST Special Publication 800-78 (where the token-based access control function employs cryptographic verification); and (iii) the access control system is consistent with FiXs Rules and Guidance and

Copyright© 2008
 Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

		employs biometric verification).	applicable NIST Special Publication 800-76 (where the token-based access control function employs biometric verification)
PE	3.3	Physical and environmental protection policy; procedures addressing physical access control; FIPS 201; NIST Special Publications 800-73, 800-76, and 800-78; information system design documentation	Physical and environmental protection policy; procedures addressing physical access control are consistent with FiXs Rules and Guidance , applicable FIPS 201; NIST Special Publications 800-73, 800-76, and 800-78; information system design documentation; other relevant documents or records
PL	5.1	federal legislation	(i) the organization conducts a privacy impact assessment on the information system in accordance with FiXs Rules , applicable OMB policy; and (ii) the privacy impact assessment is consistent with FiXs Rules, and appropriate federal legislation and OMB policy.
PL	5.1	Security planning policy; procedures addressing privacy impact assessments on the information system; federal legislation and OMB policy	Security planning policy; procedures addressing privacy impact assessments on the information system; appropriate FiXs Rules, applicable federal legislation and OMB policy
PS	3.1	appropriate legislation, OPM policy, regulations, and guidance	appropriate FiXs Rules , federal legislation and OMB policy; privacy impact assessment; other relevant documents or records.
PS	3.1	Personnel security policy; procedures addressing position categorization; appropriate codes of federal regulations, OPM policy and guidance;	Personnel security policy; procedures addressing position categorization; appropriate codes of federal regulations, applicable FiXs Rules ; OPM policy and guidance;
PS	2.1	consistent with applicable federal regulations and OPM policy and guidance;	consistent with applicable FiXs Rules , federal regulations and OPM policy and guidance and/or FiXs Rules ; (Due to other than Federal interoperability a provision is required for FiXs Decision to determine appropriate PS screening criteria).

PS	2.1	appropriate codes of federal regulations; OPM policy and guidance;	appropriate codes of federal regulations, applicable FiXs Rules ; OPM policy and guidance;
RA	2.1	potential impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level impacts	(iii) the organization considers in the security categorization of the information system, potential impacts to other organizations and, in accordance with FiXs Guidance consider potential national-level impacts and applicable sections of: USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, in applying the security categorization of the system;
RA	2.1	(v) designated, senior-level organizational officials review and approve the security categorization of the information system.	(v) designated, senior-level FiXs organizational officials review and approve the security categorization of the information system
RA	2.1	(i) the organization conducts the security categorization of the information system as an organization-wide exercise with the involvement of senior-level officials including, but not limited to, authorizing officials, information system owners, chief information officer, senior agency information security officer, and mission/information owners;	(i) the organization conducts the security categorization of the information system as an organization-wide exercise with the involvement of senior-level personnel including, but not limited to, FiXs authorizing official , information system owners, chief information officer, senior organization information security officer, and mission/information owners;
IA	7.1	Determine if the information system employs authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module	Determine if the information system employs authentication methods that meet the requirements of FiXs Guidance , applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module
IA	7	Control: The information system employs authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.	Control: The information system employs authentication methods that meet the requirements of FiXs Rules and: applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.

RA	3	<p>The organization conducts assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency (including information and information systems managed/operated by external parties).</p>	<p>The organization conducts assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the FiXs Network (including information and information systems managed/operated by external parties).</p>
IA	4.2	<p>Determine if the organization uses a Personal Identity Verification (PIV) card token to uniquely identify and authenticate federal employees, contractors in accordance with FIPS 201 and NIST Special Publications 800-73, 800-76, and 800-78.</p>	<p>Determine if the organization uses a Personal Identity Verification (PIV) card or FiXs Certified Credential token to uniquely identify and authenticate federal employees, contractors in accordance with FiXs Rules and Guidance, FIPS 201 and NIST Special Publications 800-73, 800-76, and 800-78.</p>
IA	4.2	<p>Examine: Identification and authentication policy; procedures addressing identifier management; information system design documentation; FIPS 201; NIST Special Publications 800-73, 800-76, 800-78; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records].</p>	<p>Examine: Identification and authentication policy; procedures addressing identifier management; information system design documentation; FiXs Rules and Guidance applicable; FIPS 201; NIST Special Publications 800-73, 800-76, 800-78; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records].</p>
PE	3.1	<p>(i) the access control system is consistent with FIPS 201 and NIST Special Publication 800-73 (where the Personal Identity Verification (PIV) credential is used as an identification token and token-based access control is employed); (ii) the access control system is consistent with NIST Special Publication 800-78 (where the token-based access control function employs cryptographic verification); and (iii) the access control system is consistent with NIST Special Publication 800-76 (where the token-based access control function employs biometric verification).</p>	<p>(i) the access control system is consistent with, FiXs Rules and Guidance, applicable FIPS 201 and NIST Special Publication 800-73 (where the FiXs Certified Credential is used as an identification token and token-based access control is employed); (ii) the access control system is consistent with FiXs Rules and Guidance, applicable NIST Special Publication 800-78 (where the token-based access control function employs cryptographic verification); and (iii) the access control system is consistent with FiXs Rules and Guidance and applicable NIST Special Publication 800-76 (where the</p>

			token-based access control function employs biometric verification).
PE	3.1	Examine: Physical and environmental protection policy; procedures addressing physical access control; FIPS 201; NIST Special Publications 800-73, 800-76, and 800-78; information system design documentation; other relevant documents or records]. (L) (M) (H)	Examine: Physical and environmental protection policy; procedures addressing physical access control; FiXs Rules and Guidance, applicable FIPS 201; NIST Special Publications 800-73, 800-76, and 800-78; information system design documentation; other relevant documents or records]. (L) (M) (H)
IA	4.1	Examine: Identification and authentication policy; procedures addressing identifier management; information system design documentation; FIPS 201; NIST Special Publications 800-73, 800-76, 800-78; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records]. (L) (M) (H)	Examine: Identification and authentication policy; procedures addressing identifier management; information system design documentation; FiXs Rules and Guidance ; FIPS 201; NIST Special Publications 800-73, 800-76, 800-78; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records]. (L) (M) (H)
AC	20.1	Examine: Access control policy; procedures addressing the use of external information systems; external information systems terms and conditions; list of types of applications accessible from external information systems; maximum FIPS 199 impact level for information processed, stored, or transmitted on external information systems; information system configuration settings and associated documentation; other relevant documents or records]. (L) (M) (H)	Access control policy; procedures addressing the use of external information systems; external information systems terms and conditions; list of types of applications accessible from external information systems; maximum FIPS 199 or FiXs Guidance for impact level for information processed, stored, or transmitted on external information systems; information system configuration settings and associated documentation; other relevant documents or records

AC	20.1	<p>(ii) the organization defines the maximum FIPS 199 for security category of information that can be processed, stored, and transmitted on the external information system; and (iii) the organization establishes terms and conditions for authorized individuals to access the information system from an external information system that include the types of applications that can be accessed on the organizational information system from the external information system and the maximum FIPS 199 security category of information that can be processed, stored, and transmitted on the external information system.</p>	<p>(ii) the organization defines the maximum FIPS 199 or FiXs Guidance for security category of information that can be processed, stored, and transmitted on the external information system; and (iii) the organization establishes terms and conditions for authorized individuals to access the information system from an external information system that include the types of applications that can be accessed on the organizational information system from the external information system and the maximum FIPS 199 or FiXs Guidance for security category of information that can be processed, stored, and transmitted on the external information system.</p>
AC	20.1	<p>Examine: Access control policy; procedures addressing the use of external information systems; external information systems terms and conditions; list of types of applications accessible from external information systems; maximum FIPS 199 impact level for information processed, stored, or transmitted on external information systems; information system configuration settings and associated documentation; other relevant documents or records].</p>	<p>Access control policy; procedures addressing the use of external information systems; external information systems terms and conditions; list of types of applications accessible from external information systems; maximum FIPS 199 or FiXs Guidance for impact level for information processed, stored, or transmitted on external information systems; information system configuration settings and associated documentation; other relevant documents or records</p>
MP	4.1	<p>(v) the organization protects information system media commensurate with the FIPS 199 security categorization of the information contained on the media.</p>	<p>(v) the organization protects information system media commensurate with the FIPS 199 or FiXs Guidance for security categorization of the information contained on the media.</p>
RA	2.1	<p>(ii) the security categorization is consistent with FIPS 199 and NIST Special Publication 800-60;</p>	<p>(ii) the security categorization is consistent with FiXs Guidance and applicable FIPS 199 and NIST Special Publication 800-60;</p>

RA	<p>2.1 Risk assessment policy; procedures addressing security categorization of organizational information and information systems; security planning policy and procedures; (ii) the security categorization is consistent with FIPS 199 and NIST Special Publication 800-60; NIST Special Publication 800-60; information system security plan; other relevant documents or records]. (L) (M) (H)</p>	<p>Risk assessment policy; procedures addressing security categorization of organizational information and information systems; security planning policy and procedures; (ii) the security categorization is consistent with FiXs Guidance and applicable FIPS 199 and NIST Special Publication 800-60; information system security plan; other relevant documents or records].</p>
----	---	--

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

FiXs ASSURANCE LEVEL IMPLEMENTATIONS

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

FiXs Credential Name	Assurance Level	Who
HSPD-12 Compatible Credentials	High (4)	<ul style="list-style-type: none"> • FiXs Member Company (or Subscriber) employees or contractors who perform work under a Federal government contract that includes the identity FAR clause.
		<ul style="list-style-type: none"> • Employees of a FiXs Member Company (or Subscriber) that requires an HSPD-12 Compatible Credential for some or all of their employees.
DoD Logical Access Credentials (LACS)/Physical Access Credentials (PACS) Credentials	High (4)	<ul style="list-style-type: none"> • FiXs Member Company (or Subscriber) employees or contractors on U.S. Department of Defense contracts who require long term (6 months or greater) access to DoD physical or logical resources.
		<ul style="list-style-type: none"> • FiXs Member Company (or Subscriber) employees who are required to authenticate to DoD resources at the highest level of assurance (Level 4).
DoD and Commercial use PACS/Short-term LACS Credentials	Medium High (3)	<ul style="list-style-type: none"> • FiXs Member Company (or Subscriber) employees or contractors who require physical access to a U.S. Department of Defense facility.
		<ul style="list-style-type: none"> • FiXs Member Company (or Subscriber) employees who are required to authenticate to DoD resources at a medium high level of assurance (3).
		<ul style="list-style-type: none"> • FiXs Member Company (or Subscriber) employees who do not have a requirement to authenticate to government facilities but do have a need for a medium high level of assurance for commercial use for physical/logical access.
Non-Security Clearance Contractor and Commercial use Credential	Medium High (3)	<ul style="list-style-type: none"> • Participants are those individuals needing physical access to Govt. facilities on a limited basis or for commercial uses not requiring access to government facilities. Examples of the would be: <ul style="list-style-type: none"> ○ Transportation Workers ○ Commercial Vendors <ul style="list-style-type: none"> ■ Delivery Personnel ■ Grounds personnel ■ Repair Technicians ■ Cleaning & Maintenance personnel

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

		<ul style="list-style-type: none"> ○ Facility Visitors for occasional official business ○ Leaders of tour groups, school personnel, on official tours ○ Health Care employees/patients ○ Financial/Insurance sector employees/customers
Enhanced First Responder	Medium High (3)	<ul style="list-style-type: none"> ● Participants who may need a FiXs Medium High Level (3) Enhanced First Responder Credential may include first responders identified by the authority having jurisdiction as holding sensitive positions or requiring access to secure Federal, State, or local facilities. These individuals may include but are not limited to: <ul style="list-style-type: none"> ○ Police Officers ○ Sheriffs Officers ○ Corrections Officers ○ Municipal, County, State and Industrial Fire Fighters ○ Emergency Medical Technicians and Paramedics
Enhanced Clinical First Responder Credential	Medium High (3)	<ul style="list-style-type: none"> ● Participants who may need a FiXs Medium High Level (3) Enhanced Clinical First Responder Credential may include first responders identified by the authority having jurisdiction as holding sensitive positions or requiring access to secure Federal, State, or local facilities. These individuals may include but are not limited to: <ul style="list-style-type: none"> ○ Physicians ○ Registered Nurses ○ <u>Behavioral Health Professionals[1]</u> ○ Advanced Practice Nurses[2] ○ Physicians Assistants ○ Dentists ○ Emergency Medical Technicians and Paramedics

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

Standard First Responder Credential	Medium (2)	<ul style="list-style-type: none"> • Participants who may need a FiXs Medium Level limited to: <ul style="list-style-type: none"> ◦ (2) Standard First Responder Credential may include but are not limited to: <ul style="list-style-type: none"> ◦ Municipal, County, State and Industrial Fire Fighters ◦ Emergency Medical Technicians ◦ Public Works Employees ◦ Red Cross, Salvation Army and other humanitarian volunteers ◦ National Citizen Corps Volunteers
Standard Clinical First Responder Credential	Medium (2)	<ul style="list-style-type: none"> • Participants who may need a FiXs Medium Level (2) Standard Clinical First Responder Credential may include but are not limited to: <ul style="list-style-type: none"> ◦ Pharmacists ◦ Licensed Practical Nurses ◦ Respiratory Therapists and Technicians ◦ Cardiovascular Technologist and Technicians ◦ Radiological Technologists & Technicians ◦ Surgical Technologists ◦ Medical and Clinical Laboratory Technologists
[1] Marriage and Family Therapists, Medical and Public Health Social Workers, Mental Health and Substance abuse Social Workers, Psychologists, and Mental Health Counselors. ESAR-VHP Interim Technical and Policy Guidelines, Standards, and Definitions – Version 2 June 2005 [2] Nurse Practitioners, Nurse Anesthetists, Certified Nurse Midwives, Clinical Nurses Specialists. ESAR-VHP Interim Technical and Policy Guidelines, Standards, and Definitions – Version 2 June 2005		

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

ACCESS CONTROL

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

FAMILY:	ACCESS CONTROL			Impact			Assessment Method			Assessment Results	FS/PS/NS
Num	ID	Assessment Procedure		L	M	H					
1	AC-1	ACCESS CONTROL POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.		L	M	H					FS/PS/NS
	AC-1.1	Determine if: (i) the organization develops and documents access control policy and procedures; (ii) the organization disseminates access control policy and procedures to appropriate elements within the organization; (iii) responsible parties within the organization periodically review access control policy and procedures; and (iv) the organization updates access control policy and procedures when organizational review indicates updates are required.					Examine: Access control policy and procedures; other relevant documents or records. (L) (M) (H) Interview: Organizational personnel with access control responsibilities. (H)				

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

	AC-1.2	Determine if: (i) the access control policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance; (ii) the access control policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and (iii) the access control procedures address all areas identified in the access control policy and address achieving policy-compliant implementations of all associated security controls.					Examine: Access control policy and procedures; other relevant documents or records. (L) (M) (H) Interview: Organizational personnel with access control responsibilities. (H)		
2	AC-2	ACCOUNT MANAGEMENT Control: The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts [Assignment: organization-defined frequency, at least annually].	L	M	H				FS/PS/NS

	AC-2.1	Determine if: (i) the organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts; (ii) the organization defines the frequency of information system account reviews; (iii) the organization reviews information system accounts at the organization-defined frequency, at least annually; and (iv) the organization initiates required actions on information system accounts based on the review				Examine: Access control policy; procedures addressing account management; information system security plan; list of active system accounts along with the name of the individual associated with each account; lists of recently transferred, separated, or terminated employees; list of recently disabled information system accounts along with the name of the individual associated with each account; system-generated records with user IDs and last login date; other relevant documents or records. (L) (M) (H) Interview: Organizational personnel with account management responsibilities. (M) (H)		
3	AC-2-1	ACCOUNT MANAGEMENT Control Enhancement: The organization employs automated mechanisms to support the management of information system accounts.	L	M	H			FS/PS/NS
	AC-2-1-1	Determine if the organization employs automated mechanisms to support information system account management functions.				Examine: Procedures addressing account management; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records]. (M) (H) Test: Automated mechanisms implementing account management functions. (H)		

Copyright© 2008
 Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

4	AC-2-2	ACCOUNT MANAGEMENT Control Enhancement: The information system automatically terminates temporary and emergency accounts after [Assignment: organization-defined time period for each type of account].	L	M	H			FS/PS/NS
	AC-2-2-1	Determine if: (i) the organization defines a time period after which the information system terminates temporary and emergency accounts; and (ii) the information system automatically terminates temporary and emergency accounts after organization-defined time period for each type of account.				Examine: Information system security plan; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. (M) (H) Test: Automated mechanisms implementing account management functions. (H)		
5	AC-2-3	ACCOUNT MANAGEMENT Control Enhancement: The information system automatically disables inactive accounts after [Assignment: organization-defined time period].	L	M	H			FS/PS/NS
	AC-2-3-1	Determine if: (i) the organization defines a time period after which the information system disables inactive accounts; and (ii) the information system automatically disables inactive accounts after organization-defined time period.				Examine: Procedures addressing account management; information system security plan; information system design documentation; information system configuration settings and associated documentation; information system-generated list of last login dates; information system-generated list of active accounts;		

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

						information system audit records; other relevant documents or records. (M) (H) Test: Automated mechanisms implementing account management functions. (H)		
6	AC-2(4)	ACCOUNT MANAGEMENT Control Enhancement: The organization employs automated mechanisms to audit account creation, modification, disabling, and termination actions and to notify, as required, appropriate individuals.	L	M	H			FS/PS/NS
	AC-2(4).1	Determine if: (i) the organization employs automated mechanisms to audit account creation, modification, disabling, and termination actions; and (ii) the organization employs automated mechanisms to notify, as required, appropriate individuals.				Examine: Procedures addressing account management; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. (M) (H) Test: Automated mechanisms implementing account management functions. (H)		
7	AC-3	ACCESS ENFORCEMENT Control: The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy.	L	M	H			FS/PS/NS

	AC-3.1	Determine if: (i) the information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy; and (ii) user privileges on the information system are consistent with the documented user authorizations.				Examine: Access control policy; procedures addressing access enforcement; information system configuration settings and associated documentation; list of assigned authorizations (user privileges); information system audit records; other relevant documents or records. (L) (M) (H) Test: Automated mechanisms implementing access enforcement policy. (H)		
8	AC-3-1	Control Enhancement: The information system restricts access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.	L	M	H			FS/PS/NS
	AC-3-1-1	Determine if: (i) the organization explicitly defines privileged functions and security-relevant information for the information system; (ii) the organization explicitly authorizes personnel access to privileged functions and security-relevant information in accordance with organizational policy; and (iii) the information system restricts access to privileged functions (deployed in hardware, software, and firmware) and security-relevant				Examine: Access control policy; procedures addressing access enforcement; list of privileged functions and security relevant information; information system configuration settings and associated documentation; list of assigned authorizations (user privileges); information system audit records; other relevant documents or records. (M) (H) Test: Automated mechanisms implementing access enforcement policy. (H)		

		information to explicitly authorized personnel (e.g., security administrators).					
9	AC-3- ICS-1	ACCESS ENFORCEMENT ICS Control Enhancements: The ICS requires dual authorization, based on approved organizational procedures, to privileged functions that have impacts on facility, public, and environmental safety.	L	M	H		FS/PS/NS
	AC- 3(ICS- 1)-1	Determine if: (i) the organization explicitly defines privileged functions for the ICS that have impacts on facility, public, and environmental safety; and (ii) the organization develops and approves procedures addressing dual authorization requirements for the ICS.				Examine: Access control policy; procedures addressing access enforcement and dual authorization; list of privileged functions for ICS; ICS configuration settings and associated documentation; list of assigned authorizations (user privileges); ICS audit records; other relevant documents or records. (M) (H)	
10	AC-4	INFORMATION FLOW ENFORCEMENT Control: The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.	L	M	H		FS/PS/NS

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

	AC-4.1	Determine if the information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.				Examine: Access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; information system baseline configuration; list of information flow authorizations; information system audit records; other relevant documents or records. (M) (H) Test: Automated mechanisms implementing information flow enforcement policy. (H)		
	AC-4.2	Determine if interconnection agreements address the types of permissible and impermissible flow of information between information systems and the required level of authorization to allow information flow as defined in the information flow enforcement policy and procedures.				Examine: Access control policy; procedures addressing information flow enforcement; information system interconnection agreements; information system configuration settings and associated documentation; list of information flow control authorizations; information system audit records; other relevant documents or records. (M) (H)		
11	AC-4-1	INFORMATION FLOW ENFORCEMENT Control Enhancement: The information system implements information flow control enforcement using explicit labels on information, source, and destination objects as a basis for flow control decisions.	L	M	H			FS/PS/NS

	AC-4-1-1	Determine if the information system implements information flow control enforcement using explicit labels on information, source, and destination objects as a basis for flow control decisions.				Examine: Access control policy; procedures addressing information flow enforcement; information system design documents; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. Test: Automated mechanisms implementing information flow enforcement policy.		
12	AC-4-2	INFORMATION FLOW ENFORCEMENT Control Enhancement: The information system implements information flow control enforcement using protected processing domains (e.g., domain type-enforcement) as a basis for flow control decisions.	L	M	H			FS/PS/NS
	AC-4-2-1	Determine if the information system implements information flow control enforcement using protected processing domains (e.g., domain type-enforcement) as a basis for flow control decisions.				Examine: Access control policy; procedures addressing information flow enforcement; information system design documents; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. Test: Automated mechanisms implementing information flow enforcement policy.		
13	AC-4-3	INFORMATION FLOW ENFORCEMENT	L	M	H			FS/PS/NS

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

		Control Enhancement: The information system implements information flow control enforcement using dynamic security policy mechanisms as a basis for flow control decisions.					
	AC-4-3-1	Determine if the information system implements information flow control enforcement using dynamic security policy mechanisms as a basis for flow control decisions.				Examine: Access control policy; procedures addressing information flow enforcement; information system design documents; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. Test: Automated mechanisms implementing information flow enforcement policy.	
14	AC-5	SEPARATION OF DUTIES Control: The information system enforces separation of duties through assigned access authorizations.	L	M	H		FS/PS/NS
	AC-5.1	Determine if: (i) the organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals; and (ii) the information system enforces separation of duties through assigned access authorizations.				Examine: Access control policy; procedures addressing separation of duties; information system configuration settings and associated documentation; list of separation of duties authorizations; information system audit records; other relevant documents or records. (M) (H) Interview: Organizational personnel with responsibilities for defining appropriate	

						divisions of responsibility and separation of duties. (H) Test: Automated mechanisms implementing separation of duties policy. (H)		
15	AC-6	LEAST PRIVILEGE Control: The information system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.	L	M	H			FS/PS/NS
	AC-6.1	Determine if: (i) the organization assigns the most restrictive set of rights/privileges or accesses needed by users for the performance of specified tasks; and (ii) the information system enforces the most restrictive set of rights/privileges or accesses needed by users.				Examine: Access control policy; procedures addressing least privilege; list of assigned access authorizations (user privileges); information system configuration settings and associated documentation; information system audit records; other relevant documents or records. (M) (H) Interview: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks. (H)		
16	AC-7	UNSUCCESSFUL LOGIN ATTEMPTS Control: The information system enforces a limit of [Assignment: organization-defined number] consecutive invalid access attempts by a user during a [Assignment:	L	M	H			FS/PS/NS

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

		organization-defined time period] time period. The information system automatically [Selection: locks the account/node for an [Assignment: organization-defined time period], delays next login prompt according to [Assignment: organization-defined delay algorithm.]] when the maximum number of unsuccessful attempts is exceeded.				
	AC-7.1	Determine if: (i) the organization defines the maximum number of consecutive invalid access attempts to the information system by a user and the time period in which the consecutive invalid access attempts occur; (ii) the information system enforces the organization-defined limit of consecutive invalid access attempts by a user during the organization-defined time period; (iii) the organization defines the time period for lock out mode or delay period; (iv) the organization selects either a lock out mode for the organization-defined time period or delays next login prompt for the organization-defined delay period for information system responses to consecutive invalid access attempts; (v) the information system enforces			Examine: Access control policy; procedures addressing unsuccessful logon attempts; information system security plan; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. (L) (M) (H) Test: Automated mechanisms implementing the access control policy for unsuccessful login attempts. (H)	

		the organization-selected lock out mode or delayed login prompt.					
17	AC-7(1)	UNSUCCESSFUL LOGIN ATTEMPTS Control Enhancement: The information system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.	L	M	H		FS/PS/NS
	AC-7(1).1	Determine if the information system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful login attempts is exceeded.				<p>Examine: Access control policy; procedures addressing unsuccessful logon attempts; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; information system audit records; other relevant documents or records.</p> <p>Test: Automated mechanisms implementing the access control policy for unsuccessful login attempts.</p>	
18	AC-8	SYSTEM USE NOTIFICATION Control: The information system displays an approved, system use notification message before granting system access informing	L	M	H		FS/PS/NS

		<p>potential users: (i) that the user is accessing a U.S. Government information system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring and recording. The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.</p>					
	AC-8.1	<p>Determine if:</p> <p>(i) the information system displays a system use notification message before granting system access informing potential users:</p> <ul style="list-style-type: none"> - that the user is accessing a U.S. Government information system; - that system usage may be monitored, recorded, and subject to audit; - that unauthorized use of the system is prohibited and subject to criminal and civil penalties; - that use of the system indicates 			<p>Examine: Access control policy; procedures addressing system use notification; information system notification messages; information system configuration settings and associated documentation; other relevant documents or records. (L) (M) (H)</p> <p>Test: Automated mechanisms implementing the access control policy for system use notification. (H)</p>		

		consent to monitoring and recording; (ii) the system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries). (iii) the organization approves the information system use notification message before its use; and (iv) the system use notification message remains on the screen until the user takes explicit actions to log on to the information system.					
19	AC-9	PREVIOUS LOGON NOTIFICATION Control: The information system notifies the user, upon successful logon, of the date and time of the last logon, and the number of unsuccessful logon attempts since the last successful logon.	L	M	H		FS/PS/NS
	AC-9.1	Determine if the information system, upon successful logon, displays the date and time of the last logon and the number of unsuccessful logon attempts since the last successful logon.				Examine: Access control policy; procedures addressing previous logon notification; information system notification messages; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. Test: Automated mechanisms implementing the access control policy for previous logon notification.	

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

20	AC-10	CONCURRENT SESSION CONTROL Control: The information system limits the number of concurrent sessions for any user to [Assignment: organization-defined number of sessions].	L	M	H			FS/PS/NS
	AC-10.1	Determine if: (i) the organization defines the maximum number of concurrent sessions for information system users; and (ii) the information system limits the number of concurrent sessions for users to the organization-defined number of sessions.				Examine: Access control policy; procedures addressing concurrent session control; information system configuration settings and associated documentation; information system security plan; other relevant documents or records. (H) Test: Automated mechanisms implementing the access control policy for concurrent session control. (H)		
21	AC-11	SESSION LOCK Control: The information system prevents further access to the system by initiating a session lock after [Assignment: organization-defined time period] of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures.	L	M	H			FS/PS/NS
	AC-11.1	Determine if: (i) the organization defines the time period of user inactivity that initiates a session lock within the information system;				Examine: Access control policy; procedures addressing session lock; information system design documentation; information system configuration settings and associated		

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

		(ii) the information system initiates a session lock after the organization-defined time period of inactivity; and (iii) the information system maintains the session lock until the user reestablishes access using appropriate identification and authentication procedures.				documentation; information system security plan; other relevant documents or records. (M) (H) Test: Automated mechanisms implementing the access control policy for session lock. (H)		
22	AC-12	SESSION TERMINATION Control: The information system automatically terminates a remote session after [Assignment: organization-defined time period] of inactivity.	L	M	H			FS/PS/NS
	AC-12.1	Determine if: (i) the organization defines the time period of user inactivity that initiates a remote session termination within the information system; and (ii) the information system automatically terminates a remote session after the organization-defined time period of inactivity.				Examine: Access control policy; procedures addressing session termination; information system design documentation; information system configuration settings and associated documentation; information system security plan; other relevant documents or records. (M) (H) Test: Automated mechanisms implementing the access control policy for session termination. (H)		
23	AC-12(1)	SESSION TERMINATION Control Enhancement: Automatic session termination applies to local and remote sessions.	L	M	H			FS/PS/NS
	AC-12(1).1	Determine if automatic session termination applies to local and remote sessions.				Examine: Access control policy; procedures addressing session termination; information system design		

						documentation; information system configuration settings and associated documentation; other relevant documents or records. (H) Test: Automated mechanisms implementing the access control policy for session termination. (H)		
24	AC-13	SUPERVISION AND REVIEW — ACCESS CONTROL Control: The organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls.	L	M	H			FS/PS/NS
	AC-13.1	Determine if the organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls.				Examine: Access control policy; procedures addressing supervision and review of access control enforcement and usage; organizational records of supervisory notices of disciplinary actions to users; information system exception reports; other relevant documents or records. (L) (M) (H) Interview: Organizational personnel with supervisory and access control responsibilities. (H)		
25	AC-13	SUPERVISION AND REVIEW — ACCESS CONTROL Control Enhancement: (1) The organization employs automated mechanisms to facilitate the review of user activities.	L	M	H			FS/PS/NS

	AC-13-1-1	Determine if the organization employs automated mechanisms within the information system to support and facilitate the review of user activities.				Examine: Access control policy; procedures addressing supervision and review of access control enforcement and usage; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. (M) (H) Test: Automated mechanisms supporting the access control policy for supervision and review of user activities. (H)		
26	AC-14	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION Control: The organization identifies and documents specific user actions that can be performed on the information system without identification or authentication.	L	M	H			FS/PS/NS
	AC-14.1	Determine if the organization identifies and documents specific user actions that can be performed on the information system without identification or authentication.				Examine: Access control policy; procedures addressing permitted actions without identification and authentication; information system configuration settings and associated documentation; information system security plan; other relevant documents or records. (L) (M) (H) Test: Automated mechanisms implementing the access control policy for permitted actions without identification and authentication. (H)		

27	AC-14-1	<p>PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION</p> <p>Control Enhancement:</p> <p>The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives.</p>	L	M	H			FS/PS/NS
	AC-14-1-1	<p>Determine if the organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives.</p>				<p>Examine: Access control policy; procedures addressing permitted actions without identification and authentication; information system configuration settings and associated documentation; list of organization-defined actions that can be performed without identification and authentication; other relevant documents or records. (M) (H)</p> <p>Interview: Organizational personnel with responsibilities for defining permitted actions without identification and authentication. (H)</p>		
28	AC-15	<p>AUTOMATED MARKING</p> <p>Control: The information system marks output using standard naming conventions to identify any special dissemination, handling, or distribution instructions.</p>	L	M	H			FS/PS/NS

	AC-15.1	Determine if: (i) the organization identifies standard naming conventions for information system output; and (ii) the information system marks output using standard naming conventions to identify any special dissemination, handling, or distribution instructions.				Examine: Access control policy; procedures for addressing automated marking of information system output; information system output; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. (H) Interview: Organizational personnel with responsibilities for defining special dissemination, handling, and marking instructions for information system output. (H) Test: Automated mechanisms implementing automated marking of information system output. (H)		
28	AC-16	AUTOMATED LABELING Control: The information system appropriately labels information in storage, in process, and in transmission.	L	M	H			FS/PS/NS
	AC-16.1	Determine if the information system appropriately labels information in storage, in process, and in transmission.				Examine: Access control policy; procedures addressing automated (internal) labeling of information within the information system; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. Test: Automated mechanisms		

						implementing automated (internal) labeling within the information system.		
29	AC-17	REMOTE ACCESS Control: The organization authorizes, monitors, and controls all methods of remote access to the information system.	L	M	H			FS/PS/NS
	AC-17.1	Determine if the organization documents, monitors, and controls all methods of remote access to the information system.				Examine: Access control policy; procedures addressing remote access to the information system; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. (L) (M) (H) Interview: Organizational personnel with remote access authorization, monitoring, and control responsibilities. (M) (H)		
30	AC-17-1	REMOTE ACCESS Control Enhancement: The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.	L	M	H			FS/PS/NS
	AC-17-1-1	Determine if the information system employs automated mechanisms to facilitate the monitoring and control of remote access methods.				Examine: Access control policy; procedures addressing remote access to the information system; information system configuration settings and associated documentation; other relevant documents or records. (M) (H)		

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

							Test: Automated mechanisms implementing the access control policy for remote access. (H)		
31	AC-17-2	REMOTE ACCESS Control Enhancement: The organization uses cryptography to protect the confidentiality and integrity of remote access sessions.	L	M	H				FS/PS/NS
	AC-17-2-1	Determine if the information system employs cryptography to protect the confidentiality and integrity of remote access sessions				Examine: Access control policy; procedures addressing remote access to the information system; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. (M) (H) Test: Automated mechanisms implementing cryptographic protections for remote access. (H)			
32	AC-17-3	REMOTE ACCESS Control Enhancement: The organization controls all remote accesses through a limited number of managed access control points.	L	M	H				FS/PS/NS
	AC-17-3-1	Determine if: (i) the organization defines managed access control points for remote access to the information system; and (ii) the information system controls all				Examine: Access control policy; procedures addressing remote access to the information system; information system design documentation; list of managed access control points; information system configuration settings and associated documentation; information system audit records; other			

		remote accesses through a limited number of managed access control points.				relevant documents or records. (M) (H) Test: Automated mechanisms implementing the access control policy for remote access. (H)		
33	AC-17-4	REMOTE ACCESS Control Enhancement: The organization permits remote access for privileged functions only for compelling operational needs and documents the rationale for such access in the security plan for the information system.	L	M	H			FS/PS/NS
	AC-17-4-1	Determine if: (i) the organization defines the situations and compelling operational needs when remote access to privileged functions on the information system is allowed; and (ii) the organization permits remote access for privileged functions only for compelling operational needs and documents the rationale for such access in the security plan for the information system.				Examine: Access control policy; procedures addressing remote access to the information system; information system configuration settings and associated documentation; information system security plan; information system audit records; other relevant documents or records. (M) (H) Test: Automated mechanisms implementing the access control policy for remote access. (H)		
34	AC-18	WIRELESS ACCESS RESTRICTIONS Control: The organization: (i) establishes usage restrictions and implementation guidance for wireless technologies; and (ii)	L	M	H			FS/PS/NS

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

		authorizes, monitors, controls wireless access to the information system.					
	AC-18.1	Determine if: (i) the organization establishes usage restrictions and implementation guidance for wireless technologies; (ii) the organization authorizes, monitors, and controls wireless access to the information system; and (iii) the wireless access restrictions are consistent with NIST Special Publications 800-48 and 800-97.				Examine: Access control policy; procedures addressing wireless implementation and usage (including restrictions); NIST Special Publications 800-48 and 800-97; activities related to wireless authorization, monitoring, and control; information system audit records; other relevant documents or records. (L) (M) (H) Test: Wireless access usage and restrictions. (M) (H)	
35	AC-18-1	WIRELESS ACCESS RESTRICTIONS Control Enhancement: The organization uses authentication and encryption to protect wireless access to the information system.	L	M	H		FS/PS/NS
	AC-18-1-1	Determine if the organization uses authentication and encryption to protect wireless access to the information system.				Examine: Access control policy; procedures addressing wireless implementation and usage (including restrictions); information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. (M) (H) Test: Automated mechanisms implementing the access control policy	

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

						for wireless access to the information system. (H)		
36	AC-18-2	<p>WIRELESS ACCESS RESTRICTIONS</p> <p>Control Enhancement: The organization scans for unauthorized wireless access points [Assignment: organization-defined frequency] and takes appropriate action if such an access points are discovered.</p>	L	M	H			FS/PS/NS
	AC-18-2-1	<p>Determine if:</p> <ul style="list-style-type: none"> (i) the organization defines the frequency of scans for unauthorized wireless access points; and (ii) the organization scans for unauthorized wireless access points in accordance with organization-defined frequency and takes appropriate action if such an access points are discovered. 				<p>Examine: Access control policy; procedures addressing wireless implementation and usage (including restrictions); wireless scanning reports; other relevant documents or records. (H)</p> <p>Test: Scanning procedure for unauthorized wireless access points. (H)</p>		
37	AC-19	<p>ACCESS CONTROL FOR PORTABLE AND MOBILE DEVICES</p> <p>Control: The organization: (i) establishes usage restrictions and implementation guidance for organization-controlled portable and mobile devices; and (ii) authorizes, monitors, and controls device access to organizational information systems.</p>	L	M	H			FS/PS/NS

	AC-19.1	Determine if: (i) the organization defines a mandatory suite of protective software and security protocols to be installed on and executed by the information system and portable and mobile devices; (ii) the organization establishes usage restrictions and implementation guidance for organization-controlled portable and mobile devices; and (iii) the organization authorizes, monitors, and controls device access to organizational information systems.				Examine: Access control policy; procedures addressing access control for portable and mobile devices; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. (M) (H) Interview: Organizational personnel who use portable and mobile devices to access the information system. (M) (H) Test: Automated mechanisms implementing access control policy for portable and mobile devices. (H)		
38	AC-20	USE OF EXTERNAL INFORMATION SYSTEMS Control: The organization establishes terms and conditions for authorized individuals to: (i) access the information system from an external information system; and (ii) process, store, and/or transmit organization-controlled information using an external information system.	L	M	H			FS/PS/NS

	AC-20.1	Determine if: (i) the organization defines the types of applications that can be accessed from the external information system; (ii) the organization defines the maximum FIPS 199 or FiXs Guidance for security category of information that can be processed, stored, and transmitted on the external information system; and (iii) the organization establishes terms and conditions for authorized individuals to access the information system from an external information system that include the types of applications that can be accessed on the organizational information system from the external information system and the maximum FIPS 199 or FiXs Guidance for security category of information that can be processed, stored, and transmitted on the external information system.				Examine: Access control policy; procedures addressing the use of external information systems; external information systems terms and conditions; list of types of applications accessible from external information systems; maximum FIPS 199 or FiXs Guidance for impact level for information processed, stored, or transmitted on external information systems; information system configuration settings and associated documentation; other relevant documents or records. (L) (M) (H) Interview: Organizational personnel who use external information systems to access the information system. (M) (H)		
39	AC-20(1)	USE OF EXTERNAL INFORMATION SYSTEMS Control Enhancement: The organization prohibits authorized individuals from using an external information system to access the information system or to process, store, or transmit organization-controlled information	L	M	H			FS/PS/NS

		except in situations where the organization: (i) can verify the employment of required security controls on the external system as specified in the organization's information security policy and system security plan; or (ii) has approved information system connection or processing agreements with the organizational entity hosting the external information system.					
	AC-20(1).1	<p>Determine if the organization prohibits authorized individuals from using an external information system to access the information system or to process, store, or transmit organization-controlled information except in situations where the organization:</p> <ul style="list-style-type: none"> - verifies, for authorized exceptions, the employment of required security controls on the external system as specified in the organization's information security policy and system security plan when allowing connections to the external information system; or - approves, for authorized exceptions, information system connection or processing 			<p>Examine: Access control policy; procedures addressing the use of external information systems; information system security plan; information system configuration settings and associated documentation; information system connection or processing agreements; account management documents; other relevant documents or records. (M) (H)</p>		

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

AWARENESS & TRAINING

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

FAMILY:		AWARENESS & TRAINING	Impact			Assessment Method	Assessment Results	FS/PS/NS
Num	ID	Assessment Procedure	L	M	H			FS/PS/NS
1	AT-1	<p>SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES</p> <p>Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.</p>						
	AT-1.1	<p>Determine if:</p> <ul style="list-style-type: none"> (i) the organization develops and documents security awareness and training policy and procedures; (ii) the organization disseminates security awareness and training policy and procedures to appropriate elements within the organization; (iii) responsible parties within the organization periodically review security awareness and training policy and procedures; and 				<p>Examine: Security awareness and training policy and procedures; other relevant documents or records. (L) (M) (H)</p> <p>Interview: Organizational personnel with security awareness and training responsibilities. (H)</p>		

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

		(iv) the organization updates security awareness and training policy and procedures when organizational review indicates updates are required.				
	AT-1.2	Determine if: (i) the security awareness and training policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance; (ii) the security awareness and training policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and (iii) the security awareness and training procedures address all areas identified in the security awareness and training policy and address achieving policy-compliant implementations of all associated security controls.			Examine: Security awareness and training policy and procedures; other relevant documents or records. (L) (M) (H) Interview: Organizational personnel with security awareness and training responsibilities. (H)	
2	AT-2	SECURITY AWARENESS Control: The organization provides basic security awareness training to all information system users (including managers and senior executives) before authorizing access to the system, when required by system changes, and [Assignment: organization-defined]	L	M	H	FS/PS/NS

		frequency, at least annually] thereafter.					
	AT-2.1	Determine if: (i) the organization provides basic security awareness training to all information system users (including managers and senior executives) before authorizing access to the system and when required by system changes; (ii) the security awareness training is consistent with applicable regulations and NIST Special Publication 800-50; (iii) the security awareness and training materials address the specific requirements of the organization and the information systems to which personnel have authorized access; (iv) the organization defines the frequency of refresher security awareness training; and (v) the organization provides refresher security awareness training in accordance with organization-defined frequency, at least annually.			Examine: Security awareness and training policy; procedures addressing security awareness training implementation; NIST Special Publication 800-50; appropriate codes of federal regulations; security awareness training curriculum; security awareness training materials; information system security plan; other relevant documents or records. (L) (M) (H)		
3	AT-3	SECURITY TRAINING Control: The organization identifies personnel that have significant information system security roles and responsibilities during the system development life cycle,	L	M	H		FS/PS/NS

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

		documents those roles and responsibilities, and provides appropriate information system security training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) [Assignment: organization-defined frequency] thereafter.				
AT-3.1	Determine if: (i) the organization identifies personnel with significant information system security responsibilities and documents those roles and responsibilities; (ii) the organization provides security training to personnel with identified information system security roles and responsibilities before authorizing access to the system or performing assigned duties and when required by system changes; (iii) the security training materials address the procedures and activities necessary to fulfill the organization-defined roles and responsibilities for information system security; (iv) the security training is consistent with applicable regulations and NIST Special Publication 800-50; (v) the organization defines the frequency of refresher security training; and			Examine: Security awareness and training policy; procedures addressing security training implementation; NIST Special Publication 800-50; codes of federal regulations; security training curriculum; security training materials; information system security plan; other relevant documents or records. (L) (M) (H) Interview: Organizational personnel with significant information system security responsibilities. (H)		

		(vi) the organization provides refresher security training in accordance with organization-defined frequency, at least annually.					
4	AT-4	SECURITY TRAINING RECORDS Control: The organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training.					FS/PS/NS
	AT-4.1	Determine if the organization monitors and documents basic security awareness training and specific information system security training.				Examine: Security awareness and training policy; procedures addressing security training records; security awareness and training records; other relevant documents or records. (L) (M) (H)	
5	AT-5	CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS Control: The organization establishes and maintains contacts with special interest groups, specialized forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations to stay up to date with the latest recommended security practices, techniques, and technologies and to share the latest security-related information including threats, vulnerabilities, and incidents.	L	M	H		FS/PS/NS

AT-5.1	Determine if the organization establishes and maintains contact with special interest groups, specialized forums, or professional associations to keep current with state-of-the-practice security techniques and technologies and to share security-related information.			Examine: Security awareness and training policy; procedures addressing contacts with security groups and associations; list of organization-defined key contacts to obtain ongoing information system security knowledge, expertise, and general information; other relevant documents or records.	
FS - Fully Satisfied PS - Partially Satisfied NS - Not Satisfied Impacts: Low Medium High Assessment Methods: Interview Demonstrate Test Observe					Assessment Results
					FS 0
					PS 0
					NS 0
					Total 0

AUDIT & ACCOUNTABILITY

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

FAMILY : AUDIT & ACCOUNTABILITY			Impact			Assessment Method	Assessment Results	FS/PS/NS
Num	ID	Assessment Procedure	L	M	H			
1	AU-1	AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.	L	M	H			FS/PS/NS
	AU-1.1	Determine if: (i) the organization develops and documents audit and accountability policy and procedures; (ii) the organization disseminates audit and accountability policy and procedures to appropriate elements within the organization; (iii) responsible parties within the organization periodically review audit and accountability policy and procedures; and (iv) the organization updates audit and accountability policy and				Examine: Audit and accountability policy and procedures; other relevant documents or records]. (L) (M) Interview: Organizational personnel with audit and accountability responsibilities. (H)		

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

		procedures when organizational review indicates updates are required.					
	AU-1.2	Determine if: (i) the audit and accountability policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance; (ii) the audit and accountability policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and (iii) the audit and accountability procedures address all areas identified in the audit and accountability policy and address achieving policy-compliant implementations of all associated security controls.				Examine: Audit and accountability policy and procedures; other relevant documents or records]. (L) (M) (H) Interview: Organizational personnel with audit and accountability responsibilities. (H)	
2	AU-2	AUDITABLE EVENTS Control: The information system generates audit records for the following events: [Assignment: organization-defined auditable events].	L	M	H		FS/PS/NS

	AU-2.1	Determine if: (i) the organization defines information system auditable events; (ii) the organization-defined auditable events are adequate to support after-the-fact investigations of security incidents; and (iii) the information system generates audit records for the organization-defined auditable events.					
3	AU-2-1	AUDITABLE EVENTS Control Enhancement: The information system provides the capability to compile audit records from multiple components throughout the system into a system wide (logical or physical), time-correlated audit trail.	L	M	H		FS/PS/NS
	AU-2-1-1	Determine if: (i) the organization defines the components of the information system that generate audit records; and (ii) the information system compiles audit records from the organization-defined (multiple) components within the information system into a system wide (logical or physical), time-correlated audit trail.				Examine: Audit and accountability policy; procedures addressing auditable events; information system design documentation; information system configuration settings and associated documentation; list of organization-defined auditable events; information system audit records; other relevant documents or records. (H) Test: Automated mechanisms	

						implementing a system-wide auditing capability]. (H)		
4	AU-2-2	AUDITABLE EVENTS Control Enhancement: The information system provides the capability to manage the selection of events to be audited by individual components of the system.	L	M	H			FS/PS/NS
	AU-2-2-1	Determine if the information system provides the capability to manage the selection of events to be audited by individual components of the system.				Examine: Audit and accountability policy; procedures addressing auditable events; information system design documentation; information system configuration settings and associated documentation; list of organization-defined audit events; information system audit records; other relevant documents or records. (H) Test: Automated mechanisms implementing Information system auditing for the specified components of the information system. (H)		
5	AU-2-3	AUDITABLE EVENTS Control Enhancement: The organization periodically reviews and updates the list of organization-defined audit events.	L	M	H			FS/PS/NS

	AU-2-3-1	Determine if the organization periodically reviews and updates the list of organization-defined auditable events.				Examine: [SELECT FROM: Audit and accountability policy; procedures addressing auditable events; list of organization-defined auditable events; information system audit records; information system incident reports; other relevant documents or records]. (M) (H) Interview: [SELECT FROM: Organizational personnel with auditing and accountability responsibilities]. (H)		
6	AU-3	CONTENT OF AUDIT RECORDS Control: The information system produces audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.	L	M	H			FS/PS/NS
	AU-3.1	Determine if the information system audit records capture sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.				Examine: Audit and accountability policy; procedures addressing content of audit records; list of organization-defined auditable events; information system audit records; information system incident reports; other relevant documents or records. (L) (M) (H) Test: Automated mechanisms implementing information		

						system auditing of auditable events. (H)		
7	AU-3-1	CONTENT OF AUDIT RECORDS Control Enhancement: The information system provides the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.	L	M	H			FS/PS/NS
	AU-3-1-1	Determine if the information system provides the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.				Examine: Audit and accountability policy; procedures addressing content of audit records; information system design documentation; information system security plan; information system configuration settings and associated documentation; other relevant documents or records]. (M) (H) Test: Information system audit capability to include more detailed information in audit records for audit events identified by type, location, or subject]. (H)		

8	AU-3-2	CONTENT OF AUDIT RECORDS Control Enhancement: The information system provides the capability to centrally manage the content of audit records generated by individual components throughout the system.	L	M	H			FS/PS/NS
	AU-3-2-1	Determine if the information system provides the capability to centrally manage the content of audit records generated from multiple components throughout the system.				<p>Examine: Audit and accountability policy; procedures addressing content of audit records; information system design documentation; list of organization-defined auditable events; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. (H)</p> <p>Test: Automated mechanisms implementing information system auditing with central management capability. (H)</p>		
9	AU-4	AUDIT STORAGE CAPACITY Control: The organization allocates sufficient audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.	L	M	H			FS/PS/NS

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

	AU-4.1	Determine if: (i) the organization defines audit record storage capacity for the information system components that generate audit records; and (ii) the organization establishes information system configuration settings to reduce the likelihood of the audit record storage capacity being exceeded.				Examine: Audit and accountability policy; procedures addressing audit storage capacity; information system design documentation; organization-defined audit record storage capacity for information system components generating audit records; list of organization-defined auditable events; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. (L) (M) (H)	
10	AU-5	RESPONSE TO AUDIT PROCESSING FAILURES Control: The information system alerts appropriate organizational officials in the event of an audit processing failure and takes the following additional actions: [Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)].	L	M	H		FS/PS/NS

	AU-5.1	Determine if: (i) the organization defines actions to be taken in the event of an audit processing failure; (ii) the organization defines personnel to be notified in case of an audit processing failure; and (iii) the information system alerts appropriate organizational officials and takes any additional organization-defined actions in the event of an audit failure or audit storage capacity being reached.				Examine: Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; information system security plan; information system configuration settings and associated documentation; list of personnel to be notified in case of an audit processing failure; information system audit records; other relevant documents or records. (L) (M) (H) Test: Automated mechanisms implementing information system response to audit processing failures. (H)	
11	AU-5.1	RESPONSE TO AUDIT PROCESSING FAILURES Control Enhancement: The information system provides a warning when allocated audit record storage volume reaches [Assignment: organization-defined percentage of maximum audit record storage capacity].	L	M	H		FS/PS/NS

	AU-5-1-1	Determine if: (i) the organization defines percentage of maximum audit record storage capacity; (ii) the information system provides a warning when the allocated audit record storage volume reaches the organization-defined percentage of maximum audit record storage capacity.			Examine: Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; information system security plan; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. (H) Test: Automated mechanisms implementing audit storage limit warnings. (H)		
12	AU-5-2	RESPONSE TO AUDIT PROCESSING FAILURES Control Enhancement: The information system provides a real-time alert when the following audit failure events occur: [Assignment: organization-defined audit failure events requiring real-time alerts].	L	M	H		FS/PS/NS
	AU-5-2-1	Determine if: (i) the organization defines audit failure events requiring real-time alerts; and (ii) the information system provides a real-time alert when organization-defined audit failure events occur.			Examine: Audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; information system security plan; information system configuration settings and associated documentation;		

						information system audit records; other relevant documents or records. (H) Test: Automated mechanisms implementing real time audit alerts. (H)		
13	AU-6	AUDIT MONITORING, ANALYSIS, AND REPORTING Control: The organization regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.	L	M	H			FS/PS/NS
	AU-6.1	Determine if: (i) the organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity;(ii) the organization investigates suspicious activity or suspected violations; (iii) the organization reports findings of inappropriate/unusual activities, suspicious behavior, or suspected violations to appropriate officials; and (iv)the organization takes necessary actions in response to the reviews/analyses of audit records.						

14	AU-6-1	<p>AUDIT MONITORING, ANALYSIS, AND REPORTING</p> <p>Control Enhancement: The organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.</p>	L	M	H			FS/PS/NS
	AU-6-1-1	Determine if the organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.				<p>Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. (H)</p> <p>Test: Automated mechanisms integrating audit monitoring, analysis, and reporting into an organizational process for investigation and response to suspicious activities. (H)</p>		
15	AU-6-2	<p>AUDIT MONITORING, ANALYSIS, AND REPORTING</p> <p>Control Enhancement: The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications:</p>	L	M	H			FS/PS/NS

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

		[Assignment: organization-defined list of inappropriate or unusual activities that are to result in alerts].						
	AU-6-2-1	Determine if: (i) the organization defines inappropriate or unusual activities with security implications; and (ii) the organization employs automated mechanisms to alert security personnel of the occurrence of any organization-defined inappropriate or unusual activities with security implications.				Examine: Audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; information system design documentation; information system configuration settings and associated documentation; information system security plan; information system audit records; other relevant documents or records. (M) (H) Test: Automated mechanisms implementing security alerts. (M) (H)		
16	AU-7	AUDIT REDUCTION AND REPORT GENERATION Control: The information system provides an audit reduction and report generation capability.	L	M	H		FS/PS/NS	

	AU-7.1	Determine if the information system provides an audit reduction and report generation capability.				Examine: Audit and accountability policy; procedures addressing audit reduction and report generation; information system design documentation; audit reduction, review, and reporting tools; information system audit records; other relevant documents or records. (M) (H) Interview: Organizational personnel with information system audit monitoring, analysis, and reporting responsibilities. (H) Test: Audit reduction and report generation capability. (M) (H)	
17	AU-7-1	AUDIT REDUCTION AND REPORT GENERATION Control Enhancement: The information system provides the capability to automatically process audit records for events of interest based upon selectable, event criteria.	L	M	H		FS/PS/NS

	AU-7-1-1	Determine if the information system provides the capability to automatically process audit records for events of interest based upon selectable, event criteria.				Examine: Audit and accountability policy; procedures addressing audit reduction and report generation; information system design documentation; information system configuration settings and associated documentation; audit reduction, review, and reporting tools; information system audit records; other relevant documents or records. (M) (H) Test: Audit reduction and report generation capability. (H)		
18	AU-8	TIME STAMPS Control: The information system provides time stamps for use in audit record generation.	L	M	H			FS/PS/NS
	AU-8.1	Determine if the information system provides time stamps for use in audit record generation.				Examine: Audit and accountability policy; procedures addressing time stamp generation; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. (L) (M) (H) Test: Automated mechanisms implementing time stamp generation. (M) (H) APPENDIX		

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

19	AU-8-1	TIME STAMPS Control Enhancement: The organization synchronizes internal information system clocks [Assignment: organization-defined frequency].	L	M	H			FS/PS/NS
	AU-8-1-1	Determine if: (i) the organization defines the frequency of internal clock synchronization for the information system; and (ii) the organization synchronizes internal information system clocks periodically in accordance with organization-defined frequency.				Examine: Audit and accountability policy; procedures addressing time stamp generation; information system security plan; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. (M) (H) Test: Automated mechanisms implementing internal information system clock synchronization. (H)		
20	AU-9	PROTECTION OF AUDIT INFORMATION Control: The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	L	M	H			FS/PS/NS

	AU-9.1	Determine if the information system protects audit information and audit tools from unauthorized access, modification, and deletion.				Examine: Audit and accountability policy; procedures addressing protection of audit information; access control policy and procedures; information system design documentation; information system configuration settings and associated documentation, information system audit records; audit tools; other relevant documents or records. (L) (M) (H) Test: Automated mechanisms implementing audit information protection. (H)		
21	AU-9-1	PROTECTION OF AUDIT INFORMATION Control Enhancement: The information system produces audit records on hardware-enforced, write-once media.	L	M	H			FS/PS/NS
	AU-9-1-1	Determine if the information system produces audit information on hardware-enforced, write-once media.				Examine: Audit and accountability policy; procedures addressing protection of audit information; access control policy and procedures; information system design documentation; information system hardware settings; information system configuration settings and associated documentation, information		

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

						system audit records; other relevant documents or records. Test: Media storage devices.		
22	AU-10	NON-REPUDIATION Control: The information system provides the capability to determine whether a given individual took a particular action.	L	M	H			FS/PS/NS
	AU-10.1	Determine if the information system provides the capability to determine whether a given individual took a particular action (e.g., created information, sent a message, approved information [e.g., to indicate concurrence or sign a contract] or received a message).				Examine: Audit and accountability policy; procedures addressing non-repudiation; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. Test: Automated mechanisms implementing non-repudiation capability.		
23	AU-11	AUDIT RECORD RETENTION Control: The organization retains audit records for [Assignment: organization-defined time period] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	L	M	H			FS/PS/NS

	AU-11.1	Determine if: (i) the organization defines the retention period for audit records generated by the information system; and (ii) the organization retains information system audit records for the organization-defined time period to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.			Examine: Audit and accountability policy; procedures addressing audit record retention; organization-defined retention period for audit records; information system audit records; other relevant documents or records. (L) (M) Interview: Organizational personnel with information system audit record retention responsibilities. (H)		
FS - Fully Satisfied PS - Partially Satisfied NS - Not Satisfied							Assessment Results
Impacts: Low Medium High							FS 0
Assessment Methods: Interview Demonstrate Test Observe							PS 0
							NS 0
							Total 0

CERTIFICATION, ACCREDITATION & SECURITY ASSESSMENTS

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

FAMILY: CERTIFICATION, ACCREDITATION & SECURITY ASSESSMENTS			Impact			Assessment Method	Assessment Results	FS/PS/NS
Num	ID	Assessment Procedure	L	M	H			
1	CA-1	<p>CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENT POLICIES AND PROCEDURES</p> <p>Control: The organization develops, disseminates, and periodically reviews/updates: (i) formal, documented, security assessment and certification and accreditation policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security assessment and certification and accreditation policies and associated assessment, certification, and accreditation controls.</p>						FS/PS/NS
	CA-1.1	<p>Determine if:</p> <ul style="list-style-type: none"> (i) the organization develops and documents security assessment and certification and accreditation policies and procedures; (ii) the organization disseminates security assessment and certification and accreditation policies and procedures to appropriate elements within the organization; (iii) responsible parties within the organization periodically review policy and procedures; and (iv) 				<p>Examine: Security assessment and certification and accreditation policies and procedures; other relevant documents or records. (L) (M) (H)</p> <p>Interview: Organizational personnel with security assessment and certification and accreditation responsibilities. (H)</p>		

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

		the organization updates security assessment and certification and accreditation policies and procedures when organizational review indicates updates are required.					
	CA-1.2	Determine if: (i) the security assessment and certification and accreditation policies address purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance; (ii) the security assessment and certification and accreditation policies are consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and (iii) the security assessment and certification and accreditation procedures address all areas identified in the security assessment and certification and accreditation policies and address achieving policy-compliant implementations of all associated security controls.				Examine: Security assessment and certification and accreditation policies and procedures; other relevant documents or records. (L) (M) (H) Interview: Organizational personnel with security assessment and certification and accreditation responsibilities. (H)	
2	CA-2	SECURITY ASSESSMENTS Control: The organization conducts an assessment of the security controls in the information system [Assignment: organization-defined frequency, at least annually] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.	L	M	H		FS/PS/NS

CA-2.1	<p>Determine if:</p> <ul style="list-style-type: none"> (i) the information system is in the inventory of major information systems; and (ii) the organization conducts an assessment of the security controls in the information system at an organization-defined frequency, at least annually. 			<p>Examine: Security assessment policy; procedures addressing security assessments; information system security plan; security assessment plan; security assessment report; assessment evidence; other relevant documents or records. (L) (M) (H)</p>	
CA-3	<p>INFORMATION SYSTEM CONNECTIONS Control: The organization authorizes all connections from the information system to other information systems outside of the accreditation boundary through the use of system connection agreements and monitors/controls the system connections on an ongoing basis.</p>	L	M	H	FS/PS/NS

CA-3.1		Determine if: (i) the organization identifies all connections to external information systems (i.e., information systems outside of the accreditation boundary); (ii) the organization authorizes all connections from the information system to external information systems through the use of system connection agreements; (iii) the organization monitors/controls the system interconnections on an ongoing basis; and (iv) information system connection agreements are consistent with NIST Special Publication 800-47.				Examine: Access control policy; procedures addressing information system connections; NIST Special Publication 800-47; system and communications protection policy; personnel security policy; information system connection agreements; information system security plan; information system design documentation; information system configuration management and control documentation; security assessment report; plan of action and milestones; other relevant documents or records. (L) (M) (H) Interview: Organizational personnel with responsibility for developing, implementing, or approving information system connection agreements. (H)	
3	CA-4	SECURITY CERTIFICATION Control: The organization conducts an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.	L	M	H		FS/PS/NS

	CA-4.1	Determine if: (i) the organization conducts an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system; and (ii) the organization employs a security certification process in accordance with OMB policy and NIST Special Publications 800-37 and 800-53A.			Examine: Certification and accreditation policy; procedures addressing security certification; information system security plan; security assessment plan; security assessment report; assessment evidence; plan of action and milestones; other relevant documents or records. (L) (M) (H) Interview: Organizational personnel with security certification responsibilities]. (H)		
4	CA-4-1	SECURITY CERTIFICATION Control Enhancement: The organization employs an independent certification agent or certification team to conduct an assessment of the security controls in the information system.	L	M	H		FS/PS/NS
	CA-4-1-1	Determine if the organization employs an independent certification agent or certification team to conduct an assessment of the security controls in the information system.				Examine: Certification and accreditation policy; procedures addressing security certification; security accreditation package (including information system security plan, security assessment report, plan of action and milestones, authorization statement); other relevant documents or records. (M) (H)	

5	CA-5	<p>PLAN OF ACTION AND MILESTONES</p> <p>Control: The organization develops and updates [Assignment: organization-defined frequency], a plan of action and milestones for the information system that documents the organization's planned, implemented, and evaluated remedial actions to correct deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.</p>	L	M	H			FS/PS/NS
6	CA-5.1	<p>Determine if:</p> <ul style="list-style-type: none"> (i) the organization develops and updates at the organization-defined frequency, a plan of action and milestones for the information system; and (ii) the plan of action and milestones documents the planned, implemented, and evaluated remedial actions by the organization to correct any deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the information system. 				<p>Examine: Certification and accreditation policy; procedures addressing plan of action and milestones; information system security plan; security assessment plan; security assessment report; assessment evidence; plan of action and milestones; other relevant documents or records. (L) (M) (H)</p> <p>Interview: Organizational personnel with plan of action and milestones development and implementation responsibilities. (H)</p>		
6	CA-6	<p>SECURITY ACCREDITATION</p> <p>Control: The organization authorizes (i.e., accredits) the information system for processing before operations and updates the authorization [Assignment: organization-defined frequency, at least every three years] or when there is a significant change to the system. A senior organizational official signs and approves</p>	L	M	H			FS/PS/NS

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

		the security accreditation.					
	CA-6.1	Determine if: (i) the organization authorizes (i.e., accredits) the information system for processing before operations and updates the authorization in accordance with organization-defined frequency, at least every three years; (ii) a senior organizational official signs and approves the security accreditation; (iii) the security accreditation process employed by the organization is consistent with NIST Special Publications 800-37; and (iv) the organization updates the authorization when there is a significant change to the information system.				Examine: Certification and accreditation policy; procedures addressing security accreditation; NIST Special Publication 800-37; security accreditation package (including information system security plan; security assessment report; plan of action and milestones; authorization statement); other relevant documents or records. (L) (M) (H) Interview: Organizational personnel with security accreditation responsibilities. (H)	
7	CA-7	CONTINUOUS MONITORING Control: The organization monitors the security controls in the information system on an ongoing basis.	L	M	H		FS/PS/NS
	CA-7.1	Determine if: (i) the organization monitors the security controls in the information system on an ongoing basis; and (ii) the organization employs a security control monitoring process consistent with NIST Special Publications 800-37 and 800-53A.				Examine: Certification and accreditation policy; procedures addressing continuous monitoring of information system security controls; NIST Special Publications 800-37 and 800-53A; information system security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; other relevant documents or records. (L) (M) (H) Interview: Organizational	

					personnel with continuous monitoring responsibilities. (H)		
	CA-7.2	Determine if: (i) the organization conducts security impact analyses on changes to the information system; (ii) the organization documents and reports changes to or deficiencies in the security controls employed in the information system; and (iii) the organization makes adjustments to the information system security plan and plan of action and milestones, as appropriate, based on the activities associated with continuous monitoring of the security controls.			Examine: Certification and accreditation policy; procedures addressing continuous monitoring of information system security controls; information system security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; other relevant documents or records. (L) (M) (H) Interview: Organizational personnel with continuous monitoring responsibilities. (H)		
8	CA-7-1	CONTINUOUS MONITORING Control Enhancement: The organization employs an independent certification agent or certification team to monitor the security controls in the information system on an ongoing basis.	L	M	H		FS/PS/NS

CA-7-1-1	<p>Determine if the organization employs an independent certification agent or certification team to monitor the security controls in the information system on an ongoing basis.</p>			<p>Examine: Certification and accreditation policy; procedures addressing continuous monitoring of information system security controls; information system security plan; security assessment report; plan of action and milestones; information system monitoring records; security impact analyses; status reports; other relevant documents or records.</p> <p>Interview : Organizational personnel with continuous monitoring responsibilities.</p>									
FS - Fully Satisfied PS - Partially Satisfied NS - Not Satisfied Impacts: Low Medium High Assessment Methods: Interview Demonstrate Test Observe					Assessment Results <table border="1" data-bbox="1727 845 2050 1013"> <tr> <td>FS</td><td>0</td></tr> <tr> <td>PS</td><td>0</td></tr> <tr> <td>NS</td><td>0</td></tr> <tr> <td>Total</td><td>0</td></tr> </table>	FS	0	PS	0	NS	0	Total	0
FS	0												
PS	0												
NS	0												
Total	0												

CONFIGURATION MANAGEMENT

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

FAMILY: CONFIGURATION MANAGEMENT			Impact			Assessment Method	Assessment Results	FS/PS/NS
Num	ID	Assessment Procedure	L	M	H			
1	CM-1	CONFIGURATION MANAGEMENT POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	L	M	H			FS/PS/NS
	CM-1.1	Determine if: (i) the organization develops and documents configuration management policy and procedures; (ii) the organization disseminates configuration management policy and procedures to appropriate elements within the organization; (iii) responsible parties within the organization periodically review configuration management policy and				Examine: Configuration management policy and procedures; other relevant documents or records. (L) (M) (H) Interview: Organizational personnel with configuration management and control responsibilities. (H)		

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

		procedures; and (iv) the organization updates configuration management policy and procedures when organizational review indicates updates are required.				
	CM-1.2	Determine if: (i) the configuration management policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance; (ii) the configuration management policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and (iii) the configuration management procedures address all areas identified in the configuration management policy and address achieving policy-compliant implementations of all associated security controls.			Examine: Configuration management policy and procedures; other relevant documents or records. (L) (M) (H) Interview: Organizational personnel with configuration management and control responsibilities. (H)	
2	CM-2	BASELINE CONFIGURATION Control: The organization develops, documents, and maintains a current baseline configuration of the information system.	L	M	H	FS/PS/NS

	CM-2.1	Determine if: (i) the organization develops, documents, and maintains a baseline configuration of the information system; (ii) the baseline configuration shows relationships among information system components and is consistent with the FiXs Federated Architecture; (iii) the baseline configuration provides the organization with a well-defined and documented specification to which the information system is built; and (iv) the organization documents deviations from the baseline configuration, in support of mission needs/objectives.				Examine: Configuration management policy; procedures addressing the baseline configuration of the information system; FiXs Federated Architecture documentation; information system design documentation; information system architecture and configuration documentation; other relevant documents or records. (L) (M) (H)		
3	CM-2-1	BASELINE CONFIGURATION Control Enhancement: The organization updates the baseline configuration of the information system as an integral part of information system component installations.	L	M	H			FS/PS/NS
	CM-2-1-1	Determine if: (i) the organization identifies the frequency of updates to the baseline configuration and instances that trigger configuration updates; and (ii) the organization updates the baseline configuration of the information system as an integral part				Examine: Configuration management policy; procedures addressing the baseline configuration of the information system; information system architecture and configuration documentation; other relevant documents or records. (M) (H)		

		of information system component installations.					
4	CM-2-2	<p>BASELINE CONFIGURATION Control Enhancement:</p> <p>The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.</p>	L	M	H		FS/PS/NS
	CM-2-2-1	Determine if the organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.				<p>Examine: Configuration management policy; procedures addressing the baseline configuration of the information system; information system design documentation; information system architecture and configuration documentation; other relevant documents or records. (H)</p> <p>Test: Automated mechanisms implementing baseline configuration maintenance. (H)</p>	
5	CM-3	<p>CONFIGURATION CHANGE CONTROL</p> <p>Control: The organization authorizes, documents, and controls changes to the information system.</p>	L	M	H		FS/PS/NS

	CM-3.1	Determine if: (i) the organization authorizes, documents, and controls changes to the information system; (ii) the organization manages configuration changes to the information system using an organizationally approved process; (iii) the organization includes emergency changes in the configuration change control process, including changes resulting from the remediation of flaws; and (iv) the organization audits activities associated with configuration changes to the information system.				Examine: Configuration management policy; procedures addressing information system configuration change control; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records. (M) (H)	
6	CM-3-1	CONFIGURATION CHANGE CONTROL Control Enhancement: The organization employs automated mechanisms to: (i) document proposed changes to the information system; (ii) notify appropriate approval authorities; (iii) highlight approvals that have not been received in a timely manner; (iv) inhibit change until necessary approvals are received; and (v) document completed changes to the information system.	L	M	H		FS/PS/NS

	CM-3-1-1	Determine if: (i) the organization employs automated mechanisms to document proposed changes to the information system; (ii) the organization employs automated mechanisms to notify appropriate approval authorities; (iii) the organization employs automated mechanisms to highlight approvals that have not been received in a timely manner; (iv) the organization employs automated mechanisms to inhibit change until necessary approvals are received; and (v) the organization employs automated mechanisms to document completed changes to the information system.			Examine: Configuration management policy; procedures addressing information system configuration change control; information system design documentation; information system architecture and configuration documentation; automated configuration control mechanisms; change control records; information system audit records; other relevant documents or records. (H) Test: Automated mechanisms implementing configuration change control. (H)		
7	CM-3(ICS-1)	CONFIGURATION CHANGE CONTROL ICS Control Enhancements: The organization tests, validates, and documents changes (e.g., patches and updates) before implementing the changes on the operational ICS.	L	M	H		FS/PS/NS
	CM-3(ICS-1).1	Determine if the organization tests, validates, and documents changes (e.g., patches and updates) before implementing the changes on the operational ICS.				Examine: Configuration management policy; procedures addressing ICS configuration change control; ICS architecture and configuration documentation; change control records; ICS audit	

						records; other relevant documents or records. (M) (H)		
8	CM-4	<p>MONITORING CONFIGURATION CHANGES</p> <p>Control: The organization monitors changes to the information system conducting security impact analyses to determine the effects of the changes.</p>	L	M	H			FS/PS/NS
	CM-4.1	<p>Determine if:</p> <ul style="list-style-type: none"> (i) the organization identifies the types of information system changes to be monitored; (ii) the organization monitors changes to the information system; and (iii) the organization conducts security impact analyses to assess the effects of the information system changes. 				<p>Examine: Configuration management policy; procedures addressing the monitoring of configuration changes to the information system; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records. (M) (H)</p>		
9	CM-5	<p>ACCESS RESTRICTIONS FOR CHANGE</p> <p>Control: The organization: (i) approves individual access privileges and enforces physical and logical access restrictions associated with changes to the information system; and (ii) generates, retains, and reviews records reflecting all such changes.</p>	L	M	H			FS/PS/NS

	CM-5.1	Determine if: (i) the organization maintains a list of qualified and authorized personnel permitted to access the information system for the express purpose of initiating changes; (ii) the organization approves individual access privileges and enforces physical and logical access restrictions associated with changes to the information system; and (iii) the organization generates, retains, and reviews records reflecting all such changes to the information system.			Examine: Configuration management policy; procedures addressing access restrictions for changes to the information system; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or records. (M) (H)		
10	CM-5-1	ACCESS RESTRICTIONS FOR CHANGE Control Enhancement: The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.	L	M	H		FS/PS/NS
	CM-5-1-1	Determine if the organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.				Examine: Configuration management policy; procedures addressing access restrictions for changes to the information system; information system design documentation; information system architecture and configuration documentation; change control records; information system audit records; other relevant documents or	

						records. (H)		
						Test: Automated mechanisms implementing access restrictions for changes to the information system. (H)		
11	CM-6	CONFIGURATION SETTINGS Control: The organization: (i) establishes mandatory configuration settings for information technology products employed within the information system; (ii) configures the security settings of information technology products to the most restrictive mode consistent with operational requirements; (iii) documents the configuration settings; and (iv) enforces the configuration settings in all components of the information system.	L	M	H			FS/PS/NS
	CM-6.1	Determine if: (i) the organization establishes mandatory configuration settings for information technology products employed within the information system; (ii) the organization configures the security settings of information technology products to the most restrictive mode consistent with operational requirements; (iii) the organization documents the configuration settings; and				Examine: Configuration management policy; procedures addressing configuration settings for the information system; information system configuration settings and associated documentation; NIST Special Publication 800-70; other relevant documents or records. (L) (M) (H) Test: Information system configuration settings. (M) (H)		

		(iv) the organization enforces the configuration settings in all components of the information system.					
12	CM-6-1	CONFIGURATION SETTINGS Control Enhancement: The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.	L	M	H		FS/PS/NS
	CM-6-1-1	Determine if the information system employs automated mechanisms to centrally manage, apply, and verify configuration settings.				Examine: Configuration management policy; procedures addressing configuration settings for the information system; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. (H) Test: Automated mechanisms implementing the centralized management, application, and verification of configuration settings. (H)	
13	CM-7	LEAST FUNCTIONALITY Control: The organization configures the information system to provide only essential capabilities and specifically prohibits and/or restricts the use of the following functions, ports, protocols, and/or services: [Assignment: organization-defined list]	L	M	H		FS/PS/NS

		of prohibited and/or restricted functions, ports, protocols, and/or services].					
	CM-7.1	Determine if: (i) the organization identifies prohibited or restricted functions, ports, protocols, and services for the information system; (ii) the organization configures the information system to provide only essential capabilities; and (iii) the organization configures the information system to specifically prohibit and/or restrict the use of organization-defined prohibited and/or restricted functions, ports, protocols, and/or services.				Examine: Configuration management policy; procedures addressing least functionality in the information system; information system security plan; information system configuration settings and associated documentation; other relevant documents or records. (M) (H) Test: Information system for disabling or restriction of functions, ports, protocols, and services. (M) (H)	
14	CM-7-1	LEAST FUNCTIONALITY Control Enhancement: The organization reviews the information system [Assignment: organization-defined frequency], to identify and eliminate unnecessary functions, ports, protocols, and/or services.	L	M	H		
	CM-7-1-1	Determine if: (i) the organization defines the frequency of the information system reviews to identify and eliminate unnecessary functions, ports, protocols, and services; and (ii) the organization reviews the information system to identify and				Examine: Configuration management policy; procedures addressing least functionality in the information system; information system security plan; information system configuration settings and associated documentation; other relevant	

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

		eliminate unnecessary functions, ports, protocols, and/or services in accordance with the organizational defined frequency.			documents or records]. (H)		
15	CM-8	<p>INFORMATION SYSTEM COMPONENT INVENTORY</p> <p>Control: The organization develops, documents, and maintains a current inventory of the components of the information system and relevant ownership information.</p>	L	M	H		FS/PS/NS
	CM-8.1	<p>Determine if:</p> <p>(i) the organization develops, documents, and maintains a current inventory of the components of the information system; and</p> <p>(ii) the inventory of information system components includes any information determined to be necessary by the organization to achieve effective property accountability.</p>				<p>Examine: Configuration management policy; procedures addressing information system component inventory; information system inventory records; other relevant documents or records.</p> <p>(L) (M) (H)</p>	
16	CM-8-1	<p>INFORMATION SYSTEM COMPONENT INVENTORY</p> <p>Control Enhancement:</p> <p>The organization updates the inventory of information system components as an integral part of component installations.</p>	L	M	H		FS/PS/NS

	CM-8-1-1	Determine if the organization updates the inventory of information system components as an integral part of component installations.			Examine: Configuration management policy; procedures addressing information system component inventory; information system inventory records; component installation records; other relevant documents or records. (M) (H) Interview: Organizational personnel with information system installation and inventory responsibilities. (H)		
17	CM-8-2	INFORMATION SYSTEM COMPONENT INVENTORY Control Enhancement: The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.	L	M	H		FS/PS/NS
	CM-8-2-1	Determine if the organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available inventory of information system components.			Examine: Configuration management policy; procedures addressing information system component inventory; information system design documentation; information system inventory records; component installation records; other relevant documents or records. (H)		

					Test: Automated mechanisms implementing information system component inventory management. (H)	
FS - Fully Satisfied	PS - Partially Satisfied	NS - Not Satisfied				Assessment Results
Impacts: Low	Medium	High				FS
Assessment Methods:	Interview	Demonstrate	Test	Observe		PS
						NS
						Total

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

CONTINGENCY PLANNING

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

FAMILY: CONTINGENCY PLANNING			Impact			Assessment Method	Assessment Results	FS/PS/NS
Num	ID	Assessment Procedure	L	M	H			
1	CP-1	<p>CONTINGENCY PLANNING POLICY AND PROCEDURES</p> <p>Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.</p>	L	M	H			FS/PS/NS
	CP-1.1	<p>Determine if:</p> <p>(i) the organization develops and documents contingency planning policy and procedures; (ii) the organization disseminates contingency planning policy and procedures to appropriate elements within the organization; (iii) responsible parties within the organization periodically review contingency planning policy and procedures; and (iv) the organization updates contingency planning policy and procedures when organizational review indicates updates are required.</p>				<p>Examine: Configuration management policy and procedures; other relevant documents or records. (L) (M) (H)</p> <p>Interview: Organizational personnel with configuration management and control responsibilities. (H)</p>		

Copyright© 2008
 Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

	CP-1.2	Determine if: (i) the contingency planning policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance; (ii) the contingency planning policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and (iii) the contingency planning procedures address all areas identified in the contingency planning policy and address achieving policy-compliant implementations of all associated security controls.				Examine: Configuration management policy and procedures; other relevant documents or records. (L) (M) Interview: Organizational personnel with configuration management and control responsibilities. (H)	
2	CP-2	CONTINGENCY PLAN Control: The organization develops and implements a contingency plan for the information system addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. Designated officials within the organization review and approve the contingency plan and distribute copies of the plan to key contingency personnel.	L	M	H		FS/PS/NS

	CP-2.1	Determine if: (i) the organization develops and documents a contingency plan for the information system; (ii) the contingency plan is consistent with NIST Special Publication 800-34; (iii) the contingency plan addresses contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the information system after a disruption or failure; (iv) the contingency plan is reviewed and approved by designated organizational officials; and (v) the organization disseminates the contingency plan to key contingency personnel.			Examine: Configuration management policy; procedures addressing the baseline configuration of the information system; FiXs Federated Architecture documentation; information system design documentation; information system architecture and configuration documentation; other relevant documents or records. (L) (M) (H)		
	CP-2.2	Determine if key contingency personnel and the key operating elements within the organization understand the contingency plan and are ready to implement the plan.			Interview: Organizational personnel with contingency planning and plan implementation responsibilities. (M) (H)		
3	CP-2-1	CONTINGENCY PLAN Control Enhancement: The organization coordinates contingency plan development with organizational elements responsible for related plans.	L	M	H		FS/PS/NS

	CP-2-1-1	Determine if the organization coordinates the contingency plan with other related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, Emergency Action Plan).			Examine: [SELECT FROM: Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; other related plans; other relevant documents or records. (M) (H) Interview: [SELECT FROM: Organizational personnel with contingency planning and plan implementation responsibilities and responsibilities in related plan areas. (M) (H)		
4	CP-2-2	CONTINGENCY PLAN Control Enhancement: The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during crisis situations	L	M	H		FS/PS/NS
	CP-2-2-1	Determine if the organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during crisis situations.					
5	CP-3	CONTINGENCY TRAINING Control: The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides	L	M	H		FS/PS/NS

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

		refresher training [Assignment: organization-defined frequency, at least annually.]					
	CP-3.1	Determine if: (i) the organization provides contingency training to personnel with significant contingency roles and responsibilities; (ii) the organization records the type of contingency training received and the date completed; (iii) the organization defines frequency of refresher contingency training; and (iv) the organization provides initial training and refresher training in accordance with organization-defined frequency, at least annually.				Examine: Contingency planning policy; contingency plan; procedures addressing contingency training; contingency training curriculum; contingency training material; information system security plan; other relevant documents or records. (M) (H) Interview: Organizational personnel with contingency planning, plan implementation, and training responsibilities. (M) (H)	
	CP-3.2	Determine if contingency training material addresses the procedures and activities necessary to fulfill identified organizational contingency roles and responsibilities.				Examine: Contingency planning policy; contingency plan; procedures addressing contingency training; contingency training curriculum; contingency training material; other relevant documents or records. (M) (H)	
6	CP-3-1	CONTINGENCY TRAINING Control Enhancement: The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.	L	M	H		FS/PS/NS

	CP-3-1-1	Determine if: (i) the organization incorporates simulated events into contingency training; and (ii) the training is effective in getting organizational personnel to respond as expected to simulated crisis situations.			Examine: Contingency planning policy; contingency plan; procedures addressing contingency training; contingency training curriculum; contingency training material; other relevant documents or records. (H) Interview: Organizational personnel with contingency planning, plan implementation, and training responsibilities. (H)		
7	CP-3-2	CONTINGENCY TRAINING Control Enhancement: The organization employs automated mechanisms to provide a more thorough and realistic training environment.	L	M	H		FS/PS/NS
	CP-3-2-1	Determine if: (i) the organization employs automated mechanisms for contingency training; and (ii) the automated mechanisms improve the effectiveness of the contingency training.			Examine: Contingency planning policy; contingency plan; procedures addressing contingency training; automated mechanisms supporting contingency training; contingency training curriculum; contingency training material; other relevant documents or records. Interview: Organizational personnel with contingency planning, plan implementation, and training responsibilities.		

8	CP-4	<p>CONTINGENCY PLAN TESTING AND EXERCISES</p> <p>Control: The organization: (i) tests and/or exercises the contingency plan for the information system [Assignment: organization-defined frequency, at least annually] using [Assignment: organization-defined tests and/or exercises] to determine the plan's effectiveness and the organization's readiness to execute the plan; and (ii) reviews the contingency plan test/exercise results and initiates corrective actions.</p>	L	M	H			FS/PS/NS
	CP-4.1	<p>Determine if:</p> <ul style="list-style-type: none"> (i) the organization defines the frequency of contingency plan tests and/or exercises; (ii) the organization defines the set of contingency plan tests and/or exercises; (iii) the organization tests/exercises the contingency plan using organization-defined tests/exercises in accordance with organization-defined frequency; (iv) the organization documents the results of contingency plan testing/exercises; and (v) the organization reviews the contingency plan test/exercise results and takes corrective actions. 				<p>Examine: Contingency planning policy; contingency plan, procedures addressing contingency plan testing and exercises; information system security plan; contingency plan testing and/or exercise documentation; other relevant documents or records. (L) (M) (H)</p>		

	CP-4.2	Determine if the contingency plan tests/exercises address key aspects of the plan.				Examine: Contingency planning policy; contingency plan; procedures addressing contingency plan testing and exercises; contingency plan testing and/or exercise documentation; contingency plan test results; other relevant documents or records. (L) (M) (H)		
9	CP-4-1	CONTINGENCY PLAN TESTING AND EXERCISES Control Enhancement: The organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans.	L	M	H			FS/PS/NS
	CP-4-1-1	Determine if the organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, Emergency Action Plan).				Examine: Contingency planning policy; contingency plan; procedures addressing contingency plan testing and exercises; contingency plan testing and/or exercise documentation; other relevant documents or records. (M) (H) Interview: Organizational personnel with contingency planning, plan implementation, and testing responsibilities. (M) (H)		

10	CP-4-2	<p>CONTINGENCY PLAN TESTING AND EXERCISES</p> <p>Control Enhancement:</p> <p>The organization tests/exercises the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations.</p>	L	M	H			FS/PS/NS
	CP-4-2-1	<p>Determine if the organization conducts contingency plan testing at the alternate processing site to familiarize contingency personnel with the facility and its resources and to evaluate the site's capabilities to support contingency operations.</p>				<p>Examine: Contingency planning policy; contingency plan, procedures addressing contingency plan testing and exercises; contingency plan testing and/or exercise documentation; contingency plan test results; other relevant documents or records. (H)</p>		
11	CP-4-3	<p>CONTINGENCY PLAN TESTING AND EXERCISES</p> <p>Control Enhancement:</p> <p>The organization employs automated mechanisms to more thoroughly and effectively test/exercise the contingency plan by providing more complete coverage of contingency issues, selecting more realistic test/exercise scenarios and environments, and more effectively stressing the information system and supported missions.</p>	L	M	H			FS/PS/NS

	CP-4-3-1	Determine if: (i) the organization employs automated mechanisms for contingency plan testing/exercises; and (ii) the automated mechanisms improve the effectiveness of the contingency plan testing/exercises.			Examine: Contingency planning policy; contingency plan; procedures addressing contingency plan testing and exercises; automated mechanisms supporting contingency plan testing/exercises; contingency plan testing and/or exercise documentation; other relevant documents or records.		
12	CP-5	CONTINGENCY PLAN UPDATE Control: The organization reviews the contingency plan for the information system [Assignment: organization-defined frequency, at least annually] and revises the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.	L	M	H		FS/PS/NS
	CP-5.1	Determine if: (i) the organization defines the frequency of contingency plan reviews and updates; (ii) the organization updates the contingency plan in accordance with organization-defined frequency, at least annually; and (iii) the revised plan addresses the system/organizational changes identified by the organization or any problems encountered by the organization during plan implementation, execution, and testing.			Examine: Contingency planning policy; contingency plan; procedures addressing contingency plan reviews and updates; information system security plan; other relevant documents or records. (L) (M) (H)		

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

	CP-5.2	Determine if the organization communicates necessary changes to the contingency plan to other organizational elements with related plans.				Examine: Contingency planning policy; contingency plan; procedures addressing contingency plan reviews and updates; other relevant documents or records. (M) (H) Interview: Organizational personnel with contingency plan update responsibilities; organizational personnel with mission-related and operational responsibilities. (M) (H)		
13	CP-6	ALTERNATE STORAGE SITE Control: The organization identifies an alternate storage site and initiates necessary agreements to permit the storage of information system backup information.	L	M	H			FS/PS/NS
	CP-6.1	Determine if: (i) the organization identifies an alternate storage site; and (ii) alternate storage site agreements are currently in place (if needed) to permit storage of information system backup information.				Examine: Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site agreements; other relevant documents or records. (M) (H)		
	CP-6.2	Determine if the alternate storage site is available, accessible, and meets the requirements (including necessary equipment and supplies) to permit the storage of information system backup				Examine: Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site; other relevant documents or		

		information consistent with the organization's recovery time objectives and recovery point objectives.			records. (M) (H) Interview: Organizational personnel with alternate storage site responsibilities. (H)		
14	CP-6-1	ALTERNATE STORAGE SITE Control Enhancement: The organization identifies an alternate storage site that is geographically separated from the primary storage site so as not to be susceptible to the same hazards.	L	M	H		FS/PS/NS
	CP-6-1-1	Determine if: (i) the contingency plan identifies the primary storage site hazards; and (ii) the alternate storage site is sufficiently separated from the primary storage site so as not to be susceptible to the same hazards identified at the primary site.				Examine: [SELECT FROM: Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site; other relevant documents or records]. (M) (H)	
15	CP-6-2	ALTERNATE STORAGE SITE Control Enhancement: The organization configures the alternate storage site to facilitate timely and effective recovery operations.	L	M	H		FS/PS/NS
	CP-6-2-1	Determine if the alternate storage site is configured to enable timely and effective recovery of system backup information (i.e., meeting recovery time and recovery point objectives) in accordance with the provisions of alternate storage site agreements.				Examine: Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site agreements; alternate storage site; other relevant documents or records. (H)	

16	CP-6-3	<p>ALTERNATE STORAGE SITE</p> <p>Control Enhancement:</p> <p>The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.</p>	L	M	H			FS/PS/NS
	CP-6-3-1	<p>Determine if:</p> <ul style="list-style-type: none"> (i) the contingency plan identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster; and (ii) the contingency plan defines explicit mitigation actions for potential accessibility problems. 				Examine: Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site; other relevant documents or records. (M) (H)		
17	CP-7	<p>ALTERNATE PROCESSING SITE</p> <p>Control: The organization identifies an alternate processing site and initiates necessary agreements to permit the resumption of information system operations for critical mission/business functions within [Assignment: organization-defined time period] when the primary processing capabilities are unavailable.</p>	L	M	H			FS/PS/NS
	CP-7.1	<p>Determine if:</p> <ul style="list-style-type: none"> (i) the organization identifies an alternate processing site; (ii) the organization defines the time period within which processing must be resumed at the alternate processing site; and (iii) alternate processing site agreements are currently in place (if needed) to 				Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site agreements; information system security plan; other relevant documents or records. (M) (H)		

Copyright© 2008
 Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

		permit the resumption of information system operations for critical mission/business functions within organization-defined time period.					
	CP-7.2	Determine if the alternate processing site is available, accessible, and meets the requirements (including necessary equipment and supplies) for resuming information system operations for critical mission/business functions within organization-defined time period.			Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; other relevant documents or records. (M) (H) Interview: Organizational personnel with alternate processing site responsibilities. (H)		
18	CP-7-1	ALTERNATE PROCESSING SITE Control Enhancement: The organization identifies an alternate processing site that is geographically separated from the primary processing site so as not to be susceptible to the same hazards.	L	M	H		FS/PS/NS
	CP-7-1-1	Determine if: (i) the contingency plan identifies the primary processing site hazards; and (ii) the alternate processing site is sufficiently separated from the primary processing site so as not to be susceptible to the same hazards identified at the primary site.			Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; other relevant documents or records. (M) (H)		

	CP-7-2	ALTERNATE PROCESSING SITE Control Enhancement: The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.	L	M	H		
	CP-7-2-1	Determine if: (i) the contingency plan identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster; and (ii) the contingency plan defines explicit mitigation actions for potential accessibility problems.				Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; other relevant documents or records. (M) (H)	
19	CP-7-3	ALTERNATE PROCESSING SITE Control Enhancement: The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.	L	M	H		FS/PS/NS
	CP-7-3-1	Determine if alternate processing site agreements contain priority-of-service provisions in accordance with the organization's availability requirements.				Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site agreements; other relevant documents or records. (M) (H)	
20	CP-7-4	ALTERNATE PROCESSING SITE Control Enhancement: The organization fully configures the alternate processing site so that it is ready to be used as the operational site	L	M	H		FS/PS/NS

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

		supporting a minimum required operational capability.					
	CP-7-4-1	Determine if alternate processing site agreements specify the requirements needed to support the minimum required operational capability of the organization.				Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; alternate processing site agreements; other relevant documents or records. (H)	
	CP-7-4-2	Determine if the alternate processing site is configured to support the minimum required operational capability of the organization and is ready to use as the operational site.				Examine: Contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; alternate processing site agreements; other relevant documents or records. (H) Test: Information system at the alternate processing site. (H)	
21	CP-8	TELECOMMUNICATIONS SERVICES Control: The organization identifies primary and alternate telecommunications services to support the information system and initiates necessary agreements to permit the resumption of system operations for critical mission/business functions within [Assignment: organization-defined time period] when the primary telecommunications capabilities are unavailable.	L	M	H		FS/PS/NS

	CP-8.1	Determine if: (i) the organization identifies primary and alternate telecommunications services to support the information system; (ii) the organization defines the time period within which resumption of information system operations must take place; and (iii) alternate telecommunications service agreements are in place to permit the resumption of telecommunications services for critical mission/business functions within the organization-defined time period when the primary telecommunications capabilities are unavailable.				Examine: Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; information system security plan; primary and alternate telecommunications service agreements; other relevant documents or records. (M) (H)		
	CP-8.2	Determine if: (i) telecommunications services supporting the organization are used for national security emergency preparedness; and (ii) a common carrier provides telecommunications services.				Examine: Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecommunications service agreements; other relevant documents or records. (M) (H)		
22	CP-8-1	TELECOMMUNICATIONS SERVICES Control Enhancement: The organization develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with the organization's availability requirements	L	M	H			FS/PS/NS

	CP-8-1-1	Determine if primary and alternate telecommunications service agreements contain priority-of-service provisions in accordance with the availability requirements defined in the organization's contingency plan.				Examine: Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecommunications service agreements; other relevant documents or records. (M) (H)		
23	CP-8-2	TELECOMMUNICATIONS SERVICES Control Enhancement: The organization obtains alternate telecommunications services that do not share a single point of failure with primary telecommunications services.	L	M	H			FS/PS/NS
	CP-8-2-1	Determine if primary and alternate telecommunications services share a single point of failure.				Examine: Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecommunications service agreements; other relevant documents or records. (M) (H) Interview: Organizational personnel with contingency planning and plan implementation responsibilities; telecommunications service providers. (M) (H)		

24	CP-8-3	<p>TELECOMMUNICATIONS SERVICES Control Enhancement:</p> <p>The organization obtains alternate telecommunications service providers that are sufficiently separated from primary service providers so as not to be susceptible to the same hazards.</p>	L	M	H			FS/PS/NS
	CP-8-3-1	<p>Determine if the alternate telecommunications service provider's site is sufficiently separated from the primary telecommunications service provider's site so as not to be susceptible to the same hazards identified at the primary site.</p>				<p>Examine: [SELECT FROM: Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecommunications service agreements; alternate telecommunications service provider's site; primary telecommunications service provider's site; other relevant documents or records]. (H)</p> <p>Interview: [SELECT FROM: Organizational personnel with contingency planning and plan implementation responsibilities; telecommunications service providers]. (H)</p>		
25	CP-8-4	<p>TELECOMMUNICATIONS SERVICES Control Enhancement:</p> <p>The organization requires primary and alternate telecommunications service providers to have adequate contingency plans.</p>	L	M	H			FS/PS/NS

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

	CP-8-4-1	Determine if the contingency plans for the primary and alternate telecommunications service providers are sufficient to meet the needs of the organization.			Examine: Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecommunications service agreements; other relevant documents or records]. (H) Interview: Organizational personnel with contingency planning, plan implementation, and testing responsibilities; telecommunications service providers. (H) Test: Operational capability by exercising priority-of-service provisions of alternate telecommunications service agreements. (H)	
26	CP-9	INFORMATION SYSTEM BACKUP Control: The organization conducts backups of user-level and system-level information (including system state information) contained in the information system [Assignment: organization-defined frequency] and protects backup information at the storage location.	L	M	H	
	CP-9.1	Determine if: (i) the organization defines the frequency of information systems backups; (ii) the organization defines the user-level and system-level information (including system state information) that			Examine: [SELECT FROM: Contingency planning policy; contingency plan; procedures addressing information system backup; information system security plan; backup storage	

		is required to be backed up; and (iii) the organization identifies the location(s) for storing backup information			location(s); other relevant documents or records. (L) (M) (H)		
	CP-9.2	Determine if: (i) the organization backs up the required user-level and system-level information (including system state information) in accordance with the organization-defined frequency; (ii) the organization stores backup information in designated locations in accordance with information system backup procedures; and (iii) the organization protects backup information at the designated storage locations			Examine: [SELECT FROM: Contingency planning policy; contingency plan; procedures addressing information system backup; information system security plan; backup storage location(s); other relevant documents or records. (L) (M) (H)]		
27	CP-9-1	INFORMATION SYSTEM BACKUP Control Enhancement: The organization tests backup information [Assignment: organization-defined frequency] to verify media reliability and information integrity.	L	M	H		FS/PS/NS
	CP-9-1-1	Determine if: (i) the organization defines the frequency of information system backup testing; (ii) the organization conducts information system backup testing within the organization-defined frequency; and (iii) testing results verify backup media reliability and information integrity.			Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; information system security plan; information system backup test results; backup storage		

						location(s); other relevant documents or records. (M) (H)		
28	CP-9-2	INFORMATION SYSTEM BACKUP Control Enhancement: The organization selectively uses backup information in the restoration of information system functions as part of contingency plan testing.	L	M	H			FS/PS/NS
	CP-9-2-1	Determine if the organization uses selected backup information in the restoration of information system functions as part of contingency plan testing.				Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; information system backup test results; contingency plan test results; other relevant documents or records. (H)		
29	CP-9-3	INFORMATION SYSTEM BACKUP Control Enhancement: The organization stores backup copies of the operating system and other critical information system software in a separate facility or in a fire-rated container that is not collocated with the operational software.	L	M	H			FS/PS/NS
	CP-9-3-1	Determine if the organization stores backup copies of operating system and other critical information system software in a separate facility or in a fire-rated container that is not collocated with the operational software.				Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; backup storage location(s); other relevant documents or records. (H)		

30	CP-9-4	INFORMATION SYSTEM BACKUP Control Enhancement: The organization protects system backup information from unauthorized modification.	L	M	H			FS/PS/NS
	CP-9-4-1	Determine if the organization employs appropriate mechanisms to protect the integrity of information system backup information				<p>Examine: Contingency planning policy; contingency plan; procedures addressing information system backup; information system design documentation; backup storage location(s); information system configuration settings and associated documentation; other relevant documents or records. (M) (H)</p> <p>Interview: Organizational personnel with information system backup responsibilities. (M) (H)</p>		
31	CP-10	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION Control: The organization employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure.	L	M	H			FS/PS/NS

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

	CP-10.1	Determine if the organization identifies the means for capturing the information system's operational state including appropriate system parameters, patches, configuration settings, and application/system software prior to system disruption or failure.			Examine: Contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; information system configuration settings and associated documentation; information system design documentation; other relevant documents or records. (L) (M) (H)		
	CP-10.2	Determine if the organization makes available and applies mechanisms and procedures for recovery and reconstitution of the information system to known secure state after disruption or failure.			Examine: Contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; information system configuration settings and associated documentation; information system design documentation; other relevant documents or records. (L) (M) (H)		
32	CP-10-1	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION Control Enhancement: The organization includes a full recovery and reconstitution of the information system as part of contingency plan testing.	L	M	H		FS/PS/NS

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

CP-10-1-1	<p>Determine if the organization includes a full recovery and reconstitution of the information system as part of contingency plan testing.</p>			<p>Examine: Contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; contingency plan test procedures; contingency plan test results; other relevant documents or records. (H)</p> <p>Interview: Organizational personnel with information system recovery and reconstitution responsibilities; organizational personnel with contingency testing responsibilities. (H)</p>	
<p>FS - Fully Satisfied PS - Partially Satisfied NS - Not Satisfied Impacts: Low Medium High Assessment Methods: Interview</p>					Assessment Results
					FS 0
					PS 0
					NS 0
					Total 0

Copyright© 2008
 Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

IDENTIFICATION & AUTHENTICATION

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

A-124

Page 1423 of 1794

FAMILY: IDENTIFICATION & AUTHENTICATION			Impact			Assessment Method	Assessment Results	FS/PS/NS
Num	ID	Assessment Procedure	L	M	H			
1	IA-1	IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.	L	M	H			FS/PS/NS
	IA-1.1	Determine if: (i) the organization develops and documents identification and authentication policy and procedures; (ii) the organization disseminates identification and authentication policy and procedures to appropriate elements within the organization; (iii) responsible parties within the organization periodically review identification and authentication policy and procedures; and (iv) the				Examine: Identification and authentication policy and procedures; other relevant documents or records. (L) (M) Interview: Organizational personnel with identification and authentication responsibilities. (H)		

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

		organization updates identification and authentication policy and procedures when organizational review indicates updates are required.					
	IA-1.2	Determine if: (i) the identification and authentication policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance; (ii) the identification and authentication policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and (iii) the identification and authentication procedures address all areas identified in the identification and authentication policy and address achieving policy-compliant implementations of all associated security controls.				Examine: Identification and authentication policy and procedures; other relevant documents or records. (L) (M) Interview: Organizational personnel with identification and authentication responsibilities. (H)	
2	IA-2	USER IDENTIFICATION AND AUTHENTICATION Control: The information system uniquely identifies and authenticates users (or processes acting on behalf of users).	L	M	H		FS/PS/NS

	IA-2.1	Determine if: (i) the information system uniquely identifies and authenticates users (or processes acting on behalf of users); and (ii) authentication levels for users (or processes acting on behalf of users) are consistent NIST Special Publication 800-63 and e-authentication risk assessment results.				Examine: Identification and authentication policy; NIST Special Publication 800-63; procedures addressing user identification and authentication; information system design documentation; e-authentication risk assessment results; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. (L) (M) (H) Test: Automated mechanisms implementing identification and authentication capability for the information system. (M) (H)	
3	IA-2-1	USER IDENTIFICATION AND AUTHENTICATION Control Enhancement: The information system employs multifactor authentication for remote system access that is NIST Special Publication 800-63 [Selection: organization-defined level 3, level 3 using a hardware authentication device, or level 4] compliant.	L	M	H		FS/PS/NS

	IA-2(1).1	Determine if: (i) the organization defines the NIST Special Publication 800-63 authentication levels for the information system; and (ii) the information system employs multifactor authentication for remote system access that is NIST Special Publication 800-63 compliant in accordance with the organizational selection of level 3, level 3 using a hardware authentication device, or level 4.				Examine: : Identification and authentication policy; NIST Special Publication 800-63; procedures addressing user identification and authentication; information system security plan; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. (M)		
4	IA-2(2)	USER IDENTIFICATION AND AUTHENTICATION Control Enhancement: The information system employs multifactor authentication for local system access that is NIST Special Publication 800-63 [Selection: organization-defined level 3 or level 4] compliant.	L	M	H			FS/PS/NS
	IA-2(2).1	Determine if: (i) the organization defines the NIST Special Publication 800-63 authentication levels for the information system; and (ii) the information system employs multifactor authentication for local system access that is NIST Special Publication 800-63 compliant in accordance with the organizational selection of level 3 or level 4				Examine: Identification and authentication policy; NIST Special Publication 800-63; procedures addressing user identification and authentication; information system security plan; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. (H)		

5	IA-2(3)	USER IDENTIFICATION AND AUTHENTICATION Control Enhancement: The information system employs multifactor authentication for remote system access that is NIST Special Publication 800-63 level 4 compliant.	L	M	H			FS/PS/NS
	IA-2(3).1	Determine if: (i) the organization defines the NIST Special Publication 800-63 authentication levels for the information system; and (ii) the information system employs multifactor authentication for remote system access that is NIST Special Publication 800-63 level 4 compliant.				Examine: Identification and authentication policy; NIST Special Publication 800-63; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. (H)		
6	IA-3	DEVICE IDENTIFICATION AND AUTHENTICATION Control: The information system identifies and authenticates specific devices before establishing a connection.	L	M	H			FS/PS/NS
	IA-3.1	Determine if: (i) the organization defines specific devices requiring identification and authentication before establishing connections to the information system; and (ii) the information system identifies and authenticates specific devices identified by the organization before establishing connections				Examine: Identification and authentication policy; procedures addressing device identification and authentication; information system design documentation; device connection reports; information system configuration settings and associated documentation; other relevant documents or records. (M) (H)		

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

						Test: Automated mechanisms implementing device identification and authentication. (H)		
7	IA-4	IDENTIFIER MANAGEMENT Control: The organization manages user identifiers by: (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user identifier from an appropriate organization official; (iv) issuing the user identifier to the intended party; (v) disabling the user identifier after [Assignment: organization-defined time period] of inactivity; and (vi) archiving user identifiers.	L	M	H			FS/PS/NS
	IA-4.1	Determine if: (i) the organization manages user identifiers by uniquely identifying each user; (ii) the organization manages user identifiers by verifying the identity of each user; (iii) the organization manages user identifiers by receiving authorization to issue a user identifier from an appropriate organization official; (iv) the organization manages user identifiers by issuing the identifier to the intended party; (v) the organization defines the time period of inactivity after which a user identifier is to be disabled; (vi) the organization				Examine: Identification and authentication policy; procedures addressing identifier management; information system security plan; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records. (L) (M) (H) Test: Identity verification capability for the information system and for organizational		

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

		manages user identifiers by disabling the identifier after the organization-defined time period of inactivity; and (vii) the organization manages user identifiers by archiving identifiers.		facilities. (M) (H)	
IA-4.2	Determine if the organization uses a Personal Identity Verification (PIV) card or FiXs Certified Credential token to uniquely identify and authenticate federal employees, contractors in accordance with FiXs Rules and Guidance, FIPS 201 and NIST Special Publications 800-73, 800-76, and 800-78.			Examine: Identification and authentication policy; procedures addressing identifier management; information system design documentation; FiXs Rules and Guidance applicable; FIPS 201; NIST Special Publications 800-73, 800-76, 800-78; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records. (L) (M) (H) Test: Identity verification capability for the information system and for organizational facilities. (M) (H)	

	IA-5	AUTHENTICATOR MANAGEMENT Control: The organization manages information system authenticators by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically.	L	M	H		
	IA-5.1	Determine if: (i) the organization manages information system authenticators by defining initial authenticator content; (ii) the organization manages information system authenticators by establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; (iii) the organization manages information system authenticators by changing default authenticators upon information system installation; and (iv) the organization manages information system authenticators by changing/refreshing authenticators periodically				Examine: Identification and authentication policy; procedures addressing authenticator management; information system design documentation; information system configuration settings and associated documentation; list of information system accounts; other relevant documents or records. (L) (M) Test: Automated mechanisms implementing authenticator management functions. (M) (H)	

8	IA-6	AUTHENTICATOR FEEDBACK Control: The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.					FS/PS/NS
	IA-6.1	Determine if the information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.			<p>Examine: Identification and authentication policy; procedures addressing authenticator feedback; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. (L) (M) (H)</p> <p>Test: Automated mechanisms implementing authenticator feedback. (M) (H)</p>		
9	IA-7	CRYPTOGRAPHIC MODULE AUTHENTICATION Control: The information system employs authentication methods that meet the requirements of FiXs Rules and: applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.	L	M	H		FS/PS/NS

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

IA-7.1	Determine if the information system employs authentication methods that meet the requirements of FiXs Guidance, applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module (for non-national security systems, the cryptographic requirements are defined by FIPS 140-2, as amended).			Examine: Identification and authentication policy; FIPS 140-2 (as amended); procedures addressing cryptographic module authentication; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. (L) (M) (H) Test: Automated mechanisms implementing cryptographic module authentication. (M) (H)	
FS - Fully Satisfied PS - Partially Satisfied NS - Not Satisfied Impacts: Low Medium High Assessment Methods: Interview Demonstrate Test Observe					Assessment Results
					FS 0
					PS 0
					NS 0
					Total 0

INCIDENT RESPONSE

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

A-135

Page 1434 of 1794

Family:		Incident Response	Impact			Assessment Method	Assessment Results	FS/PS/NS
Num	ID	Assessment Procedure	L	M	H			
1	IR-1	INCIDENT RESPONSE POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.	L	M	H			FS/PS/NS
	IR-1.1	Determine if: (i) the organization develops and documents incident response policy and procedures; (ii) the organization disseminates incident response policy and procedures to appropriate elements within the organization; (iii) responsible parties within the organization periodically review incident response policy and procedures; and (iv) the organization updates incident response policy and procedures when organizational review indicates updates are required.				Examine: Incident response policy and procedures; other relevant documents or records. (L) (M) (H) Interview: Organizational personnel with incident response planning and plan implementation responsibilities. (H)		

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

	IR-1.2	Determine if: (i) the incident response policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance; (ii) the incident response policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and (iii) the incident response procedures address all areas identified in the incident response policy and address achieving policy-compliant implementations of all associated security controls.				Examine: Incident response policy and procedures; other relevant documents or records. (L) (M) (H) Interview: Organizational personnel with incident response planning and plan implementation responsibilities. (H)	
2	IR-2	INCIDENT RESPONSE TRAINING Control: The organization trains personnel in their incident response roles and responsibilities with respect to the information system and provides refresher training [Assignment: organization-defined frequency, at least annually].	L	M	H		FS/PS/NS

		Determine if: (i) the organization identifies and documents personnel with incident response roles and responsibilities; (ii) the organization provides incident response training to personnel with incident response roles and responsibilities; (iii) incident response training material addresses the procedures and activities necessary to fulfill identified organizational incident response roles and responsibilities; (iv) the organization defines the frequency of refresher incident response training; and (v) the organization provides refresher incident response training in accordance with organization-defined frequency, at least annually.				Examine: Incident response policy; procedures addressing incident response training; incident response training material; information system security plan; incident response training records; other relevant documents or records. (M) (H) Interview: Organizational personnel with incident response training and operational responsibilities. (M) (H)	
3	IR-2-1	INCIDENT RESPONSE TRAINING Control Enhancement: The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations	L	M	H		FS/PS/NS

	IR-2-1-1	Determine if the organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.			Examine: Incident response policy; procedures addressing incident response training; incident response training material; other relevant documents or records. (H) Interview: Organizational personnel with incident response training and operational responsibilities. (H)		
4	IR-2-2	INCIDENT RESPONSE TRAINING Control Enhancement: The organization employs automated mechanisms to provide a more thorough and realistic training environment.	L	M	H		FS/PS/NS
	IR-2-2-1	Determine if the organization employs automated incident response training mechanisms to provide a more thorough and realistic training environment.			Examine: Incident response policy; procedures addressing incident response training; incident response training material; automated mechanisms supporting incident response training; other relevant documents or records. Interview: Organizational personnel with incident response training and operational responsibilities. Test: Simulated incident response training events.		

5	IR-3	<p>INCIDENT RESPONSE TESTING AND EXERCISES</p> <p>Control: The organization tests and/or exercises the incident response capability for the information system [Assignment: organization-defined frequency, at least annually] using [Assignment: organization-defined tests and/or exercises] to determine the incident response effectiveness and documents the results.</p>	L M H			FS/PS/NS
	IR-3.1	<p>Determine if:</p> <ul style="list-style-type: none"> (i) the organization defines incident response tests/exercises; (ii) the organization defines the frequency of incident response tests/exercises; (iii) the organization tests/exercises the incident response capability for the information system using organization-defined tests/exercises in accordance with organization-defined frequency; and (iv) the organization documents the results of incident response tests/exercises. 		<p>Examine: Incident response policy; procedures addressing incident response testing and exercises; information system security plan; incident response testing material; incident response test results; other relevant documents or records. (M) (H)</p>		
6	IR-3-1	<p>INCIDENT RESPONSE TESTING AND EXERCISES</p> <p>Control Enhancement:</p> <p>The organization employs automated mechanisms to more thoroughly and effectively test/exercise the incident response capability.</p>	L M H			FS/PS/NS

Copyright© 2008
 Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

	IR-3-1-1	Determine if: (i) the organization employs automated mechanisms to more thoroughly and effectively test/exercise the incident response capability for the information system; and (ii) the automated mechanisms supporting incident response testing provide more complete coverage of incident response issues, more realistic test/exercise scenarios, and a greater stress on the incident response capability.			Examine: Incident response policy; procedures addressing incident response testing and exercises; information system security plan; incident response testing documentation; automated mechanisms supporting incident response tests/exercises; other relevant documents or records. (H) Interview: Organizational personnel with incident response testing responsibilities. (H)		
7	IR-4	INCIDENT HANDLING Control: The organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.	L	M	H		FS/PS/NS
	IR-4.1	Determine if: (i) the organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; and (ii) the incident handling capability is consistent with NIST Special Publication 800-61.			Examine: Incident response policy; procedures addressing incident handling; NIST Special Publication 800-61; other relevant documents or records. (L) (M) (H) Interview: Organizational personnel with incident handling responsibilities. (M) (H) Test: Incident handling capability for the organization. (H)		

8	IR-4-1	INCIDENT HANDLING Control Enhancement: The organization employs automated mechanisms to support the incident handling process.	L	M	H			FS/PS/NS
	IR-4-1-1	Determine if the organization employs automated mechanisms to support the incident handling process.				Examine: Incident response policy; procedures addressing incident handling; automated mechanisms supporting incident handling; other relevant documents or records. (M) (H) Interview: Organizational personnel with incident handling responsibilities. (H)		
9	IR-5	INCIDENT MONITORING Control: The organization tracks and documents information system security incidents on an ongoing basis.	L	M	H			FS/PS/NS
	IR-5.1	Determine if the organization tracks and documents information system security incidents on an ongoing basis.				Examine: incident response policy; procedures addressing incident monitoring; incident response records and documentation; other relevant documents or records. (M) (H) Interview: Organizational personnel with incident monitoring responsibilities. (H) Test: Incident monitoring capability for the organization. (H)		

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

10	IR-5-1	INCIDENT MONITORING Control Enhancement: The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.	L M H			FS/PS/NS
	IR-5-1-1	Determine if the organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.		Examine: Incident response policy; procedures addressing incident monitoring; information system design documentation; information system configuration settings and associated documentation; automated mechanisms supporting incident monitoring; other relevant documents or records. (H) Interview: Organizational personnel with incident monitoring responsibilities. (H)		
11	IR-6	Control: The organization promptly reports incident information to appropriate authorities.	L M H			FS/PS/NS

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

	IR-6.1	Determine if: (i) the organization promptly reports incident information to appropriate authorities; (ii) incident reporting is consistent with NIST Special Publication 800-61. (iii) the types of incident information reported, the content and timeliness of the reports, and the list of designated reporting is consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance; and (iv) weaknesses and vulnerabilities in the information system are reported to appropriate organizational officials in a timely manner to prevent security incidents.				Examine: Incident response policy; procedures addressing incident reporting; NIST Special Publication 800-61; incident reporting records and documentation; other relevant documents or records. (L) (M) (H) Interview: Organizational personnel with incident reporting responsibilities. (M) (H) Test: Incident reporting capability for the organization. (H)	
12	IR-6-1	INCIDENT REPORTING Control Enhancement: The organization employs automated mechanisms to assist in the reporting of security incidents.	L	M	H		FS/PS/NS
	IR-6-1-1	Determine if the organization employs automated mechanisms to assist in the reporting of security incidents.				Examine: Incident response policy; procedures addressing incident reporting; automated mechanisms supporting incident reporting; other relevant documents or records. (M) (H) Interview: Organizational personnel with incident reporting responsibilities. (H)	

13	IR-7	<p>INCIDENT RESPONSE ASSISTANCE</p> <p>Control: The organization provides an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The support resource is an integral part of the organization's incident response capability.</p>	L M H			FS/PS/NS
	IR-7.1	<p>Determine if:</p> <ul style="list-style-type: none"> (i) the organization provides an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents; and (ii) the incident response support resource is an integral part of the organization's incident response capability. 		<p>Examine: Incident response policy; procedures addressing incident response assistance; other relevant documents or records. (L) (M) (H)</p> <p>Interview: Organizational personnel with incident response assistance and support responsibilities. (M) (H)</p>		
14	IR-7-1	<p>INCIDENT RESPONSE ASSISTANCE</p> <p>Control Enhancement:</p> <p>The organization employs automated mechanisms to increase the availability of incident response-related information and support.</p>	L M H			FS/PS/NS

IR-7-1-1	<p>Determine if the organization employs automated mechanisms to increase the availability of incident response-related information and support for incident response support.</p>		<p>Examine: Incident response policy; procedures addressing incident response assistance; automated mechanisms supporting incident response support and assistance; other relevant documents or records. (M) (H)</p> <p>Interview: Organizational personnel with incident response support and assistance responsibilities and organizational personnel that require incident response support and assistance. (H)</p>									
<p>FS - Fully Satisfied PS - Partially Satisfied NS - Not Satisfied Impacts: Low Medium High Assessment Methods: Interview Demonstrate Test Observe</p>				<p>Assessment Results</p> <table border="1" data-bbox="1727 845 2023 1008"> <tr> <td>FS</td><td>0</td></tr> <tr> <td>PS</td><td>0</td></tr> <tr> <td>NS</td><td>0</td></tr> <tr> <td>Total</td><td>0</td></tr> </table>	FS	0	PS	0	NS	0	Total	0
FS	0											
PS	0											
NS	0											
Total	0											

MAINTENANCE

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

FAMILY:		MAINTENANCE	Impact			Assessment Method	Assessment Results	FS/PS/NS
Num	ID	Assessment Procedure	L	M	H			
1	MA-1	SYSTEM MAINTENANCE POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.	L	M	H			FS/PS/NS
	MA-1.1	Determine if: (i) the organization develops and documents information system maintenance policy and procedures; (ii) the organization disseminates information system maintenance policy and procedures to appropriate elements within the organization; (iii) responsible parties within the organization periodically review information system maintenance policy and procedures; and (iv) the organization updates				Examine: Information system maintenance policy and procedures; other relevant documents or records. (L) (M) (H) Interview: Organizational personnel with information system maintenance responsibilities. (H)		

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

		information system maintenance policy and procedures when organizational review indicates updates are required.				
	MA-1.2	Determine if: (i) the information system maintenance policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance; (ii) the information system maintenance policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and (iii) the information system maintenance procedures address all areas identified in the system maintenance policy and address achieving policy-compliant implementations of all associated security controls.			Examine: Information system maintenance policy and procedures; other relevant documents or records. (L) (M) (H) Interview: Organizational personnel with information system maintenance responsibilities. (H)	
2	MA-2	CONTROLLED MAINTENANCE Control: The organization schedules, performs, documents, and reviews records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor	L	M	H	FS/PS/NS

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

		specifications and/or organizational requirements.					
	MA-2.1	Determine if the organization schedules, performs, documents, and reviews records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.				Examine: information system maintenance policy; procedures addressing controlled maintenance for the information system; maintenance records; manufacturer/vendor maintenance specifications; other relevant documents or records. (L) (M) (H) Interview: Organizational personnel with information system maintenance responsibilities. (M) (H)	
3	MA-2-1	CONTROLLED MAINTENANCE Control Enhancement: The organization maintains maintenance records for the information system that include: (i) the date and time of maintenance; (ii) name of the individual performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) a list of equipment removed or replaced (including identification numbers, if applicable).	L	M	H		FS/PS/NS

	MA-2-1-1	Determine if the organization maintains maintenance records for the information system that include: (i) the date and time of maintenance; (ii) name of the individual performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) a list of equipment removed or replaced (including identification numbers, if applicable).				Examine: Information system maintenance policy; procedures addressing controlled maintenance for the information system; maintenance records; other relevant documents or records. (M) (H)		
4	MA-2-2	CONTROLLED MAINTENANCE Control Enhancement: The organization employs automated mechanisms to schedule and conduct maintenance as required, and to create up-to-date, accurate, complete, and available records of all maintenance actions, both needed and completed.	L	M	H			FS/PS/NS
	MA-2-2-1	Determine if the organization employs automated mechanisms to schedule and conduct maintenance as required, and to create accurate, complete, and available records of all maintenance actions, both needed and completed.				Examine: Information system maintenance policy; procedures addressing controlled maintenance for the information system; automated mechanisms supporting information system maintenance activities; information system configuration settings and associated documentation; maintenance records; other relevant documents or records. (H)		

5	MA-3	MAINTENANCE TOOLS Control: The organization approves, controls, and monitors the use of information system maintenance tools and maintains the tools on an ongoing basis.	L	M	H		FS/PS/NS
	MA-3.1	Determine if: (i) the organization approves, controls, and monitors the use of information system maintenance tools; and (ii) the organization maintains maintenance tools on an ongoing basis.				Examine: [SELECT FROM: Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; maintenance records; other relevant documents or records]. (M) (H)	
6	MA-3-1	MAINTENANCE TOOLS Control Enhancement: The organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications.	L	M	H		FS/PS/NS
	MA-3-1-1	Determine if the organization inspects all maintenance tools (e.g., diagnostic and test equipment) carried into a facility by maintenance personnel for obvious improper modifications.				Examine: Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; maintenance records; other relevant documents or records. (H) Interview: Organizational personnel with information system maintenance responsibilities. (H)	

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

7	MA-3-2	<p>MAINTENANCE TOOLS</p> <p>Control Enhancement:</p> <p>The organization checks all media containing diagnostic and test programs for malicious code before the media are used in the information system.</p>	L	M	H			FS/PS/NS
	MA-3-2-1	<p>Determine if the organization checks all media containing diagnostic test programs (e.g., software or firmware used for information system maintenance or diagnostics) for malicious code before the media are used in the information system.</p>				<p>Examine: Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; information system media containing maintenance programs (including diagnostic and test programs); maintenance records; other relevant documents or records. (H)</p> <p>Interview: Organizational personnel with information system maintenance responsibilities. (H)</p>		
8	MA-3-3	<p>MAINTENANCE TOOLS</p> <p>Control Enhancement:</p> <p>The organization checks all maintenance equipment with the capability of retaining information so that no organizational information is written on the equipment or the equipment is appropriately sanitized before release; if the equipment cannot be sanitized, the equipment remains within the facility or is destroyed, unless an appropriate</p>	L	M	H			FS/PS/NS

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

		organization official explicitly authorizes an exception.					
	MA-3-3-1	Determine if: (i) the organization either checks all maintenance equipment with the capability of retaining information so that no organizational information is written on the equipment or the equipment is appropriately sanitized before release; and (ii) the organization retains the maintenance equipment within the facility or destroys the equipment if the equipment cannot be sanitized, unless an appropriate organization official explicitly authorizes an exception.				Examine: Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; information system media containing maintenance programs (including diagnostic and test programs); maintenance records; other relevant documents or records. (H) Interview: Organizational personnel with information system maintenance responsibilities. (H)	
9	MA-3-4	MAINTENANCE TOOLS Control Enhancement: The organization employs automated mechanisms to restrict the use of maintenance tools to authorized personnel only.	L	M	H		FS/PS/NS

	MA-3-4-1	Determine if the organization employs automated mechanisms to restrict the use of maintenance tools to authorized personnel only.				Examine: Information system maintenance policy; information system maintenance tools and associated documentation; procedures addressing information system maintenance tools; automated mechanisms supporting information system maintenance activities; information system design documentation; information system configuration settings and associated documentation; maintenance records; other relevant documents or records. Test: Automated mechanisms supporting information system maintenance activities.		
10	MA-4	REMOTE MAINTENANCE Control: The organization authorizes, monitors, and controls any remotely executed maintenance and diagnostic activities, if employed.	L	M	H			FS/PS/NS
	MA-4.1	Determine if the organization authorizes, monitors, and controls remotely executed maintenance and diagnostic activities, if employed.				Examine: Information system maintenance policy; procedures addressing remote maintenance for the information system; information system design documentation; information system configuration settings and associated documentation; maintenance records; other relevant documents or records. (L) (M) (H) Interview: Organizational personnel		

					with information system maintenance responsibilities. (M) (H)		
11	MA-4-1	REMOTE MAINTENANCE Control Enhancement: The organization audits all remote maintenance and diagnostic sessions and appropriate organizational personnel review the maintenance records of the remote sessions.	L	M	H		FS/PS/NS
	MA-4-1-1	Determine if: (i) the organization audits all remote maintenance and diagnostic sessions; and (ii) designated organizational personnel review the maintenance records of remote sessions				Examine: Information system maintenance policy; procedures addressing remote maintenance for the information system; maintenance records; audit records; other relevant documents or records. (M) (H) Interview: Organizational personnel with information system maintenance responsibilities. (M) (H)	
12	MA-4-2	REMOTE MAINTENANCE Control Enhancement: The organization addresses the installation and use of remote maintenance and diagnostic links in the security plan for the information system.	L	M	H		FS/PS/NS
	MA-4-2-1	Determine if the organization addresses the installation and use of remote maintenance and diagnostic links in the security plan for the information system.				Examine: Information system maintenance policy; procedures addressing remote maintenance for the information system; information system security plan; maintenance records;	

					audit records; other relevant documents or records. (M) (H)		
13	MA-4-3	REMOTE MAINTENANCE Control Enhancement: The organization does not allow remote maintenance or diagnostic services to be performed by a provider that does not implement for its own information system, a level of security at least as high as that implemented on the system being serviced, unless the component being serviced is removed from the information system and sanitized (with regard to organizational information) before the service begins and also sanitized (with regard to potentially malicious software) after the service is performed and before being reconnected to the information system.	L	M	H		FS/PS/NS
	MA-4-3-1	Determine if the organization does not allow remote diagnostic or maintenance services to be performed by a provider that does not implement for its own information system, a level of security at least as high as the level of security implemented on the information system being serviced, unless the component being serviced is removed from the information system and			Examine: Information system maintenance policy; procedures addressing remote maintenance for the information system; service provider contracts and/or service level agreements; maintenance records; audit records; other relevant documents or records. (H) Interview: Organizational personnel with information system maintenance responsibilities; information system		

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

		sanitized (with regard to organizational information) before the service begins and also sanitized (with regard to potentially malicious software) after the service is performed and before being reconnected to the information system.			maintenance provider. (H)		
14	MA-5	MAINTENANCE PERSONNEL Control: The organization allows only authorized personnel to perform maintenance on the information system.	L	M	H		FS/PS/NS
	MA-5.1	Determine if the organization allows only authorized personnel to perform maintenance on the information system.			Examine: Information system maintenance policy; procedures addressing maintenance personnel; service provider contracts and/or service level agreements; list of authorized personnel; maintenance records; other relevant documents or records. (L) (M) (H) Interview: Organizational personnel with information system maintenance responsibilities. (M) (H)		
15	MA-6	TIMELY MAINTENANCE Control: The organization obtains maintenance support and spare parts for [Assignment: organization-defined list of key information system components] within [Assignment: organization-defined time period] of failure.					

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

MA-6.1	<p>Determine if:</p> <ul style="list-style-type: none"> (i) the organization defines key information system components; (ii) the organization defines the time period within which support and spare parts must be obtained after a failure; and (iii) the organization obtains maintenance support and spare parts for the organization-defined list of key information system components within the organization-defined time period of failure. 			<p>Examine: Information system maintenance policy; procedures addressing timely maintenance for the information system; service provider contracts and/or service level agreements; inventory and availability of spare parts; information system security plan; other relevant documents or records. (M) (H)</p> <p>Interview: Organizational personnel with information system maintenance responsibilities. (M) (H)</p>		
FS - Fully Satisfied PS - Partially Satisfied NS - Not Satisfied Impacts: Low Medium High Assessment Methods: Interview Demonstrate Test Observe						Assessment Results
FS	0					
PS	0					
NS	0					
Total	0					

MEDIA PROTECTION

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

A-160

Page 1459 of 1794

FAMILY: MEDIA PROTECTION			Impact			Assessment Method			Assessment Results	FS/PS/NS
Num	ID	Assessment Procedure	L	M	H					
1	MP-1	<p>MEDIA PROTECTION POLICY AND PROCEDURES</p> <p>Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.</p>	L	M	H					FS/PS/NS
	MP-1.1	<p>Determine if:</p> <ul style="list-style-type: none"> (i) the organization develops and documents media protection policy and procedures; (ii) the organization disseminates media protection policy and procedures to appropriate elements within the organization; (iii) responsible parties within the organization periodically review media protection policy and procedures; and (iv) the organization updates media protection policy and procedures when organizational review indicates updates are required. 				<p>Examine: Media protection policy and procedures; other relevant documents or records. (L) (M) (H)</p> <p>Interview: Organizational personnel with information system media protection responsibilities. (H)</p>				

Copyright© 2008
 Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

	MP-1.2	Determine if: (i) the media protection policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance; (ii) the media protection policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and (iii) the media protection procedures address all areas identified in the media protection policy and address achieving policy-compliant implementations of all associated security controls.			Examine: Media protection policy and procedures; other relevant documents or records. (L) (M) (H) Interview: Organizational personnel with information system media protection responsibilities. (H)		
2	MP-2	MEDIA ACCESS Control: The organization restricts access to information system media to authorized individuals.	L	M	H		FS/PS/NS
	MP-2.1	Determine if the organization restricts access to information system media to authorized users.			Examine: Information system media protection policy; procedures addressing media access; access control policy and procedures; physical and environmental protection policy and procedures; media storage facilities; access control records; other relevant documents or records. (L) (M) (H) Interview: Organizational personnel with information system media protection responsibilities. (M) (H)		

3	MP-2-1	<p>MEDIA ACCESS</p> <p>Control Enhancement: The organization employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.</p>	L	M	H			FS/PS/NS
4	MP-2-1-1	<p>Determine if:</p> <ul style="list-style-type: none"> (i) the organization employs automated mechanisms to restrict access to media storage areas; and (ii) the organization employs automated mechanisms to audit access attempts and access granted 				<p>Examine: Information system media protection policy; procedures addressing media access; access control policy and procedures; physical and environmental protection policy and procedures; media storage facilities; access control devices; access control records; audit records; other relevant documents or records. (M) (H)</p> <p>Test: Automated mechanisms implementing access restrictions to media storage areas. (H)</p>		
4	MP-3	<p>MEDIA LABELING</p> <p>Control: The organization: (i) affixes external labels to removable information system media and information system output indicating the distribution limitations, handling caveats and applicable security markings (if any) of the information; and (ii) exempts [Assignment: organization-defined list of media types or hardware components] from labeling so long as they remain within [Assignment: organization-defined protected environment].</p>	L	M	H			FS/PS/NS

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

		Determine if: (i) the organization defines its protected environment for media labeling requirements; (ii) the organization identifies media types and hardware components that are exempted from external labeling requirements; (iii) the organization exempts the organization-defined list of media types and hardware components from labeling so long as they remain within the organization-defined protected environment; and (iv) the organization affixes external labels to removable information storage media and information system output indicating the distribution limitations, handling caveats and applicable security markings (if any) of the information.				Examine: Information system media protection policy; procedures addressing media labeling; physical and environmental protection policy and procedures; information system security plan; removable storage media and information system output; other relevant documents or records. (H)	
5	MP-4	MEDIA STORAGE Control: The organization physically controls and securely stores information system media within controlled areas.	L	M	H		FS/PS/NS

		Determine if: (i) the organization defines controlled areas for information system media; (ii) the organization selects and documents the media and associated information contained on that media requiring physical protection in accordance with an organizational assessment of risk; (iii) the organization defines the specific measures used to protect the selected media and information contained on that media; (iv) the organization physically controls and securely stores information system media within controlled areas; and (v) the organization protects information system media commensurate with the FIPS 199 or FiXs Guidance for security categorization of the information contained on the media.				Examine: Information system media protection policy; procedures addressing media storage; physical and environmental protection policy and procedures; access control policy and procedures; information system security plan; information system media; other relevant documents or records. (M) (H)	
6	MP-5	MEDIA TRANSPORT Control: The organization protects and controls information system media during transport outside of controlled areas and restricts the activities associated with transport of such media to authorized personnel.	L	M	H		FS/PS/NS

	MP-5.1	Determine if: (i) the organization identifies personnel authorized to transport information system media outside of controlled areas; (ii) the organization controls information system media during transport outside of controlled areas; and (iii) the organization restricts the activities associated with transport of information system media to authorized personnel.		Examine: Information system media protection policy; procedures addressing media transport; physical and environmental protection policy and procedures; access control policy and procedures; information system security plan; list of organization-defined personnel authorized to transport information system media outside of controlled areas; information system media; information system media transport records; information system audit records; other relevant documents or records. (M) (H)		
	MP-5-1	Determine if: (i) the organization defines security measures (e.g., locked container, cryptography) for information system media transported outside of controlled areas; (ii) the organization protects digital and non-digital media during transport outside of controlled areas using the organization-defined security measures.		Examine: Information system media protection policy; procedures addressing media transport; physical and environmental protection policy and procedures; access control policy and procedures; information system security plan; information system media transport records; audit records; other relevant documents or records. (M) (H) Interview: Organizational personnel with information system media transport responsibilities. (H)		
7	MP-5-2	MEDIA TRANSPORT Control Enhancement: The organization documents, where appropriate, activities associated with the transport of information system media using [Assignment: organization-defined system of	L M H			FS/PS/NS

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

		records].					
	MP-5-2-1	Determine if: (i) the organization defines a system of records for documenting activities associated with the transport of information system media; and (ii) the organization documents, where appropriate, activities associated with the transport of information system media using the organization-defined system of records.			Examine: Information system media protection policy; procedures addressing media transport; physical and environmental protection policy and procedures; access control policy and procedures; information system security plan; information system media transport records; audit records; other relevant documents or records. (M) (H)		
8	MP-5-3	MEDIA TRANSPORT Control Enhancement: The organization employs an identified custodian at all times to transport information system media.	L	M	H		FS/PS/NS
	MP-5-3-1	Determine if the organization employs an identified custodian at all times to transport information system media.			Examine: Information system media protection policy; procedures addressing media transport; physical and environmental protection policy and procedures; information system media transport records; audit records; other relevant documents or records. (H) Interview: Organizational personnel with information system media transport responsibilities. (H)		

9	MP-6	MEDIA SANITIZATION AND DISPOSAL Control: The organization sanitizes information system media, both digital and non-digital, prior to disposal or release for reuse.	L	M	H			FS/PS/NS
	MP-6.1	Determine if: (i) the organization identifies information system media requiring sanitization and the appropriate sanitization techniques and procedures to be used in the process; (ii) the organization sanitizes identified information system media, both paper and digital, prior to disposal or release for reuse; and (iii) information system media sanitation is consistent with NIST Special Publication 800-88.				<p>Examine: Information system media protection policy; procedures addressing media sanitization and disposal; NIST Special Publication 800-88; media sanitization records; audit records; other relevant documents or records. (L) (M) (H)</p> <p>Interview: Organizational personnel with information system media sanitization responsibilities. (M) (H)</p>		
10	MP-6-1	MEDIA SANITIZATION AND DISPOSAL Control Enhancement: The organization tracks, documents, and verifies media sanitization and disposal actions.	L	M	H			FS/PS/NS
	MP-6-1-1	Determine if the organization tracks, documents, and verifies media sanitization and disposal actions.				<p>Examine: Information system media protection policy and procedures; media sanitization records; audit records; other relevant documents or records. (H)</p> <p>Interview: Organizational personnel with information system media sanitization responsibilities. (H)</p>		

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

11	MP-6-2	MEDIA SANITIZATION AND DISPOSAL Control Enhancement: The organization periodically tests sanitization equipment and procedures to verify correct performance.	L	M	H			FS/PS/NS
	MP-6-2-1	Determine if the organization periodically tests sanitization equipment and procedures to verify correct performance.				Examine: Information system media protection policy; procedures addressing media sanitization and disposal; media sanitization equipment test records; information system audit records; other relevant documents or records. (H) Interview: Organizational personnel with information system media sanitization responsibilities. (H)		
FS - Fully Satisfied PS - Partially Satisfied NS - Not Satisfied Impacts: Low Medium High Assessment Methods: Interview Demonstrate Test Observe								Assessment Results
								FS 0
								PS 0
								NS 0
								Total 0

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

PHYSICAL & ENVIRONMENTAL PROTECTION

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

FAMILY: PHYSICAL & ENVIRONMENTAL PROTECTION			Impact			Assessment Method	Assessment Results	FS/PS/NS
Num	ID	Assessment Procedure	L	M	H			
1	PE-1	PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.	L	M	H			FS/PS/NS
	PE-1.1	Determine if: (i) the organization develops and documents physical and environmental protection policy and procedures; (ii) the organization disseminates physical and environmental protection policy and procedures to appropriate elements within the organization; (iii) responsible parties within the organization periodically review physical and environmental protection policy and procedures; and (iv) the organization updates physical and environmental protection policy and procedures when organizational review indicates updates are required.				Examine: Physical and environmental protection policy and procedures; other relevant documents or records. (L) (M) (H) Interview: Organizational personnel with physical and environmental protection responsibilities. (H)		

	PE-1.2	Determine if: (i) the physical and environmental protection policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance; (ii) the physical and environmental protection policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and (iii) the physical and environmental protection procedures address all areas identified in the physical and environmental protection policy and address achieving policy-compliant implementations of all associated security controls.				Examine: Physical and environmental protection policy and procedures; other relevant documents or records]. (L) (M) (H) Interview: Organizational personnel with physical and environmental protection responsibilities. (H)	
2	PE-2	PHYSICAL ACCESS AUTHORIZATIONS Control: The organization develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and issues appropriate authorization credentials. Designated officials within the organization review and approve the access list and authorization credentials [Assignment: organization-defined frequency, at least annually].	L	M	H		FS/PS/NS

	PE-2.1	Determine if: (i) the organization identifies areas within the facility that are publicly accessible; (ii) the organization defines the frequency of review and approval for the physical access list and authorization credentials for the facility; (iii) the organization develops and keeps current lists of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); (iv) the organization issues appropriate authorization credentials (e.g., badges, identification cards, smart cards); and (v) designated officials within the organization review and approve the access list and authorization credentials at the organization-defined frequency, at least annually.				Examine: [SELECT FROM: Physical and environmental protection policy; procedures addressing physical access authorizations; authorized personnel access list; authorization credentials; other relevant documents or records. (L) (M) (H)]	
3	PE-3	PHYSICAL ACCESS CONTROL Control: The organization controls all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and verifies individual access authorizations before granting access to the facility. The organization controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.	L	M	H		FS/PS/NS

PE-3.1	<p>Determine if:</p> <ul style="list-style-type: none"> (i) the organization controls all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); (ii) the organization verifies individual access authorizations before granting access to the facility; and (iii) the organization also controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk. 			<p>Examine: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; other relevant documents or records. (L) (M) (H)</p> <p>Interview: Organizational personnel with physical access control responsibilities. (H)</p> <p>Test: Physical access control capability. (M) (H)</p>	
PE-3.2	<p>Determine if:</p> <ul style="list-style-type: none"> (i) physical access devices (e.g., keys, locks, card readers) used at the facility are functioning properly and maintenance on these devices occurs on a regular and scheduled basis; (ii) the organization secures keys, combinations and other access devices on a regular basis; and (iii) keys and combinations to locks within the facility are periodically changed or when keys are lost, combinations are compromised, or individuals are transferred or terminated. 			<p>Examine: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; maintenance records; records of key and lock combination changes; storage locations for keys and access devices; other relevant documents or records. (L) (M) (H)</p> <p>Test: Physical access control devices. (M) (H)</p>	

	Determine if: (i) the access control system is consistent with, FiXs Rules and Guidance, applicable FIPS 201 and NIST Special Publication 800-73 (where the FiXs Certified Credential is used as an identification token and token-based access control is employed); (ii) the access control system is consistent with FiXs Rules and Guidance, applicable NIST Special Publication 800-78 (where the token-based access control function employs cryptographic verification); and (iii) the access control system is consistent with FiXs Rules and Guidance and applicable NIST Special Publication 800-76 (where the token-based access control function employs biometric verification).			Examine: Physical and environmental protection policy; procedures addressing physical access control are consistent with FiXs Rules and Guidance, applicable FIPS 201; NIST Special Publications 800-73, 800-76, and 800-78; information system design documentation; other relevant documents or records. (L) (M) (H)	
PE-3.3	Determine if: (i) the access control system is consistent with, FiXs Rules and Guidance, applicable FIPS 201 and NIST Special Publication 800-73 (where the FiXs Certified Credential is used as an identification token and token-based access control is employed); (ii) the access control system is consistent with FiXs Rules and Guidance, applicable NIST Special Publication 800-78 (where the token-based access control function employs cryptographic verification); and (iii) the access control system is consistent with FiXs Rules and Guidance and applicable NIST Special Publication 800-76 (where the token-based access control function employs biometric verification).			Examine: Physical and environmental protection policy; procedures addressing physical access control; FiXs Rules and Guidance, applicable FIPS 201; NIST Special Publications 800-73, 800-76, and 800-78; information system design documentation; other relevant documents or records. (L) (M) (H) Test: Physical access control devices. (M) (H)	

4	PE-3-1	PHYSICAL ACCESS CONTROL Control Enhancement: The organization controls physical access to the information system independent of the physical access controls for the facility.	L	M	H			FS/PS/NS
	PE-3-1	Determine if: (i) the organization identifies specific areas within the facility containing large concentrations of information system components or components requiring additional physical protection; and (ii) for an information system identified as requiring additional physical protection or part of a large concentration of information system components, the organization controls physical access to the system independent of the physical access controls for the facility.				Examine: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; information system entry and exit points; list of areas within the facility containing high concentrations of information system components or information system components requiring additional physical protection; other relevant documents or records. (H)		
5	PE-4	ACCESS CONTROL FOR TRANSMISSION MEDIUM Control: The organization controls physical access to information system distribution and transmission lines within organizational facilities.	L	M	H			FS/PS/NS
	PE-4.1	Determine if the organization controls physical access to information system distribution and transmission lines within organizational facilities.				Examine: Physical and environmental protection policy; procedures addressing access control for transmission medium; information system design documentation; facility		

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

					communications and wiring diagrams; other relevant documents or records. (H)		
6	PE-5	ACCESS CONTROL FOR DISPLAY MEDIUM Control: The organization controls physical access to information system devices that display information to prevent unauthorized individuals from observing the display output.	L	M	H		FS/PS/NS
	PE-5.1	Determine if the organization controls physical access to information system devices that display information to prevent unauthorized individuals from observing the display output.				Examine: Physical and environmental protection policy; procedures addressing access control for display medium; facility layout of information system components; other relevant documents or records. (M) (H)	
7	PE-6	MONITORING PHYSICAL ACCESS Control: The organization monitors physical access to the information system to detect and respond to physical security incidents.	L	M	H		FS/PS/NS
	PE-6.1	Determine if the organization monitors physical access to the information system to detect and respond to physical security incidents.				Examine: Physical and environmental protection policy; procedures addressing physical access monitoring; physical access logs or records; other relevant documents or records. (L) (M) (H) Interview: Organizational personnel with physical access monitoring	

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

						responsibilities. (M) (H) Test: Physical access monitoring capability. (M) (H)		
8	PE-6-1	MONITORING PHYSICAL ACCESS Control Enhancement: The organization monitors real-time physical intrusion alarms and surveillance equipment.	L	M	H			FS/PS/NS
	PE-6-1-1	Determine if the organization monitors real-time intrusion alarms and surveillance equipment.				Examine: Physical and environmental protection policy; procedures addressing physical access monitoring; intrusion alarm/surveillance equipment logs or records; other relevant documents or records. (M) (H) Interview: Organizational personnel with physical access monitoring responsibilities. (H)		
9	PE-6-2	MONITORING PHYSICAL ACCESS Control Enhancement: The organization employs automated mechanisms to recognize potential intrusions and initiate appropriate response actions.	L	M	H			FS/PS/NS
	PE-6-2-1	Determine if the organization employs automated mechanisms to recognize potential intrusions and initiate appropriate response actions.				Examine: Physical and environmental protection policy; procedures addressing physical access monitoring; information system design documentation; other relevant documents or records. (H)		

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

						Test: Automated mechanisms implementing physical access monitoring capability. (H)		
10	PE-7	VISITOR CONTROL Control: The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.	L	M	H			FS/PS/NS
	PE-7.1	Determine if the organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.				Examine: Physical and environmental protection policy; procedures addressing visitor access control; visitor access control logs or records; other relevant documents or records. (L) (M) (H) Interview: Organizational personnel with visitor access control responsibilities. (H) Test: Visitor access control capability. (M) (H)		
11	PE-7-1	VISITOR CONTROL Control Enhancement: The organization escorts visitors and monitors visitor activity, when required	L	M	H			FS/PS/NS

	PE-7-1-1	Determine if the organization escorts visitors and monitors visitor activity, when required.				Examine: Physical and environmental protection policy; procedures addressing visitor access control; visitor access control logs or records; other relevant documents or records. (M) (H) Interview: Organizational personnel with visitor access control responsibilities. (H)	
12	PE-8	ACCESS RECORDS Control: The organization maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) that includes: (i) name and organization of the person visiting; (ii) signature of the visitor; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; and (vii) name and organization of person visited. Designated officials within the organization review the visitor access records [Assignment: organization-defined frequency].	L	M	H		FS/PS/NS

		Determine if: (i) the organization defines the frequency of review for visitor access records; (ii) the organization maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) that includes: - name and organization of the person visiting; - signature of the visitor; - form of identification; - date of access; - time of entry and departure; - purpose of visit; - name and organization of person visited and (iii) designated officials within the organization review the visitor access logs in accordance with organization-defined frequency.				Examine: Physical and environmental protection policy; procedures addressing facility access records; information system security plan; facility access control records; other relevant documents or records. (L) (M) (H)	
13	PE-8-1	ACCESS RECORDS Control Enhancement: The organization employs automated mechanisms to facilitate the maintenance and review of access records.	L	M	H		FS/PS/NS

	PE-8-1-1	Determine the organization employs automated mechanisms to facilitate the maintenance and review of access records.			Examine: Physical and environmental protection policy; procedures addressing facility access records; automated mechanisms supporting management of access records; facility access control logs or records; other relevant documents or records. (H)		
14	PE-8-2	ACCESS RECORDS Control Enhancement: The organization maintains a record of all physical access, both visitor and authorized individuals.	L	M	H		FS/PS/NS
	PE-8-2-1	Determine if the organization maintains a record of all physical access, both visitor and authorized individuals.			Examine: Physical and environmental protection policy; procedures addressing facility access records; facility access control logs or records; other relevant documents or records. (H)		
15	PE-9	POWER EQUIPMENT AND POWER CABLING Control: The organization protects power equipment and power cabling for the information system from damage and destruction.	L	M	H		FS/PS/NS
	PE-9.1	Determine if the organization protects power equipment and power cabling for the information system from damage and destruction.			Examine: Physical and environmental protection policy; procedures addressing power equipment and cabling protection; facility housing power equipment and cabling;		

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

						other relevant documents or records. (M) (H)		
16	PE-9-1	POWER EQUIPMENT AND POWER CABLING Control Enhancement: The organization employs redundant and parallel power cabling paths.	L	M	H			
	PE-9-1-1	Determine if the organization employs redundant and parallel power cabling paths.				Examine: Physical and environmental protection policy; procedures addressing power equipment and cabling protection; facility housing power equipment and cabling; other relevant documents or records.		
17	PE-10	EMERGENCY SHUTOFF Control: The organization provides, for specific locations within a facility containing concentrations of information system resources, the capability of shutting off power to any information system component that may be malfunctioning or threatened without endangering personnel by requiring them to approach the equipment.	L	M	H			FS/PS/NS

		Determine if: (i) the organization defines the specific locations within a facility containing concentrations of information system resources (e.g., data centers, server rooms, mainframe rooms); and (ii) the organization provides, for specific locations within a facility containing concentrations of information system resources, the capability of shutting off power to any information system component that may be malfunctioning or threatened without endangering personnel by requiring them to approach the equipment.				Examine: Physical and environmental protection policy; procedures addressing power source emergency shutoff; emergency shutoff controls or switches; other relevant documents or records. (M) (H)	
18	PE-10-1	EMERGENCY SHUTOFF Control Enhancement: The organization protects the emergency power-off capability from accidental or unauthorized activation.	L	M	H		FS/PS/NS
	PE-10-1-1	Determine if the organization protects the emergency power-off capability from accidental or unauthorized activation.				Examine: Physical and environmental protection policy; procedures addressing power source emergency shutoff; emergency shutoff controls or switches; other relevant documents or records. (H)	
19	PE-11	EMERGENCY POWER Control: The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.	L	M	H		FS/PS/NS

	PE-11.1	Determine if the organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.				Examine: Physical and environmental protection policy; procedures addressing emergency power; uninterruptible power supply documentation; other relevant documents or records. (M) (H) Test: Uninterruptible power supply]. (H)		
20	PE-11-1	EMERGENCY POWER Control Enhancement: The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.	L	M	H			FS/PS/NS
	PE-11-1-1	Determine if the organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.				Examine: Physical and environmental protection policy; procedures addressing emergency power; alternate power supply documentation; alternate power test records; other relevant documents or records. (H) Test: Alternate power supply. (H)		

21	PE-11-2	EMERGENCY POWER Control Enhancement: The organization provides a long-term alternate power supply for the information system that is self-contained and not reliant on external power generation.	L	M	H		FS/PS/NS
	PE-11-2-1	Determine if the organization provides a long-term alternate power supply for the information system that is self-contained and not reliant on external power generation.				Examine: Physical and environmental protection policy; procedures addressing emergency power; alternate power supply documentation; alternate power test records; other relevant documents or records. Test: Alternate power supply.	
22	PE-12	EMERGENCY LIGHTING Control: The organization employs and maintains automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes.	L	M	H		FS/PS/NS
	PE-12.1	Determine if: (i) the organization employs and maintains automatic emergency lighting systems that activates in the event of a power outage or disruption; and (ii) the organization employs and maintains automatic emergency lighting systems that cover emergency exits and evacuation routes.				Examine: Physical and environmental protection policy; procedures addressing emergency lighting; emergency lighting documentation; emergency lighting test records; emergency exits and evacuation routes; other relevant documents or records. (L) (M) (H)	

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

						Test: Emergency lighting capability. (M) (H)		
23	PE-13	FIRE PROTECTION Control: The organization employs and maintains fire suppression and detection devices/systems that can be activated in the event of a fire.	L	M	H			FS/PS/NS
	PE-13.1	Determine if the organization employs and maintains fire suppression and detection devices/systems that can be activated in the event of a fire.				Examine: Physical and environmental protection policy; procedures addressing fire protection; fire suppression and detection devices/systems; fire suppression and detection devices/systems documentation; test records of fire suppression and detection devices/systems; other relevant documents or records. (L) (M) (H)		
24	PE-13-1	FIRE PROTECTION Control Enhancement: The organization employs fire detection devices/systems that activate automatically and notify the organization and emergency responders in the event of a fire.	L	M	H			FS/PS/NS

	PE-13-1-1	Determine if: (i) the organization employs fire detection devices/systems that activate automatically; and (ii) the organization employs fire detection devices/systems that notify the organization and emergency responders in the event of a fire.				Examine: Physical and environmental protection policy; procedures addressing fire protection; facility housing the information system; alarm service level agreements; test records of fire suppression and detection devices/systems; fire suppression and detection devices/systems documentation; other relevant documents or records. (M) (H) Test: Simulated fire detection and automated notifications. (H)	
25	PE-13-2	FIRE PROTECTION Control Enhancement: The organization employs fire suppression devices/systems that provide automatic notification of any activation to the organization and emergency responders.	L	M	H		FS/PS/NS

PE-13-2-1	Determine if the organization employs fire suppression devices/systems that provide automatic notification of any activation to the organization and emergency responders.				Examine: Physical and environmental protection policy; procedures addressing fire protection; fire suppression and detection devices/systems documentation; facility housing the information system; alarm service level agreements; test records of fire suppression and detection devices/systems; other relevant documents or records. (M) (H) Test: Simulated activation of fire suppression devices/systems and automated notifications]. (H)	
26	PE-13-3 FIRE PROTECTION Control Enhancement: The organization employs an automatic fire suppression capability in facilities that are not staffed on a continuous basis.	L	M	H		FS/PS/NS

	PE-13-3-1	Determine if the organization employs an automatic fire suppression capability in facilities that are not staffed on a continuous basis.				Examine: Physical and environmental protection policy; procedures addressing fire protection; facility housing the information system; alarm service level agreements; facility staffing plans; test records of fire suppression and detection devices/systems; other relevant documents or records. (M) (H) Test: Simulated activation of fire suppression devices/systems and automated notifications. (H)		
27	PE-14	TEMPERATURE AND HUMIDITY CONTROLS Control: The organization regularly maintains, within acceptable levels, and monitors the temperature and humidity within the facility where the information system resides.	L	M	H			FS/PS/NS
	PE-14.1	Determine if: (i) the organization regularly maintains, within acceptable levels, the temperature and humidity within the facility where the information system resides; and (ii) the organization regularly monitors the temperature and humidity within the facility where the information system resides.				Examine: Physical and environmental protection policy; procedures addressing temperature and humidity control; facility housing the information system; temperature and humidity controls; temperature and humidity controls documentation; temperature and humidity records; other		

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

					relevant documents or records. (L) (M) (H)	
28	PE-15	<p>WATER DAMAGE PROTECTION</p> <p>Control: The organization protects the information system from water damage resulting from broken plumbing lines or other sources of water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.</p>	L	M	H	FS/PS/NS
	PE-15.1	<p>Determine if:</p> <ul style="list-style-type: none"> (i) the organization identifies key personnel with knowledge of location and operational procedures for activating master shutoff valves for plumbing system; and (ii) the organization protects the information system from water damage resulting from broken plumbing lines or other sources of water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel 			<p>Examine: Physical and environmental protection policy; procedures addressing water damage protection; facility housing the information system; master shutoff values; list of key personnel with knowledge of location and activation procedures for master shutoff values for the plumbing system; master shutoff value documentation; other relevant documents or records. (L) (M) (H)</p> <p>Interview: Organization personnel with physical and environmental protection</p>	

						responsibilities. (M) (H) Test: Simulated master water shutoff value activation for the plumbing system. (M) (H)		
29	PE-15-1	WATER DAMAGE PROTECTION Control Enhancement: The organization employs mechanisms that, without the need for manual intervention, protect the information system from water damage in the event of a significant water leak.	L	M	H			FS/PS/NS
	PE-15-1-1	Determine if the organization employs mechanisms that, without the need for manual intervention, protect the information system from water damage in the event of a significant water leak.				Examine: Physical and environmental protection policy; procedures addressing water damage protection; facility housing the information system; automated mechanisms for water shutoff valves; other relevant documents or records. (H) Test: Automated mechanisms implementing master water shutoff valve activation. (H)		
30	PE-16	DELIVERY AND REMOVAL Control: The organization authorizes and controls information system-related items entering and exiting the facility and maintains appropriate records of those items.	L	M	H			FS/PS/NS

	PE-16.1	Determine if: (i) the organization controls information system-related items (i.e., hardware, firmware, software) entering and exiting the facility; and (ii) the organization maintains appropriate records of items entering and exiting the facility.			Examine: Physical and environmental protection policy; procedures addressing delivery and removal of information system components from the facility; facility housing the information system; records of items entering and exiting the facility; other relevant documents or records. (L) (M) (H)		
					Interview: Organization personnel with tracking responsibilities for information system components entering and exiting the facility. (M) (H)		
31	PE-17	ALTERNATE WORK SITE Control: The organization employs appropriate management, operational, and technical information system security controls at alternate work sites.	L	M	H		FS/PS/NS
	PE-17.1	Determine if the organization employs appropriate management, operational, and technical information system security controls at alternate work sites.			Examine: Physical and environmental protection policy; procedures addressing alternate work sites for organizational personnel; list of management, operational, and technical security controls required for alternate work sites; other relevant		

					documents or records. (M) (H)		
					Interview: Organization personnel using alternate work sites. (M) (H)		
32	PE-18	LOCATION OF INFORMATION SYSTEM COMPONENTS Control: The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	L	M	H		FS/PS/NS
	PE-18.1	Determine if: (i) the organization positions information system components within the facility to minimize potential damage from physical and environmental hazards; and (ii) the organization positions information system components within the facility to minimize the opportunity for unauthorized access.				Examine: Physical and environmental protection policy; procedures addressing positioning of information system components; documentation providing the location and position of information system components within the facility; other relevant documents or records. (M) (H)	
33	PE-18-1	LOCATION OF INFORMATION SYSTEM COMPONENTS Control Enhancement: The organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards and for existing facilities, considers the physical and environmental hazards in its risk mitigation	L	M	H		FS/PS/NS

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

		strategy.					
	PE-18-1-1	Determine if: (i) the organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards; and (ii) the organization, for existing facilities, considers the physical and environmental hazards in its risk mitigation strategy.				Examine: Physical and environmental protection policy; physical site planning documents; organizational assessment of risk, contingency plan; other relevant documents or records. (H) Interview: Organization personnel with site selection responsibilities for the facility housing the information system. (H)	
34	PE-19	INFORMATION LEAKAGE Control: The organization protects the information system from information leakage due to electromagnetic signals emanations.	L	M	H		FS/PS/NS
	PE-19.1	Determine if the organization protects the information system from information leakage due to electromagnetic signals emanations.				Examine: Physical and environmental protection policy; procedures addressing information leakage due to electromagnetic signals emanations; mechanisms	

				protecting the information system against electronic signals emanation; facility housing the information system; records from electromagnetic signals emanation tests; other relevant documents or records.	
FS - Fully Satisfied Partially Satisfied Satisfied	PS - NS - Not	Demonstrate	Test	Observe	Assessment Results
Impacts: Low Medium High					FS 0
Assessment Methods: Interview					PS 0
					NS 0
					Total 0

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

PLANNING

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

FAMILY:		PLANNING	Impact			Assessment Method	Assessment Results	FS/PS/NS
Num	ID	Assessment Procedure	L	M	H			
1	PL-1	<p>SECURITY PLANNING POLICY AND PROCEDURES</p> <p>Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.</p>	L	M	H			FS/PS/NS
	PL-1.1	<p>Determine if:</p> <ul style="list-style-type: none"> (i) the organization develops and documents security planning policy and procedures; (ii) the organization disseminates security planning policy and procedures to appropriate elements within the organization; (iii) responsible parties within the organization periodically review security planning policy and procedures; and (iv) the organization updates security planning policy and procedures when organizational review indicates updates are required. 				<p>Examine: Security planning policy and procedures; other relevant documents or records. (L) (M) (H)</p> <p>Interview: Organizational personnel with information system security planning and plan implementation responsibilities. (H)</p>		

	PL-1.2	Determine if: (i) the security planning policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance; (ii) the security planning policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and (iii) the security planning procedures address all areas identified in the security planning policy and address achieving policy-compliant implementations of all associated security controls.				Examine: Security planning policy and procedures; other relevant documents or records. (L) (M) (H) Interview: Organizational personnel with information system security planning and plan implementation responsibilities. (H)		
2	PL-2	SYSTEM SECURITY PLAN Control: The organization develops and implements a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization review and approve the plan.	L	M	H			FS/PS/NS
	PL-2.1	Determine if: (i) the organization develops and implements a security plan for the information system; (ii) the security plan provides an overview of the security requirements for the information system and a description of the security controls planned or in place for meeting the security requirements; (iii) the security plan development is consistent with NIST Special Publication 800-18 and the concepts in the NIST Risk Management Framework including baseline security control selection,				Examine: Security planning policy; procedures addressing information system security plan development and implementation; NIST Special Publication 800-18; security plan for the information system; other relevant documents or records. (L) (M) (H)		

		tailoring of the baseline, and supplementation of the tailored baseline; (iv) the security plan is consistent with the organization's information system architecture and information security architecture; and (v) designated organizational officials review and approve the security plan.			Interview: Organizational personnel with information system security planning and plan implementation responsibilities. (M) (H)		
3	PL-3	SYSTEM SECURITY PLAN UPDATE Control: The organization reviews the security plan for the information system [Assignment: organization-defined frequency, at least annually] and revises the plan to address system/organizational changes or problems identified during plan implementation or security control assessments.	L	M	H		FS/PS/NS
	PL-3.1	Determine if: (i) the organization defines the frequency of information system security plan reviews and updates; (ii) the organization updates the security plan in accordance with organization-defined frequency, at least annually; (iii) the organization receives input to update the security plan from the organization's configuration management and control process; and (iv) the updated security plan reflects the information system and organizational changes or problems identified during the implementation of the plan or the assessment of the security controls.				Examine: Security planning policy; procedures addressing information system security plan updates; information system security plan; configuration management policy and procedures; configuration management documents; security plan for the information system; record of security plan reviews and updates; other relevant documents or records. (L) (M) (H)	

4	PL-4	<p>RULES OF BEHAVIOR</p> <p>Control: The organization establishes and makes readily available to all information system users, a set of rules that describes their responsibilities and expected behavior with regard to information and information system usage. The organization receives signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information.</p>	<input type="checkbox"/> L <input type="checkbox"/> M <input type="checkbox"/> H			FS/PS/NS
	PL-4.1	<p>Determine if:</p> <ul style="list-style-type: none"> (i) the organization establishes a set of rules that describe user responsibilities and expected behavior with regard to information system usage; (ii) the organization makes the rules available to all information system users; (iii) the rules of behavior for organizational personnel are consistent with NIST Special Publication 800-18; and (iv) the organization receives a signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information. 		<p>Examine: Security planning policy; procedures addressing rules of behavior for information system users; NIST Special Publication 800-18; rules of behavior; other relevant documents or records. (L) (M) (H)</p> <p>Interview: Organizational personnel who are authorized users of the information system and have signed rules of behavior. (M) (H)</p>		
5	PL-5	<p>PRIVACY IMPACT ASSESSMENT</p> <p>Control: The organization conducts a privacy impact assessment on the information system in accordance with OMB policy.</p>	<input type="checkbox"/> L <input type="checkbox"/> M <input type="checkbox"/> H			FS/PS/NS
	PL-5.1	<p>Determine if:</p> <ul style="list-style-type: none"> (i) the organization conducts a privacy impact 		<p>Examine: Security planning policy; procedures addressing</p>		

	<p>assessment on the information system in accordance with OMB policy; and</p> <p>(ii) the privacy impact assessment is consistent with appropriate FiXs rules, federal legislation and OMB policy.</p>				<p>privacy impact assessments on the information system; appropriate FiXs rules, federal legislation and OMB policy; privacy impact assessment; other relevant documents or records. (L) (M) (H)</p>		
PL-5.1	<p>Determine if:</p> <p>(i) the organization conducts a privacy impact assessment on the information system in accordance with FiXs Rules, applicable OMB policy; and</p> <p>(ii) the privacy impact assessment is consistent with FiXs Rules, and appropriate federal legislation and OMB policy.</p>				<p>Examine: Security planning policy; procedures addressing privacy impact assessments on the information system; appropriate FiXs Rules, applicable federal legislation and OMB policy; privacy impact assessment; other relevant documents or records. (L) (M) (H)</p>		
PL-6	<p>SECURITY-RELATED ACTIVITY PLANNING</p> <p>Control: The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.</p>	L	M	H			FS/PS/NS

PL-6.1	Determine if: (i) the organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations, organizational assets, and individuals; and (ii) the organization's advance planning and coordination of security-related activities includes both emergency and non-emergency situations.			Examine: Security planning policy; procedures addressing security-related activity planning for the information system; other relevant documents or records. (M) (H) Interview: [SELECT FROM: Organizational personnel with information system security planning and plan implementation responsibilities]. (M) (H)	
Assessment Methods: Interview Demonstrate Test Observe					Assessment Results
					FS 0
					PS 0
					NS 0
					Total 0

PERSONNEL SECURITY

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

A-204

Page 1503 of 1794

Family:		Personnel Security	Impact			Assessment Method	Assessment Results	FS/PS/NS
Num	ID	Assessment Procedure	L	M	H			
1	PS-1	<p>PERSONNEL SECURITY POLICY AND PROCEDURES</p> <p>Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.</p>	L	M	H			FS/PS/NS
	PS-1.1	<p>Determine if:</p> <ul style="list-style-type: none"> (i) the organization develops and documents personnel security policy and procedures; (ii) the organization disseminates personnel security policy and procedures to appropriate elements within the organization; (iii) responsible parties within the organization periodically review personnel security policy and procedures; and (iv) the organization 				<p>Examine: Personnel security policy and procedures, other relevant documents or records. (L) (M) (H)</p> <p>Interview: Organizational personnel with personnel security responsibilities. (H)</p>		

Copyright© 2008
 Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

		updates personnel security policy and procedures when organizational review indicates updates are required.					
	PS-1.2	Determine if: (i) the personnel security policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance; (ii) the personnel security policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and (iii) the personnel security procedures address all areas identified in the personnel security policy and address achieving policy-compliant implementations of all associated security controls.				Examine: Personnel security policy and procedures; other relevant documents or records. (L) (M) (H) Interview: Organizational personnel with personnel security responsibilities. (H)	
2	PS-2	POSITION CATEGORIZATION Control: The organization assigns a risk designation to all positions and establishes screening criteria for individuals filling those positions. The organization reviews and revises position risk designations [Assignment: organization-defined frequency].	L	M	H		FS/PS/NS

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

	PS-2.1	Determine if: (i) the organization assigns a risk designations to all positions within the organization; (ii) the organization establishes a screening criteria for individuals filling organizational positions; (iii) the risk designations for the organizational positions are consistent with applicable FiXs Rules, federal regulations and OPM policy and guidance, and/or FiXs Rules; (iv) the organization defines the frequency of risk designation reviews and updates for organizational positions; and (v) the organization reviews and revises position risk designations in accordance with the organization-defined frequency.				Examine: Personnel security policy; procedures addressing position categorization; appropriate codes of federal regulations, applicable FiXs Rules; OPM policy and guidance; list of risk designations for organizational positions; information system security plan; records of risk designation reviews and updates; other relevant documents or records. (L) (M) (H)	
3	PS-3	PERSONNEL SCREENING Control: The organization screens individuals requiring access to organizational information and information systems before authorizing access.	L	M	H		FS/PS/NS

	PS-3.1	Determine if: (i) the organization screens individuals requiring access to organizational information and information systems prior to authorizing access; and (ii) the personnel screening is consistent with appropriate FiXs Rules, legislation, OPM policy, regulations, and guidance, FIPS 201 and NIST Special Publications 800-73, 800-76, and 800-78, and the criteria established for the risk designation for the assigned position.				Examine Personnel security policy; procedures addressing personnel screening; records of screened personnel; FIPS 201; NIST Special Publications 800-73, 800-76, and 800-78; other relevant documents or records. (L) (M) (H)	
4	PS-4	PERSONNEL TERMINATION Control: The organization, upon termination of individual employment, terminates information system access, conducts exit interviews, retrieves all organizational information system-related property, and provides appropriate personnel with access to official records created by the terminated employee that are stored on organizational information systems.	L	M	H		FS/PS/NS

	PS-4.1	Determine if: (i) the organization terminates information system access upon termination of individual employment; (ii) the organization conducts exit interviews of terminated personnel; (iii) the organization retrieves all organizational information system-related property from terminated personnel; and (iv) the organization retains access to official documents and records on organizational information systems created by terminated personnel.				Examine: Personnel security policy; procedures addressing personnel termination; records of personnel termination actions; list of information system accounts; other relevant documents or records. (L) (M) (H) Interview: Organizational personnel with personnel security responsibilities. (M) (H)	
5	PS-5	PERSONNEL TRANSFER Control: The organization reviews information systems/facilities access authorizations when personnel are reassigned or transferred to other positions within the organization and initiates appropriate actions.	L	M	H		FS/PS/NS

	PS-5.1	Determine if: (i) the organization reviews information systems/facilities access authorizations when personnel are reassigned or transferred to other positions within the organization; and (ii) the organization initiates appropriate actions (e.g., reissuing keys, identification cards, building passes; closing old accounts and establishing new accounts; and changing system access authorization) for personnel reassigned or transferred within the organization.				Examine: Personnel security policy; procedures addressing personnel transfer; records of personnel transfer actions; list of information system and facility access authorizations; other relevant documents or records. (L) (M) (H)	
6	PS-6	ACCESS AGREEMENTS Control: The organization completes appropriate signed access agreements for individuals requiring access to organizational information and information systems before authorizing access and reviews/updates the agreements [Assignment: organization-defined frequency].	L	M	H		FS/PS/NS

	PS-6.1	Determine if: (i) the organization completes appropriate access agreements for individuals requiring access to organizational information and information systems before authorizing access; (ii) organizational personnel sign access agreements; (iii) the organization defines the frequency of reviews and updates for access agreements; and (iv) the organization reviews and updates the access agreements in accordance with the organization-defined frequency.				Examine: Personnel security policy; procedures addressing access agreements for organizational information and information systems; information system security plan; access agreements; records of access agreement reviews and updates; other relevant documents or records. (L) (M) (H)	
7	PS-7	THIRD-PARTY PERSONNEL SECURITY Control: The organization establishes personnel security requirements including security roles and responsibilities for third-party providers and monitors provider compliance.	L	M	H		FS/PS/NS

	PS-7.1	Determine if: (i) the organization establishes personnel security requirements, including security roles and responsibilities, for third-party providers (e.g., service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, network and security management); (ii) the organization explicitly includes personnel security requirements in acquisition-related documents in accordance with NIST Special Publication 800-35; and (iii) the organization monitors third-party provider compliance with personnel security requirements.					Examine: Personnel security policy; procedures addressing third-party personnel security; list of personnel security requirements; acquisition documents; compliance monitoring process; other relevant documents or records. (L) (M) (H)		
8	PS-8	PERSONNEL SANCTIONS Control: The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.	L	M	H				FS/PS/NS

PS-8.1	Determine if: (i) the organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures; and (ii) the personnel sanctions process is consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.				Examine: Personnel security policy; procedures addressing personnel sanctions; rules of behavior; records of formal sanctions; other relevant documents or records. (L) (M) (H)	
FS - Fully Satisfied PS - Partially Satisfied NS - Not Satisfied						Assessment Results
Impacts: Low Medium High						FS
Assessment Methods: Interview Demonstrate Test Observe						PS
						NS
						Total
						0
						0
						0
						0

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

RISK ASSESSMENT

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

A-214

Page 1513 of 1794

FAMILY: RISK ASSESSMENT			Impact			Assessment Method	Assessment Results	FS/PS/NS
Num	ID	Assessment Procedure	L	M	H			
1	RA-1	RISK ASSESSMENT POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.	L	M	H			FS/PS/NS
	RA-1.1	Determine if: (i) the organization develops and documents risk assessment policy and procedures; (ii) the organization disseminates risk assessment policy and procedures to appropriate elements within the organization; (iii) responsible parties within the organization periodically review risk assessment policy and procedures; and (iv) the organization updates risk assessment policy and procedures when organizational review indicates updates are required.				Examine: Risk assessment policy and procedures; other relevant documents or records. (L) (M) (H) Interview: Organizational personnel with risk assessment responsibilities. (H)		

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

	RA-1.2	Determine if: (i) the risk assessment policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance; (ii) the risk assessment policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and (iii) the risk assessment procedures address all areas identified in the risk assessment policy and address achieving policy-compliant implementations of all associated security controls.				Examine: Risk assessment policy and procedures; other relevant documents or records. (L) (M) (H) Interview: Organizational personnel with risk assessment responsibilities. (H)		
2	RA-2	SECURITY CATEGORIZATION Control: The organization categorizes the information system and the information processed, stored, or transmitted by the system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance and documents the results (including supporting rationale) in the system security plan. Designated senior-level officials within the organization review and approve the security categorizations.	L	M	H			FS/PS/NS
	RA-2.1	Determine if: (i) the organization conducts the security categorization of the information system as an organization-wide exercise with the involvement of senior-level personnel including, but not limited to, FiXs authorizing official, information system owners, chief information officer, senior				Examine: Risk assessment policy; procedures addressing security categorization of organizational information and information systems; security planning policy and procedures; (ii) the security categorization is consistent		

3	RA-3	<p>RISK ASSESSMENT</p> <p>Control: The organization conducts assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the FiXs Network (including information and information systems managed/operated by external parties).</p>	L	M	H	FS/PS/NS

	RA-3.1	Determine if: (i) the organization assesses the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support its operations and assets (including information and information systems managed/operated by external parties); and (ii) the risk assessment is consistent with the NIST Special Publication 800-30.				Examine: Risk assessment policy; security planning policy and procedures; procedures addressing organizational assessments of risk; risk assessment; NIST Special Publication 800-30; other relevant documents or records. (L) (M) (H) Interview: Organizational personnel with risk assessment responsibilities. (M) (H)		
4	RA-4	RISK ASSESSMENT UPDATE Control: The organization updates the risk assessment [Assignment: organization-defined frequency] or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system.	L	M	H			FS/PS/NS

	RA-4.1	Determine if: (i) the organization defines the frequency of risk assessment updates; (ii) the organization updates the risk assessment in accordance with the organization-defined frequency or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system; (iii) the risk assessment update is consistent with the NIST Special Publications 800-30; and (iv) the revised risk assessment reflects the needed changes based on the organization's experiences during security plan implementation.				Examine: Risk assessment policy; security planning policy and procedures; procedures addressing risk assessment updates; risk assessment; information system security plan; records of risk assessment updates; NIST Special Publication 800-30; other relevant documents or records. (L) (M) (H)	
5	RA-5	VULNERABILITY SCANNING Control: The organization scans for vulnerabilities in the information system [Assignment: organization-defined frequency] or when significant new vulnerabilities potentially affecting the system are identified and reported.	L	M	H		FS/PS/NS

	RA-5.1	Determine if: (i) the organization defines the frequency of vulnerability scans within the information system; (ii) the organization scans for vulnerabilities in the information system in accordance with the organization-defined frequency or when significant new vulnerabilities affecting the system are identified and reported; (iii) the organization uses appropriate scanning tools and techniques to conduct the vulnerability scans including those tools that ensure interoperability among tools and automate parts of the vulnerability management process by using standards for (a) enumerating platforms, software flaws, and improper configurations, (b) formatting and making transparent checklists and test procedures, and (c) measuring vulnerability impact; (iv) the organization performs network vulnerability scanning in accordance with NIST Special Publication 800-42; and (v) the organization handles patch and vulnerability management in accordance with NIST Special Publication 800-40.				Examine: Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; information system security plan; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records. (M) (H)		
6	RA-5(1)	VULNERABILITY SCANNING Control Enhancement: The organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned.	L	M	H			FS/PS/NS

	RA-5(1).1	Determine if: (i) the organization uses vulnerability scanning tools that have the capability to readily update the list of information system vulnerabilities scanned; and (ii) the vulnerability scanning tools retrieve updated lists of information system vulnerabilities from the National Vulnerability Database (NVD).			Examine: Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; vulnerability scanning tools and techniques documentation; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records. (H) Test: Vulnerability scanning capability and associated scanning tools. (H)		
7	RA-5-2	VULNERABILITY SCANNING Control Enhancement: The organization updates the list of information system vulnerabilities scanned [Assignment: organization-defined frequency] or when significant new vulnerabilities are identified and reported.	L	M	H		FS/PS/NS
	RA-5-2-1	Determine if: (i) the organization defines the frequency of updates for information system vulnerabilities scanned; and (ii) the organization updates the list of information system vulnerabilities scanned in accordance with the organization-defined frequency or when significant new vulnerabilities are identified and reported.				Examine: Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; information system security plan; list of vulnerabilities scanned; records of updates to vulnerabilities scanned; other relevant documents or records. (H)	

8	RA-5-3	VULNERABILITY SCANNING Control Enhancement: The organization employs vulnerability scanning procedures that can demonstrate the breadth and depth of scan coverage, including vulnerabilities checked and information system components scanned.	L	M	H			FS/PS/NS
	RA-5-3-1	Determine if: (i) the organization implements procedures that can demonstrate the breadth of scan coverage (including information system components scanned); and (ii) the organization implements procedures that can demonstrate the depth of scan coverage (including vulnerabilities checked).				Examine: Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; list of vulnerabilities scanned and information system components checked; other relevant documents or records.		
FS - Fully Satisfied PS - Partially Satisfied NS - Not Satisfied Impacts: Low Medium High Assessment Methods: Interview Demonstrate Test Observe								Assessment Results
								FS 0
								PS 0
								NS 0
								Total 0

SYSTEM & SERVICES ACQUISITION

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

A-223

Page 1522 of 1794

FAMILY: SYSTEM & SERVICES ACQUISITION			Impact			Assessment Method			Assessment Results	FS/PS/NS
Num	ID	Assessment Procedure	L	M	H					
1	SA-1	SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.	L	M	H					FS/PS/NS
	SA-1.1	Determine if: (i) the organization develops and documents system and services acquisition policy and procedures; (ii) the organization disseminates system and services acquisition policy and procedures to appropriate elements within the organization; (iii) responsible parties within the organization periodically review system and services acquisition policy and procedures; and (iv) the				Examine: System and services acquisition policy and procedures; other relevant documents or records. (L) (M) (H) Interview: Organizational personnel with system and services acquisition responsibilities. (H)				

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

		organization updates system and services acquisition policy and procedures when organizational review indicates updates are required.					
	SA-1.2	Determine if: (i) the system and services acquisition policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance; (ii) the system and services acquisition policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and (iii) the system and services acquisition procedures address all areas identified in the system and services acquisition policy and address achieving policy-compliant implementations of all associated security controls.			Examine: System and services acquisition policy and procedures; other relevant documents or records. (L) (M) (H) Interview: organizational personnel with system and services acquisition responsibilities. (H)		
2	SA-2	ALLOCATION OF RESOURCES Control: The organization determines, documents, and allocates as part of its capital planning and investment control process, the resources required to adequately protect the information system.	L	M	H		FS/PS/NS

	SA-2.1	Determine if: (i) the organization determines, documents, and allocates as part of its capital planning and investment control process, the resources required to adequately protect the information system; (ii) the organization determines security requirements for the information system in mission/business case planning; (iii) the organization establishes a discrete line item for information system security in the organization's programming and budgeting documentation; and (iv) the organization's programming and budgeting process is consistent with NIST Special Publication 800-65.				Examine: System and services acquisition policy; procedures addressing the allocation of resources to information security requirements; NIST Special Publication 800-65; other relevant documents or records. (L) (M) (H) Interview: Organizational personnel with capital planning and investment responsibilities. (H)	
3	SA-3	LIFE CYCLE SUPPORT Control: The organization manages the information system using a system development life cycle methodology that includes information security considerations.	L	M	H		FS/PS/NS
	SA-3.1	Determine if: (i) the organization manages the information system using a system development life cycle methodology that includes information security considerations; and (ii) the organization uses a system development life cycle that is consistent with NIST Special Publication 800-64.				Examine: System and services acquisition policy; procedures addressing the integration of information security into the system development life cycle process; NIST Special Publication 800-64; information system development life cycle	

					documentation; other relevant documents or records. (L) (M) (H)	
					Interview: Organizational personnel with information security and system life cycle development responsibilities. (H)	
4	SA-4	ACQUISITIONS Control: The organization includes security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards.	L	M	H	
	SA-4.1	Determine if: (i) the organization includes security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards; (ii) the organization's acquisition of commercial information technology products is consistent with NIST Special Publication 800-23; (iii) references to security			Examine: System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; NIST Special Publications 800-23 and 800-70; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records. (L) (M) (H)	

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

		configuration settings and security implementation guidance in organizational acquisitions are consistent with NIST Special Publication 800-70; and (iv) acquisition contracts for information systems include, either explicitly or by reference, security requirements and/or security specifications that describe: - required security capabilities; - required design and development processes; - required test and evaluation procedures; and - required documentation.			Interview: Organizational personnel with information system security, acquisition, and contracting responsibilities. (H)	
5	SA-4-1	ACQUISITIONS Control Enhancement: The organization requires in solicitation documents that appropriate documentation be provided describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.	L	M	H	FS/PS/NS

	SA-4-1-1	Determine if the organization requires in solicitation documents that appropriate documentation be provided describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.				Examine: System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records. (M) (H) Interview: Organizational personnel with information system security, acquisition, and contracting responsibilities. (M) (H)	
6	SA-4-2	ACQUISITIONS Control Enhancement: The organization requires in solicitation documents that appropriate documentation be provided describing the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components).	L	M	H		FS/PS/NS

	SA-4-2-1	Determine if the organization requires in solicitation documents that appropriate documentation be provided describing the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components).				Examine: System and services acquisition policy; procedures addressing the integration of information security requirements and/or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for information systems or services; other relevant documents or records. Interview: Organizational personnel with information system security, acquisition, and contracting responsibilities.	
7	SA-5	INFORMATION SYSTEM DOCUMENTATION Control: The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system.	L	M	H		FS/PS/NS

	SA-5.1	Determine if: (i) the organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system; (ii) the organization makes available information on configuring, installing, and operating the information system; and (iii) the organization makes available information on effectively using the security features in the information system			Examine: System and services acquisition policy; procedures addressing information system documentation; information system documentation including administrator and user guides; other relevant documents or records. (L) (M) (H)		
8	SA-5.1	INFORMATION SYSTEM DOCUMENTATION Control Enhancement: The organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls	L	M	H		FS/PS/NS

	SA-5-1	Determine if the organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.			Examine: System and services acquisition policy; procedures addressing information system documentation; information system design documentation; other relevant documents or records. (M) (H)		
9	SA-5-2	INFORMATION SYSTEM DOCUMENTATION Control Enhancement: The organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components).	L	M	H		FS/PS/NS

	SA-5-2-1	Determine if the organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components).			Examine: System and services acquisition policy; procedures addressing information system documentation; information system design documentation; other relevant documents or records. (H) Interview: Organizational personnel with information system security documentation responsibilities; organizational personnel operating, using, and/or maintaining the information system. (H)		
10	SA-6	SOFTWARE USAGE RESTRICTIONS Control: The organization complies with software usage restrictions.	L	M	H		FS/PS/NS
	SA-6.1	Determine if: (i) The organization complies with software usage restrictions; and (ii) the organization regularly reviews/analyzes software usage for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.			Examine: System and services acquisition policy; procedures addressing software usage restrictions; site license documentation; list of software usage restrictions; other relevant documents or records. (L) (M) (H) Interview: Organizational		

						personnel with information system administration responsibilities; organizational personnel operating, using, and/or maintaining the information system. (H)		
11	SA-7	USER INSTALLED SOFTWARE Control: The organization enforces explicit rules governing the installation of software by users.	L	M	H			FS/PS/NS
	SA-7.1	Determine if: (i) the organization enforces explicit rules governing the installation of software by users; (ii) unauthorized software is present on the system; and (iii) the organization regularly reviews/analyzes user installed software for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary action.				<p>Examine: System and services acquisition policy; procedures addressing user installed software; list of rules governing user installed software; network traffic on the information system; other relevant documents or records. (L) (M) (H)</p> <p>Interview: Organizational personnel with information system administration responsibilities; organizational personnel operating, using, and/or maintaining the information system. (M) (H)</p> <p>Test: Enforcement of rules for user installed software on the information system;</p>		

						information system for prohibited software. (H)		
12	SA-8	SECURITY ENGINEERING PRINCIPLES Control: The organization designs and implements the information system using security engineering principles.	L	M	H			FS/PS/NS
	SA-8.1	Determine if: (i) the organization designs and implements the information system using security engineering principles; and (ii) the organization considers security design principles in the development and implementation of the information system consistent with NIST Special Publication 800-27.				Examine: System and services acquisition policy; procedures addressing security engineering principles used in the development and implementation of the information system; NIST Special Publication 800-27; information system design documentation; security requirements and security specifications for the information system; other relevant documents or records. (M) (H) Interview: Organizational personnel with system and services acquisition responsibilities. (H)		

13	SA-9	<p>EXTERNAL INFORMATION SYSTEM SERVICES</p> <p>Control: The organization: (i) requires that providers of external information system services employ adequate security controls in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, guidance, and established service-level agreements; and (ii) monitors security control compliance.</p>	L	M	H			FS/PS/NS
	SA-9.1	<p>Determine if:</p> <p>(i) the organization requires that providers of external information system services employ adequate security controls in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, guidance, and established service-level agreements; (ii) the organization monitors security control compliance; (iii) the organization regularly reviews/analyzes outsourced information system services for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions; and (iv) the security controls employed by providers of external information system services are compliant with</p>				<p>Examine: System and services acquisition policy; procedures addressing external information system services; acquisition contracts and service level agreements; organizational security requirements and security specifications for external provider services; security control assessment evidence from external providers of information system services; other relevant documents or records. (L) (M) (H)</p> <p>Interview: Organizational personnel with system and services acquisition responsibilities; external providers of information system services. (H)</p>		

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

		applicable federal laws, directives, policies, regulations, standards, guidance, and established service level agreements.					
14	SA-10	DEVELOPER CONFIGURATION MANAGEMENT Control: The organization requires that information system developers create and implement a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation.	L	M	H		FS/PS/NS
	SA-10.1	Determine if the organization requires that information system developers (and systems integrators) create and implement a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation.				Examine: System and services acquisition policy; procedures addressing information system developer/integrator configuration management; acquisition contracts and service level agreements; information system developer/integrator configuration management plan; security flaw tracking records; system change authorization records; other relevant documents or records. (H)	

15	SA-11	DEVELOPER SECURITY TESTING Control: The organization requires that information system developers create a security test and evaluation plan, implement the plan, and document the results.	L	M	H			FS/PS/NS
	SA-11.1	Determine if the organization requires that information system developers (and systems integrators) create a security test and evaluation plan, implement the plan, and document the results.				Examine: System and services acquisition policy; procedures addressing information system developer/integrator security testing; acquisition contracts and service level agreements; information system developer/integrator security test plans; records of developer/integrator security testing results for the information system; other relevant documents or records. (M) (H)		
FS - Fully Satisfied PS - Partially Satisfied NS - Not Satisfied Impacts: Low Medium High Assessment Methods: Interview Demonstrate Test Observe								Assessment Results
								FS 0
								PS 0
								NS 0
								Total 0

SYSTEM & COMMUNICATION PROTECTION

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

A-239

Page 1538 of 1794

FAMILY: SYSTEM & COMMUNICATION PROTECTION			Impact			Assessment Method	Assessment Results	FS/PS/NS
Num	ID	Assessment Procedure	L	M	H			
1	SC-1	<p>SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES</p> <p>Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.</p>	L	M	H			FS/PS/NS
	SC-1.1	<p>Determine if:</p> <p>(i) the organization develops and documents system and communications protection policy and procedures; (ii) the organization disseminates system and communications protection policy and procedures to appropriate elements within the organization; (iii) responsible parties within the organization periodically review system and communications protection policy and procedures; and (iv) the</p>				<p>Examine: system and communications protection policy and procedures; other relevant documents or records. (L) (M) (H)</p> <p>Interview: Organizational personnel with system and communications protection responsibilities. (H)</p>		

Copyright© 2008
 Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

		organization updates system and communications protection policy and procedures when organizational review indicates updates are required.				
	SC-1.2	Determine if: (i) the system and communications protection policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance; (ii) the system and communications protection policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and (iii) the system and communications protection procedures address all areas identified in the system and communications protection policy and address achieving policy-compliant implementations of all associated security controls.			Examine: System and communications protection policy and procedures; other relevant documents or records. (L) (M) (H) Interview: Organizational personnel with system and communications protection responsibilities. (H)	
2	SC-2	Control: The information system separates user functionality (including user interface services) from information system management functionality.	L	M	H	FS/PS/NS

	SC-2.1	Determine if the information system separates user functionality (including user interface services) from information system management functionality.				Examine: System and communications protection policy; procedures addressing application partitioning; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. (M) (H) Test: separation of user functionality from information system management functionality. (H)		
3	SC-3	SECURITY FUNCTION ISOLATION Control: The information system isolates security functions from non-security functions.	L	M	H			FS/PS/NS
	SC-3.1	Determine if: (i) the organization defines the security functions of the information system to be isolated from non-security functions; and (ii) the information system isolates security functions from non-security functions.				Examine: system and communications protection policy; procedures addressing security function isolation; list of security functions to be isolated from non-security functions; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. (H) Test: Separation of security		

						functions from non-security functions within the information system. (H)		
4	SC-3-1	SECURITY FUNCTION ISOLATION Control Enhancement: The information system employs underlying hardware separation mechanisms to facilitate security function isolation.	L	M	H			FS/PS/NS
	SC-3-1-1	Determine if the information system employs underlying hardware separation mechanisms to facilitate security function isolation.				Examine: System and communications protection policy; procedures addressing security function isolation; information system design documentation; hardware separation mechanisms; information system configuration settings and associated documentation; other relevant documents or records. Test: Hardware separation mechanisms facilitating security function isolation.		
5	SC-3-2	SECURITY FUNCTION ISOLATION Control Enhancement: The information system isolates critical security functions (i.e., functions enforcing access and information flow control) from both non-security functions and from other security functions.	L	M	H			FS/PS/NS

	SC-3-2-1	Determine if: (i) the organization defines the critical security functions of the information system to be isolated from both non-security functions and from other security functions; and (ii) the information system isolates critical security functions from both non-security functions and from other security functions.			Examine: System and communications protection policy; procedures addressing security function isolation; list of critical security functions; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. Test: Isolation of critical security functions.		
6	SC-3-3	SECURITY FUNCTION ISOLATION Control Enhancement: The information system minimizes the number of non-security functions included within the isolation boundary containing security functions.	L	M	H		FS/PS/NS
	SC-3-3-1	Determine if the information system minimizes the number of non-security functions included within the isolation boundary containing security functions.			Examine: System and communications protection policy; procedures addressing security function isolation; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.		

7	SC-3-4	SECURITY FUNCTION ISOLATION Control Enhancement: The information system security functions are implemented as largely independent modules that avoid unnecessary interactions between modules.	L	M	H			FS/PS/NS
	SC-3-4-1	Determine if the information system security functions are implemented as largely independent modules that avoid unnecessary interactions between modules.				Examine: System and communications protection policy; procedures addressing security function isolation; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.		
8	SC-3-5	SECURITY FUNCTION ISOLATION Control Enhancement: The information system security functions are implemented as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	L	M	H			FS/PS/NS
	SC-3-5-1	Determine if the information system security functions are implemented as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.				Examine: System and communications protection policy; procedures addressing security function isolation; information system design documentation; information system configuration settings and associated		

Copyright© 2008
 Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

						documentation; other relevant documents or records.		
9	SC-4	INFORMATION REMNANCE Control: The information system prevents unauthorized and unintended information transfer via shared system resources.	L	M	H			FS/PS/NS
	SC-4.1	Determine if the information system prevents unauthorized and unintended information transfer via shared system resources.				Examine: System and communications protection policy; procedures addressing information remnance; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. (M) (H) Test: Information system for unauthorized and unintended transfer of information via shared system resources. (H)		
10	SC-5	DENIAL OF SERVICE PROTECTION Control: The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined list of types of denial of service attacks or reference to source for current list].	L	M	H			FS/PS/NS

	SC-5.1	Determine if: (i) the organization defines the types of denial of service attacks (or provides references to sources of current denial of service attacks) that can be addressed by the information system; and (ii) the information system protects against or limits the effects of the organization-defined or referenced types of denial of service attacks.			Examine: System and communications protection policy; procedures addressing denial of service protection; information system design documentation; information system security plan; information system configuration settings and associated documentation; other relevant documents or records. (L) (M) (H) Test: Information system for protection against or limitation of the effects of denial of service attacks. (H)		
11	SC-5-1	DENIAL OF SERVICE PROTECTION Control Enhancement: The information system restricts the ability of users to launch denial of service attacks against other information systems or networks.	L	M	H		FS/PS/NS
	SC-5-1-1	Determine if the information system restricts the ability of users to launch denial of service attacks against other information systems or networks.			Examine: System and communications protection policy; procedures addressing denial of service protection; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.		

						Test: Information system for protection against or limitation of the effects of denial of service attacks.		
12	SC-5-2	DENIAL OF SERVICE PROTECTION Control Enhancement: The information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.	L	M	H			FS/PS/NS
	SC-5-2-1	Determine if the information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.				Examine: System and communications protection policy; procedures addressing denial of service protection; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.		
13	SC-6	RESOURCE PRIORITY Control: The information system limits the use of resources by priority.	L	M	H			FS/PS/NS
	SC-6.1	Determine if the information system limits the use of resources by priority.				Examine: System and communications protection policy; procedures addressing prioritization of information system resources; information system design documentation; information system configuration settings and		

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

						associated documentation; other relevant documents or records.		
14	SC-7	BOUNDARY PROTECTION Control: The information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.	L	M	H			FS/PS/NS
	SC-7.1	Determine if: (i) the organization defines key internal boundaries of the information system; and (ii) the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.				<p>Examine: System and communications protection policy; procedures addressing boundary protection; list of key internal boundaries of the information system; information system design documentation; boundary protection hardware and software; information system configuration settings and associated documentation; other relevant documents or records. (L) (M) (H)</p> <p>Interview: Selected organizational personnel with boundary protection responsibilities. (M) (H)</p> <p>Test: Information system monitoring and control of communications at the external boundary of the information system and at key</p>		

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

						internal boundaries within the system; automated mechanisms implementing boundary protection capability within the information system. (H)		
15	SC-7-1	BOUNDARY PROTECTION Control Enhancement: The organization physically allocates publicly accessible information system components to separate subnetworks with separate, physical network interfaces.	L	M	H			FS/PS/NS
	SC-7-1-1	Determine if the organization physically allocates publicly accessible information system components to separate subnetworks with separate, physical network interfaces.				Examine: System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system hardware and software; information system architecture; information system configuration settings and associated documentation; other relevant documents or records. (M) (H)		
16	SC-7-2	BOUNDARY PROTECTION Control Enhancement: The organization prevents public access into the organization's internal networks except as appropriately mediated.	L	M	H			FS/PS/NS

	SC-7-2-1	Determine if: (i) the organization defines the mediation necessary for public access to the organization's internal networks; and (ii) the organization prevents public access into the organization's internal networks except as appropriately mediated.				Examine: System and communications protection policy; procedures addressing boundary protection; list of mediation vehicles for allowing public access to the organization's internal networks; information system design documentation; boundary protection hardware and software; information system configuration settings and associated documentation; other relevant documents or records. (M) (H) Test: Automated mechanisms implementing access controls for public access to the organization's internal networks. (H)	
17	SC-7-3	BOUNDARY PROTECTION Control Enhancement: The organization limits the number of access points to the information system to allow for better monitoring of inbound and outbound network traffic.	L	M	H		FS/PS/NS

	SC-7-3-1	Determine if the organization limits the number of access points to the information system to allow for better monitoring of inbound and outbound network traffic.				Examine: System and communications protection policy; procedures addressing boundary protection; information system design documentation; boundary protection hardware and software; information system architecture and configuration documentation; information system configuration settings and associated documentation; other relevant documents or records. (M) (H)	
18	SC-7-4	BOUNDARY PROTECTION Control Enhancement: The organization implements a managed interface (boundary protection devices in an effective security architecture) with any external telecommunication service, implementing controls appropriate to the required protection of the confidentiality and integrity of the information being transmitted.	L	M	H		FS/PS/NS

	SC-7-4-1	Determine if: (i) the organization defines the security controls (i.e., boundary protection devices and architectural configuration of the devices) appropriate at each external interface to a telecommunication service; and (ii) the organization implements a managed interface with any external telecommunication service, implementing controls appropriate to the required protection of the confidentiality and integrity of the information being transmitted.				Examine: System and communications protection policy; procedures addressing boundary protection; information system security architecture; information system design documentation; boundary protection hardware and software; information system architecture and configuration documentation; information system configuration settings and associated documentation; other relevant documents or records. (M) (H) Interview: Selected organizational personnel with boundary protection responsibilities. (H)	
19	SC-7-5	BOUNDARY PROTECTION Control Enhancement: The information system denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).	L	M	H		FS/PS/NS

	SC-7-5-1	Determine if the information system denies network traffic by default and allows network traffic by exception.				Examine: System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. (M) (H) Interview: Selected organizational personnel with boundary protection responsibilities. (H)	
20	SC-7-6	BOUNDARY PROTECTION Control Enhancement: The organization prevents the unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms.	L	M	H		FS/PS/NS

	SC-7-6-1	Determine if the organization prevents the unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms.				Examine: System and communications protection policy; procedures addressing boundary protection; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records. (H) Test: Automated mechanisms supporting the fail-safe boundary protection capability within the information system. (H)	
21	SC-8	TRANSMISSION INTEGRITY Control: The information system protects the integrity of transmitted information.	L	M	H		FS/PS/NS
	SC-8.1	Determine if the information system protects the integrity of transmitted information.				Examine: System and communications protection policy; procedures addressing transmission integrity; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. (M) (H) Test: Transmission integrity	

						capability within the information system. (H)		
22	SC-8-1	TRANSMISSION INTEGRITY Control Enhancement: The organization employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.	L	M	H			FS/PS/NS
	SC-8-1-1	Determine if the information system employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures				Examine: System and communications protection policy; procedures addressing transmission integrity; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. (H) Test: Cryptographic mechanisms implementing transmission integrity capability within the information system. (H)		
23	SC-9	TRANSMISSION CONFIDENTIALITY Control: The information system protects the confidentiality of transmitted information.	L	M	H			FS/PS/NS

	SC-9.1	Determine if the information system protects the confidentiality of transmitted information.				Examine: system and communications protection policy; procedures addressing transmission confidentiality; information system design documentation; contracts for telecommunications services; information system configuration settings and associated documentation; other relevant documents or records. (M) (H) Test: Transmission confidentiality capability within the information system. (H)		
24	SC-9-1	TRANSMISSION CONFIDENTIALITY Control Enhancement: The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures.	L	M	H			FS/PS/NS
	SC-9-1-1	Determine if the information system employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measure.				Examine: System and communications protection policy; procedures addressing transmission confidentiality; information system design documentation; information system communications hardware and software or Protected Distribution System protection mechanisms;		

						information system configuration settings and associated documentation; other relevant documents or records. (H)		
						Test: Cryptographic mechanisms implementing transmission confidentiality capability within the information system. (H)		
25	SC-10	NETWORK DISCONNECT Control: The information system terminates a network connection at the end of a session or after [Assignment: organization-defined time period] of inactivity.	L	M	H			FS/PS/NS
	SC-10.1	Determine if: (i) the organization defines the time period of inactivity before the information system terminates a network connection; and (ii) the information system terminates a network connection at the end of a session or after the organization-defined time period of inactivity.				Examine: System and communications protection policy; procedures addressing network disconnect; information system design documentation; organization-defined time period of inactivity before network disconnect; information system configuration settings and associated documentation; other relevant documents or records. (M) (H) Test: Network disconnect capability within the information system. (M) (H)		

26	SC-11	TRUSTED PATH Control: The information system establishes a trusted communications path between the user and the following security functions of the system: [Assignment: organization-defined security functions to include at a minimum, information system authentication and reauthentication].	L	M	H			FS/PS/NS
	SC-11.1	Determine if: (i) the organization defines the security functions within the information system that are included in a trusted communications path; (ii)the organization-defined security functions include information system authentication and reauthentication; and (iii) the information system establishes a trusted communications path between the user and the organization-defined security functions within the information system				Examine: System and communications protection policy; procedures addressing trusted communications paths; information system security plan; information system design documentation; information system configuration settings and associated documentation; assessment results from independent, testing organizations; other relevant documents or records. Test: [SELECT FROM: Automated mechanisms implementing trusted communications paths within the information system].		

27	SC-12	<p>CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT</p> <p>Control: When cryptography is required and employed within the information system, the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures.</p>	L M H			FS/PS/NS
	SC-12.1	<p>Determine if the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures, when cryptography is required and employed within the information system.</p>		<p>Examine: System and communications protection policy; procedures addressing cryptographic key management and establishment; NIST Special Publications 800-56 and 800-57; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. (M) (H)</p> <p>Interview: Organizational personnel with responsibilities for cryptographic key establishment or management. (H)</p> <p>Test: Automated mechanisms implementing cryptographic key management and establishment within the</p>		

Copyright© 2008
 Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

						information system. (H)		
28	SC-13	USE OF CRYPTOGRAPHY Control: For information requiring cryptographic protection, the information system implements cryptographic mechanisms that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.	L	M	H			FS/PS/NS
	SC-13.1	Determine if, for information requiring cryptographic protection, the information system implements cryptographic mechanisms that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.				Examine: System and communications protection policy; procedures addressing use of cryptography; FIPS 140-2 (as amended); NIST Special Publications 800-56 and 800-57; information system design documentation; information system configuration settings and associated documentation; cryptographic module validation certificates; other relevant documents or records. (L) (M) (H)		
29	SC-14	PUBLIC ACCESS PROTECTIONS Control: The information system protects the integrity and availability of publicly available information and applications.	L	M	H			FS/PS/NS

	SC-14.1	Determine if the information system protects the integrity and availability of publicly available information and applications.				Examine: System and communications protection policy; procedures addressing public access protections; access control policy and procedures; boundary protection procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. (L) (M) (H) Test: Automated mechanisms implementing access controls and boundary protection for publicly available information and applications within the information system. (H)	
30	SC-15	COLLABORATIVE COMPUTING Control: The information system prohibits remote activation of collaborative computing mechanisms and provides an explicit indication of use to the local users.	L	M	H		FS/PS/NS

	SC-15.1	Determine if the information system prohibits remote activation of collaborative computing mechanisms and provides an explicit indication of use to the local users.				Examine: System and communications protection policy; procedures addressing collaborative computing; access control policy and procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. (M) (H) Test: Automated mechanisms implementing access controls for collaborative computing environments; alert notification for local users. (H)	
31	SC-15-1	COLLABORATIVE COMPUTING Control Enhancement: The information system provides physical disconnect of camera and microphone in a manner that supports ease of use.	L	M	H		FS/PS/NS
	SC-15-1-1	Determine if the information system provides physical disconnect of camera and microphone in a manner that supports ease of use.				Examine: System and communications protection policy; procedures addressing collaborative computing; access control policy and procedures; information system design documentation; information system configuration settings and associated documentation;	

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

						other relevant documents or records. Test: Physical disconnect of collaborative computing devices.	
32	SC-16	TRANSMISSION OF SECURITY PARAMETERS Control: The information system reliably associates security parameters with information exchanged between information systems.	L	M	H		FS/PS/NS
	SC-16.1	Determine if the information system reliably associates security parameters with information exchanged between information systems.				Examine: System and communications protection policy; procedures addressing transmission of security parameters; access control policy and procedures; boundary protection procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. Test: Automated mechanisms supporting reliable transmission of security	

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

						parameters between information systems.		
33	SC-17	PUBLIC KEY INFRASTRUCTURE CERTIFICATES Control: The organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.	L	M	H			FS/PS/NS
	SC-17.1	Determine if the organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.				Examine: System and communications protection policy; procedures addressing public key infrastructure certificates; public key certificate policy or policies; public key issuing process; NIST Special Publication 800-32; other relevant documents or records. (M) (H) Interview: Organizational personnel with public key infrastructure certificate issuing responsibilities. (H)		

34	SC-18	<p>MOBILE CODE</p> <p>Control: The organization: (i) establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously; and (ii) authorizes, monitors, and controls the use of mobile code within the information system.</p>	L M H			FS/PS/NS
	SC-18.1	<p>Determine if:</p> <p>(i) the organization establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously; and</p> <p>(ii) the organization authorizes, monitors, and controls the use of mobile code within the information system.</p>		<p>Examine: System and communications protection policy; procedures addressing mobile code; mobile code usage restrictions, mobile code implementation guidance; NIST Special Publication 800-28; other relevant documents or records. (M) (H)</p> <p>Interview: Organizational personnel with mobile code authorization, monitoring, and control responsibilities. (H)</p> <p>Test: Mobile code authorization and monitoring capability for the organization. (H)</p>		

35	SC-19	<p>VOICE OVER INTERNET PROTOCOL</p> <p>Control: The organization: (i) establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and (ii) authorizes, monitors, and controls the use of VoIP within the information system.</p>	L M H			FS/PS/NS
	SC-19.1	<p>Determine if:</p> <p>(i) the organization establishes usage restrictions and implementation guidance for Voice over Internet Protocol technologies based on the potential to cause damage to the information system if used maliciously; and</p> <p>(ii) the organization authorizes, monitors, and controls the use of VoIP within the information system.</p>		<p>Examine: System and communications protection policy; procedures addressing VoIP; NIST Special Publication 800-58; VoIP usage restrictions; other relevant documents or records. (M) (H)</p> <p>Interview: Organizational personnel with VoIP authorization and monitoring responsibilities. (H)</p>		
36	SC-20	<p>SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)</p> <p>Control: The information system that provides name/address resolution service provides additional data origin and integrity artifacts along with the authoritative data it returns in response to resolution queries.</p>	L M H			FS/PS/NS

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

	SC-20.1	Determine if the information system that provides the name/address lookup service for accessing organizational information resources to entities across the Internet provides artifacts for additional data origin authentication and data integrity artifacts along with the authoritative data it returns in response to resolution queries.				Examine: System and communications protection policy; procedures addressing secure name/address resolution service (authoritative source); NIST Special Publication 800-81; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. (M) (H) Test: Automated mechanisms implementing secure name/address resolution service (authoritative source) within the information system. (H)	
37	SC-20-1	SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) Control Enhancement: The information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains.	L	M	H		FS/PS/NS

	SC-20-1-1	Determine if the information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains.		Examine: System and communications protection policy; procedures addressing secure name/address resolution service (authoritative source); information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. Test: Automated mechanisms implementing child subspace security status indicators and chain of trust verification for resolution services within the information system.		
	SC-20-1-1	Determine if the information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains.		Examine: System and communications protection policy; procedures addressing secure name/address resolution service (authoritative source); information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. Test: Automated mechanisms implementing child subspace		

						security status indicators and chain of trust verification for resolution services within the information system.		
38	SC-21	SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER) Control: The information system that provides name/address resolution service for local clients performs data origin authentication and data integrity verification on the resolution responses it receives from authoritative sources when requested by client systems.	L	M	H			FS/PS/NS
	SC-21.1	Determine if the information system that provides name/address resolution service for local clients performs data origin authentication and data integrity verification on the resolution responses it receives from authoritative sources when requested by client systems.				Examine: System and communications protection policy; procedures addressing secure name/address resolution service (recursive or caching resolver); information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. (H) Test: Automated mechanisms implementing data origin authentication and integrity verification for resolution services within the information system. (H)		

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

39	SC-21-1	<p>SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)</p> <p>Control Enhancement: The information system performs data origin authentication and data integrity verification on all resolution responses whether or not local clients explicitly request this service.</p>	L M H			FS/PS/NS
	SC-21-1-1	<p>Determine if the information system performs data origin authentication and data integrity verification on all resolution response received whether or not client systems explicitly request this service.</p>		<p>Examine: system and communications protection policy; procedures addressing secure name/address resolution service (recursive or caching resolver); NIST Special Publication 800-81; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.</p>		
40	SC-22	<p>ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE</p> <p>Control: The information systems that collectively provide name/address resolution service for an organization are fault tolerant and implement role separation.</p>	L M H			FS/PS/NS

	SC-22.1	Determine if the information systems that collectively provide name/address resolution service for an organization are fault tolerant and implement role separation.				Examine: System and communications protection policy; procedures addressing architecture and provisioning for name/address resolution service; access control policy and procedures; NIST Special Publication 800-81; information system design documentation; assessment results from independent, testing organizations; information system configuration settings and associated documentation; other relevant documents or records. (M) (H) Test: Automated mechanisms supporting name/address resolution service for fault tolerance and role separation. (H)	
41	SC-23	SESSION AUTHENTICITY Control: The information system provides mechanisms to protect the authenticity of communications sessions.	L	M	H		FS/PS/NS

SC-23.1	Determine if the information system provides mechanisms to protect the authenticity of communications sessions.			Examine: System and communications protection policy; procedures addressing session authenticity; NIST Special Publications 800-52, 800-77, and 800-95; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. (M) (H) Test: Automated mechanisms implementing session authenticity. (H)	
FS - Fully Satisfied PS - Partially Satisfied NS - Not Satisfied Impacts: Low Medium High Assessment Methods: Interview					Assessment Results
					FS 0
					PS 0
					NS 0
					Total 0

SYSTEM & INFORMATION INTEGRITY

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

A-274

Page 1573 of 1794

FAMILY: SYSTEM & INFORMATION INTEGRITY			Impact			Assessment Method			Assessment Results	FS/PS/NS
Num	ID	Assessment Procedure	L	M	H					
1	SI-1	<p>SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES</p> <p>Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.</p>	L	M	H					FS/PS/NS
	SI-1.1	<p>Determine if:</p> <p>(i) the organization develops and documents system and information integrity policy and procedures; (ii) the organization disseminates system and information integrity policy and procedures to appropriate elements within the organization; (iii) responsible parties within the organization periodically review system and information integrity policy and procedures; and (iv) the organization updates system and information integrity policy and procedures when organizational review indicates updates are required.</p>				<p>Examine: System and information integrity policy and procedures; other relevant documents or records. (L) (M) (H)</p> <p>Interview: Organizational personnel with system and information integrity responsibilities. (H)</p>				

Copyright© 2008
 Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

	SI-1.2	Determine if: (i) the system and information integrity policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance; (ii) the system and information integrity policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and (iii) the system and information integrity procedures address all areas identified in the system and information integrity policy and address achieving policy-compliant implementations of all associated security controls.					Examine: System and information integrity policy and procedures; other relevant documents or records. (L) (M) (H) Interview: Organizational personnel with system and information integrity responsibilities. (H)		
2	SI-2	FLAW REMEDIATION Control: The organization identifies, reports, and corrects information system flaws.	L	M	H				FS/PS/NS

	SI-2.1	Determine if: (i) the organization identifies, reports, and corrects information system flaws; (ii) the organization installs newly released security patches, service packs, and hot fixes on the information system in a reasonable timeframe in accordance with organizational policy and procedures; (iii) the organization addresses flaws discovered during security assessments, continuous monitoring, or incident response activities in an expeditious manner in accordance with organizational policy and procedures; (iv) the organization tests information system patches, service packs, and hot fixes for effectiveness and potential side effects before installation; and (v) the organization captures all appropriate information pertaining to the discovered flaws in the information system, including the cause of the flaws, mitigation activities, and lessons learned.		Examine: System and information integrity policy; procedures addressing flaw remediation; NIST Special Publication 800-40; list of flaws and vulnerabilities potentially affecting the information system; list of recent security flaw remediation actions performed on the information system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct information system flaws); test results from the installation of software to correct information system flaws; other relevant documents or records. (L) (M) (H)		
3	SI-2-1	FLAW REMEDIATION Control Enhancement: The organization centrally manages the flaw remediation process and installs updates automatically.			Interview: Organizational personnel with flaw remediation responsibilities. (M) (H)	FS/PS/NS

	SI-2-1-1	Determine if the organization centrally manages the flaw remediation process and installs updates automatically.			Examine: System and information integrity policy; procedures addressing flaw remediation; automated mechanisms supporting centralized management of flaw remediation and automatic software updates; information system design documentation; information system configuration settings and associated documentation; list of information system flaws; list of recent security flaw remediation actions performed on the information system; other relevant documents or records. (H) Test: Automated mechanisms supporting centralized management of flaw remediation and automatic software updates. (H)		
4	SI-2-2	FLAW REMEDIATION Control Enhancement: The organization employs automated mechanisms to periodically and upon demand determine the state of information system components with regard to flaw remediation.					FS/PS/NS

	SI-2-2-1	Determine if the organization employs automated mechanisms to periodically and upon demand determine the state of information system components with regard to flaw remediation.			Examine: System and information integrity policy; procedures addressing flaw remediation; automated mechanisms supporting flaw remediation; information system design documentation; information system configuration settings and associated documentation; list of information system flaws; list of recent security flaw remediation actions performed on the information system; information system audit records; other relevant documents or records. (M) (H) Test: Automated mechanisms implementing information system flaw remediation update status. (M) (H)	
5	SI-3	MALICIOUS CODE PROTECTION Control: The information system implements malicious code protection.				FS/PS/NS

		Determine if: (i) the information system implements malicious code protection; (ii) the organization employs malicious code protection mechanisms at critical information system entry and exit points, at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code; (iii) the malicious code protection mechanisms detect and eradicate malicious code transported by electronic mail, electronic mail attachments, Internet access, removable media, or other common means, or by exploiting information system vulnerabilities; (iv) the organization updates malicious code protection mechanisms whenever new releases are available; and (v) the malicious code protection mechanisms are appropriately updated to include the latest malicious code definitions, configured to perform periodic scans of the information system as well as real-time scans of files from external sources as the files are downloaded, opened, or executed, and configured to disinfect and quarantine infected files.			Examine: System and information integrity policy; procedures addressing malicious code protection; NIST Special Publication 800-83; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records. (L) (M) (H)	
6	SI-3-1	MALICIOUS CODE PROTECTION Control Enhancement: The organization centrally manages malicious code protection mechanisms.				FS/PS/NS

	SI-3-1-1	Determine if the organization centrally manages malicious code protection mechanisms.			Examine: System and information integrity policy; procedures addressing malicious code protection; information system design documentation; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records. (M) (H)		
7	SI-3-2	MALICIOUS CODE PROTECTION Control Enhancement: The information system automatically updates malicious code protection mechanisms.					FS/PS/NS
	SI-3-2-1	Determine if the organization automatically updates malicious code protection mechanisms.			Examine: System and information integrity policy; procedures addressing malicious code protection; information system design documentation; malicious code protection mechanisms; records of malicious code protection updates; information system configuration settings and associated documentation; other relevant documents or records. (M) (H)		

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

					Test: Automatic update capability for malicious code protection. (M) (H)		
8	SI-4	INFORMATION SYSTEM MONITORING TOOLS AND TECHNIQUES Control: The organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system.					FS/PS/NS
	SI-4.1	Determine if the organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system.			Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; other relevant documents or records. (M) (H)		
9	SI-4-1	INFORMATION SYSTEM MONITORING TOOLS AND TECHNIQUES Control Enhancement: The organization interconnects and configures individual intrusion detection tools into a system wide intrusion detection system using common protocols.					FS/PS/NS

	SI-4-1-1	Determine if the organization interconnects and configures individual intrusion detection tools into a system wide intrusion detection system using common protocols.			Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols; other relevant documents or records. Test: Information system-wide intrusion detection capability.		
10	SI-4-2	INFORMATION SYSTEM MONITORING TOOLS AND TECHNIQUES Control Enhancement: The organization employs automated tools to support near-real-time analysis of events.					FS/PS/NS

	SI-4-2-1	Determine if the organization employs automated tools to support near-real-time analysis of events.				Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols documentation; other relevant documents or records. (H) Test: Automated tools supporting near real-time event analysis. (H)		
11	SI-4-3	INFORMATION SYSTEM MONITORING TOOLS AND TECHNIQUES Control Enhancement: The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.	L	M	H			FS/PS/NS

	SI-4-3-1	Determine if the organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.				Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols; other relevant documents or records. Test: Automated tools supporting the integration of intrusion detection tools and access/flow control mechanisms.	
12	SI-4-4	INFORMATION SYSTEM MONITORING TOOLS AND TECHNIQUES Control Enhancement: The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.	L	M	H		FS/PS/NS

	SI-4-4-1	Determine if: (i) the organization identifies the types of activities or conditions considered unusual or unauthorized; and (ii) the information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.				Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; types of activities or conditions considered unusual or unauthorized; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; other relevant documents or records. (M) (H) Test: Information system monitoring capability for inbound and outbound communications. (M) (H)	
13	SI-4-5	INFORMATION SYSTEM MONITORING TOOLS AND TECHNIQUES Control Enhancement: The information system provides a real-time alert when the following indications of compromise or potential compromise occur: [Assignment: organization-defined list of compromise indicators].	L	M	H		FS/PS/NS

	SI-4-5-1	Determine if: (i) the organization identifies indications of compromise or potential compromise to the security of the information system; and (ii) the information system provides a real-time alert when any of the organization-defined list of compromise, or potential compromise indicators occur.			Examine: System and information integrity policy; procedures addressing information system monitoring tools and techniques; information system security plan; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; other relevant documents or records. (H) Test: Information system monitoring real-time alert capability. (H)		
14	SI-5	SECURITY ALERTS AND ADVISORIES Control: The organization receives information system security alerts/advisories on a regular basis, issues alerts/advisories to appropriate personnel, and takes appropriate actions in response.	L	M	H		FS/PS/NS

	SI-5.1	Determine if: (i) the organization receives information system security alerts/advisories on a regular basis; (ii) the organization issues security alerts/advisories to appropriate organizational personnel; and (iii) the organization takes appropriate actions in response to security alerts/advisories.			Examine: System and information integrity policy; procedures addressing security alerts and advisories; NIST Special Publication 800-40; records of security alerts and advisories; other relevant documents or records. (L) (M) (H)		
15	SI-5.1	SECURITY ALERTS AND ADVISORIES Control Enhancement: The organization employs automated mechanisms to make security alert and advisory information available throughout the organization as needed.	L	M	H	Interview: Organizational personnel with security alert and advisory responsibilities; organizational personnel implementing, operating, maintaining, administering, and using the information system. (M) (H)	FS/PS/NS

	SI-5-1-1	Determine if the organization employs automated mechanisms to make security alert and advisory information available throughout the organization as needed.			Examine: System and information integrity policy; procedures addressing security alerts and advisories; information system design documentation; information system configuration settings and associated documentation; automated mechanisms supporting the distribution of security alert and advisory information; records of security alerts and advisories; other relevant documents or records. (H) Test: Automated mechanisms implementing the distribution of security alert and advisory information. (H)		
16	SI-6	<p>SECURITY FUNCTIONALITY VERIFICATION</p> <p>Control: The information system verifies the correct operation of security functions</p> <p>[Selection (one or more): upon system startup and restart, upon command by user with appropriate privilege, periodically every [Assignment: organization-defined time-period]] and [Selection (one or more): notifies system administrator, shuts the system down,</p>	L	M	H		FS/PS/NS

		restarts the system] when anomalies are discovered.					
	SI-6.1	Determine if: (i) the organization defines the appropriate conditions for conducting security function verification; (ii) the organization defines, for periodic security function verification, the frequency of the verifications; (iii) the organization defines information system responses to anomalies discovered during security function verification; (iv) the information system verifies the correct operation of security functions in accordance with organization-defined conditions and in accordance with organization-defined frequency (if periodic verification); and (v) the information system responds to security function anomalies in accordance with organization-defined responses.				Examine: System and information integrity policy; procedures addressing security function verification; information system design documentation; information system security plan; information system configuration settings and associated documentation; other relevant documents or records. (H) Test: Security function verification capability. (H)	
17	SI-6-1	SECURITY FUNCTIONALITY VERIFICATION Control Enhancement: The organization employs automated mechanisms to provide notification of failed automated security tests.	L	M	H		FS/PS/NS

	SI-6-1-1	Determine if the organization employs automated mechanisms to provide notification of failed security tests.				Examine: System and information integrity policy; procedures addressing security function verification; information system design documentation; information system security plan; information system configuration settings and associated documentation; other relevant documents or records. Test: Automated mechanisms implementing alerts and/or notifications for failed automated security tests.		
18	SI-6-2	SECURITY FUNCTIONALITY VERIFICATION Control Enhancement: The organization employs automated mechanisms to support management of distributed security testing.	L	M	H			FS/PS/NS

	SI-6-2-1	Determine if the organization employs automated mechanisms to support management of distributed security testing.				Examine: System and information integrity policy; procedures addressing security function verification; information system design documentation; information system security plan; information system configuration settings and associated documentation; other relevant documents or records. Test: Automated mechanisms supporting the management of distributed security function testing.		
19	SI-7	SOFTWARE AND INFORMATION INTEGRITY Control: The information system detects and protects against unauthorized changes to software and information.	L	M	H			FS/PS/NS
	SI-7.1	Determine if: (i) the information system detects and protects against unauthorized changes to software and information; and (ii) the organization employs effective integrity verification tools in accordance with good software engineering practices.				Examine: System and information integrity policy; procedures addressing software and information integrity; information system design documentation; information system configuration settings and associated documentation; integrity verification tools and applications documentation; other relevant documents or		

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

						records. (H) Test: Software integrity protection and verification capability. (H)		
20	SI-7-1	SOFTWARE AND INFORMATION INTEGRITY Control Enhancement: The organization reassesses the integrity of software and information by performing [Assignment: organization-defined frequency] integrity scans of the system.	L	M	H			FS/PS/NS
	SI-7-1-1	Determine if: (i) the organization defines the frequency of integrity scans on the information system; and (ii) the organization reassesses the integrity of software and information by performing integrity scans of the information system in accordance with the organization-defined frequency.				Examine: System and information integrity policy; procedures addressing software and information integrity; information system security plan; information system configuration settings and associated documentation; integrity verification tools and applications documentation; records of integrity scans; other relevant documents or records. (H)		
21	SI-7-2	SOFTWARE AND INFORMATION INTEGRITY Control Enhancement: The organization employs automated tools that provide notification to appropriate individuals upon discovering discrepancies during integrity verification.	L	M	H			FS/PS/NS

	SI-7-2-1	Determine if the organization employs automated tools that provide notification to appropriate individuals upon discovering discrepancies during integrity verification.			Examine: System and information integrity policy; procedures addressing software and information integrity; information system configuration settings and associated documentation; integrity verification tools and applications documentation; records of integrity scans; automated tools supporting alerts and notifications for integrity discrepancies; other relevant documents or records. (H)		
22	SI-7-3	SOFTWARE AND INFORMATION INTEGRITY Control Enhancement: The organization employs centrally managed integrity verification tools.	L	M	H		FS/PS/NS
	SI-7-3-1	Determine if the organization employs centrally managed integrity verification tools.			Examine: System and information integrity policy; procedures addressing software and information integrity; information system configuration settings and associated documentation; integrity verification tools and applications documentation; records of integrity scans; other relevant documents or records.		

23	SI-8	SPAM PROTECTION Control: The information system implements spam protection.	L	M	H			FS/PS/NS
	SI-8.1	Determine if: (i) the information system implements spam protection; (ii) the organization employs spam protection mechanisms at critical information system entry points and at workstations, servers, or mobile computing devices on the network; (iii) the organization employs spam protection mechanisms to detect and take appropriate action on unsolicited messages transported by electronic mail; and (iv) the organization updates spam protection mechanisms whenever new releases are available in accordance with organizational policy and procedures.				Examine: System and information integrity policy; procedures addressing spam protection; information system design documentation; spam protection mechanisms; information system configuration settings and associated documentation; other relevant documents or records. (M) (H) Test: Spam detection and handling capability. (M) (H)		
24	SI-8-1	SPAM PROTECTION Control Enhancement: The organization centrally manages spam protection mechanisms.	L	M	H			FS/PS/NS
	SI-8-1-1	Determine if the organization centrally manages spam protection mechanisms.				Examine: System and information integrity policy; procedures addressing spam protection; information system design documentation; spam protection mechanisms; information system		

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

						configuration settings and associated documentation; other relevant documents or records. (H)		
25	SI-8-2	SPAM PROTECTION Control Enhancement: The information system automatically updates spam protection mechanisms.	L	M	H			FS/PS/NS
	SI-8-2-1	Determine if the information system automatically updates spam protection mechanisms.				<p>Examine: System and information integrity policy; procedures addressing spam protection; information system design documentation; spam protection mechanisms; information system configuration settings and associated documentation; other relevant documents or records.</p> <p>Test: Automatic update capability for spam protection.</p>		
26	SI-9	INFORMATION INPUT RESTRICTIONS Control: The organization restricts the capability to input information to the information system to authorized personnel.	L	M	H			FS/PS/NS

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

	SI-9.1	Determine if the organization restricts the capability to input information to the information system to authorized personnel.			Examine: System and information integrity policy; procedures addressing information input restrictions; access control policy and procedures; separation of duties policy and procedures; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. (M) (H)		
27	SI-10	INFORMATION ACCURACY, COMPLETENESS, VALIDITY, AND AUTHENTICITY Control: The information system checks information for accuracy, completeness, validity, and authenticity.	L	M	H		FS/PS/NS

	SI-10.1	Determine if: (i) the information system checks information for accuracy, completeness, validity, and authenticity; (ii) checks for accuracy, completeness, validity, and authenticity of information is accomplished as close to the point of origin as possible; (iii) the information system employs rules to check the valid syntax of information inputs to verify that inputs match specified definitions for format and content; and (iv) the information system prescreens information inputs passed to interpreters to prevent the content from being unintentionally interpreted as commands.				Examine: System and information integrity policy; procedures addressing information accuracy, completeness, validity, and authenticity; access control policy and procedures; separation of duties policy and procedures; documentation for automated tools and applications to verify accuracy, completeness, validity, and authenticity of information; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. (M) (H)	
28	SI-11	ERROR HANDLING Control: The information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries.	L	M	H		FS/PS/NS

	SI-11.1	Determine if: (i) the information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries; (ii) the information system reveals only essential information to authorized individuals; and (iii) the information system does not include sensitive information in error logs or associated administrative messages.			Examine: System and information integrity policy; procedures addressing information system error handling; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records. (M) (H) Test: Information system error handling capability. (H)		
29	SI-12	INFORMATION OUTPUT HANDLING AND RETENTION Control: The organization handles and retains output from the information system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	L	M	H		FS/PS/NS
	SI-12.1	Determine if: (i) the organization handles and retains output from the information system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and operational requirements; and (ii) the organization handles output from the information system in accordance with labeled or marked instructions on information system output (including paper and digital media) that includes, but not limited to,			Examine: System and information integrity policy; procedures addressing information system output handling and retention; media protection policy and procedures; information retention records, other relevant documents or records. (M) (H) Interview: Organizational		

	special instructions for dissemination, distribution, transport, or storage of information system output.			personnel with information output handling and retention responsibilities. (H)	
FS - Fully Satisfied					Assessment Results
PS - Partially Satisfied					
NS - Not Satisfied					
Impacts: Low Medium High					
Assessment Methods: Interview	Demonstrate	Test	Observe		
				FS	0
				PS	0
				NS	0
				Total	0

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

A-300



The Federation for Identity and
Cross-Credentialing Systems®

Appendix B

FiXS PIV Security Controls Checklist

NIST 800-79-1 Compliance

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXS®)

The FiXs PIV Security Controls Checklist contains requirements from NIST 800-79-1. Applicants are assessed based on these requirements.

The checklist is separated into worksheet sections based on the NIST 800-79-1 category. The checklist has been mapped to three FiXs testing documents: FiXs Operating Rules Compliance Checklist, FiXs Operating Rules, Addendum, and the FiXs Implementation Guidelines Checklist. Where a FiXs requirement did not map to NIST 800-79-1 it was added as a new requirement at the bottom of the most relevant section.

FiXs and NIST have different naming conventions for their personnel titles. Where roles overlapped it is noted in red italics in the Compliance Checklist.

Each requirement has a suggested testing methodology, which is either to conduct an interview, perform document review, run a test on a system, or observe. In some cases more than one methodology is recommended. On the far right of each row that contains a requirement is a column which holds the results of each assessment. The result is Fully Satisfied, Partially Satisfied, or Not Satisfied. These results are tabulated at the bottom of each section.

CHANGE CONTROL RECORD SHEET

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

Control Family	Control ID	Original Content	Revised Content
NA	NA	PIV - Personal Identity Verification Controls Checklist	Federation for Identity and Cross-Credentialing Systems (FiXs) - FiXs Certified Credential Controls Checklist
NA	NA	NIST 800-79-1	FiXs Crossmap Certification Requirements to NIST 800-79-1
NA	NA	PIV (All instances of PIV)	FiXs Certified Credential
NA	NA	PCI (All instances of PCI)	Credential Issuer
NA	NA	PCIF (All instances of PCIF)	Credential Issuer Facility
PR	1	The organization has developed and posted at the Credential Issuer Facility in multiple locations (e.g., internet site, human resource offices, regional offices, provide at contractor orientation, etc.) privacy act statement/notice or FiXs provided equivalent, complaint procedures, appeals procedures for those denied identification or whose identification cards are revoked, and implements sanctions for employees violating privacy policies. The Credential Issuer collects, stores, processes and controls access and disclosure of personally identifiable information in accordance with applicable Corporate Policy and is in compliance with applicable: national, state, local and foreign laws, FiXs rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information (interview, observe).	The organization has developed and posted at the Credential Issuer Facility in multiple locations (e.g., internet site, human resource offices, regional offices, provide at contractor orientation, etc.) privacy act statement/notice or FiXs provided equivalent , complaint procedures, appeals procedures for those denied identification or whose identification cards are revoked, and implements sanctions for employees violating privacy policies. The Credential Issuer collects, stores, processes and controls access and disclosure of personally identifiable information in accordance with applicable Corporate Policy and is in compliance with applicable: national, state, local and foreign laws, FiXs rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information (interview, observe).

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

PR	1	(i) the Credential Issuer Facility has posted privacy act statement/notice, complaint procedures, appeals procedures for those denied identification or whose identification cards are revoked, and sanctions for employees violating privacy policies (interview, observe).	(i) the Credential Issuer Facility has developed and posted at the Credential Issuer Facility in multiple locations (e.g., internet site, human resource offices, regional offices, provide at contractor orientation, etc.) privacy act statement/notice or FiXs provided equivalent , complaint procedures, appeals procedures for those denied identification or whose identification cards are revoked, and sanctions for employees violating privacy policies. (interview, observe).
PR	2	The organization has conducted a Privacy Impact Assessment of their Credential Issuer information system (s), constituent with Section 208 of the E-Government Act of 2002 and at a minimum, addresses guidance found in Appendix E of OMB Memorandum 06-06.	The organization has conducted a Privacy Impact Assessment of their Credential Issuer information system (s), constituent with FiXs Rules , Guidance and applicable sections of: Section 208 of the E-Government Act of 2002, addresses guidance found in Appendix E of OMB Memorandum 06-06.
PR	2	(i) the organization has conducted a Privacy Impact Assessment of their Credential Issuer information system (s) which addresses guidance found in Appendix E of OMB Memorandum 06-06 (review);	(i) the organization has conducted a Privacy Impact Assessment of their Credential Issuer information system (s) which addresses Corporate Policy, FiXs guidance and/or incorporated Appendix E of OMB Memorandum 06-06 (review);
PR	2	(ii) the organization has submitted the Privacy Impact Assessment of their Credential Issuer information system (s) to OMB (interview).	(ii) the organization has submitted the Privacy Impact Assessment of their Credential Issuer information system (s) to FiXs Executive Board (interview).
PR	3	The organization's employee and contractor identification systems of records notices (SORN's) are updated to reflect any changes in the disclosure of information to other organizations consistent with the Privacy Act of 1974 and OMB Circular A-130, Appendix 1.	The organization's FiXs Certification Package are updated to reflect any changes in the disclosure of information to other organizations consistent with FiXs Guidance and applicable sections of the Privacy Act of 1974 and OMB Circular A-130, Appendix 1. If a SORN is required it has been updated with OMB and FiXs.
PR	3	(i) the organization updates SORN to reflect changes in the disclosure of information (review, interview).	(i) the organization updates FiXs Certification Package to reflect changes in the disclosure of information policy. If a SORN is required it has been updated with OMB and FiXs. (review, interview).

DP	1	In order to be compliant with the provisions of OMB Circular A-130, App III the Credential Issuer information system(s) are certified in accordance with NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems.	In order to be compliant with the provisions of FiXs to DMDC MOA, (and if applicable: OMB Circular A-130, App III), the Credential Issuer information system(s) are certified in accordance with NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems.
DP	2	Every product utilized by a Credential Issuer facility that it falls within one of the categories listed by the GSA FIPS 201 Evaluation program, shall be listed in the GSA FIPS 201 Evaluation Program's Approved Product List (APL)	Every product utilized by a Credential Issuer facility that it falls within one of the categories listed by the FiXs Evaluation program, shall be listed in the FiXs Approved Product List (APL)
DP	2	(i) for each product that falls within one of the categories listed within the APL, its make, model and version is compared against the APL (observe)	(i) for each product that falls within one of the categories listed within the APL, its make, model and version is compared against the APL (observe); Obtain an Inventory list of approved deployed Items {FiXs ADD-ON Rqmt}
DP	3	The organization has submitted a personalized FiXs Certified Credential Card from their production system to GSA for testing, and it has been approved.	The organization has submitted a personalized FiXs Certified Credential Card from their production system to FiXs (and GSA if applicable) for testing, and it has been approved.
DP	3	(i) the organization has a letter from the GSA showing their approval of the card (review).	(i) the organization has a letter from FiXs (and if applicable GSA) showing their approval of the card (review).
SN	2	The Credential Issuer Facility collects personal information using only forms approved by OMB under the Paperwork Reduction Act of 1995.	The Credential Issuer Facility collects personal information using only forms approved by FiXs (and if applicable OMB under the Paperwork Reduction Act of 1995.)
SN	2	(i) forms used to collect personal information have been approved by OMB (review, observe).	(i) forms used to collect personal information have been approved by FiXs (and if applicable OMB) (review, observe).
EI	2	(None)	(iii) current proof of citizenship must be checked

EI	3	Two identity source documents are checked in accordance with the requirements of Form I-9, OMB No. 1115-0136, Employment Eligibility Verification.	Two identity source documents are checked in accordance with the requirements of Form I-9 (one of which must be a photo ID), OMB No. 1115-0136, Employment Eligibility Verification. (FiXs requirement: Applicant must present 2 forms of Government issued ID Per US Form I-9 or 6 CFR Part 37 , one of which must have a photo.)
EI	3	(i) the requirement to check two identity source documents in accordance with the requirements of Form I-9 is documented (review);	(i) the requirement to check two identity source documents in accordance with the requirements of Form I-9 is documented (FiXs requirement: Applicant must present 2 forms of Government issued ID Per US Form I-9 or 6 CFR Part 37 , one of which must have a photo.) (review);
EI	New a	In a single session, the Facility Enroller [Operator] must completely and successfully capture and store an applicant's digitized photograph, fingerprint biometrics, and name identification and demographic data. All data must be correctly entered during the single session.	In a single session, the Facility Enroller [Operator] must completely and successfully capture and store an applicant's digitized photograph, fingerprint biometrics, and name identification and demographic data. All data must be correctly entered during the single session. All documents should be scanned.
EI	NEW c	One of four methods must be provided by Participant to the Authentication Station Operator [Operator] in order for the Authentication Station Operator to access the valid FiXs identifier to initiate the authentication process(Detailed in Section 2.1.5.3): 1) No Token/Verbal Communication of Organization and Employee ID 2) Presentation of Company/Organization Badge 3) Presentation of FiXs badge 4) DoD EDI PIN for CAC Cardholders	One of four methods must be provided by Participant to the Authentication Station Operator [Operator] in order for the Authentication Station Operator to access the valid FiXs identifier to initiate the authentication process(Detailed in Section 2.1.5.3): 1) No Token/Verbal Communication of Organization and Employee ID 2) Presentation of Company/Organization Badge 3) Presentation of FiXs badge 4) DoD EDI PIN for CAC Cardholders (FiXs PIN for FiXs Holders)
EI	NEW h	All certificates issued to a FiXs credential will use the DN format for subject and issuer name fields.	TBD
EI	NEW i	(None)	The DN must include a unique identification string in the CN or as a dnQualifier that will consist of a FiXs Person Designator Identifier (PDI) unique to the credential holder.

El	NEW j	(None)	The unique identifier shall be same for all certificates issued to a single credential holder and will be unique to all credentials across the FiXs network.
El	NEW k	All certificates issued to a FiXs credential will include an Organizational Unit that identifies the FiXs assurance level as follows: <ul style="list-style-type: none">• ou=FiXs4, for FiXs credentials asserting FiXs equivalent “High”• ou=FiXs3, for FiXs credentials asserting FiXs equivalent “Medium High”• ou=FiXs2, for FiXs credentials asserting FiXs equivalent “Medium”• ou=FiXs1, for FiXs credentials asserting FiXs equivalent “Low”	TBD
El	NEW t	(None)	<i>Medium High Level - Non-Security Clearance Credential for Enhanced First Responder Designees and Medium Level - Non-Security Clearance Credentials for Standard First Responder Designess</i> issuers must adhere to the Fair Credit and Reporting Act (The FCRA) and other applicable laws. All identified job skills personnel/individuals must be informed, by the credential issuer, that by giving their approval under the “Identity Verification Requirement” and entering their personally identifiable data into the system, they consent and authorize FiXs and/or third party background screening provider(s) to perform background screenings checks for them that “requires physical or logical access to their job or agency-related activity but do not fall under the category of government employee or government contractor.

EI	NEW u	(None)	<p>Medium High Level - Non-Security Clearance Credential for Enhanced First Responder Designees Identity Verification Requirements:</p> <ul style="list-style-type: none"> • Applicants must have a sponsor (authorizes the need for applicant to obtain physical and logical access to Federal facility) • Applicant must appear in person at Registration or Enrollment Station • Applicant must present 2 forms of Government issued ID Per US Form I-9 or 6 CFR Part 37 , one of which must have a photo. • Individual Information: <ul style="list-style-type: none"> ü Date of birth; ü Proof of SSN or ineligibility for an SSN; ü The applicant's address of principal residence; and ü Lawful status in the United States. ü Company-issued Employee Identification Number ü Felony and Misdemeanor convictions ü Outstanding warrant ü Terrorist Watch List • Applicants fingerprints will be collected electronically (ten flat or rolled) • Applicants pin must be used to complete the transaction
----	-------	--------	---

EI	NEW v	(None)	<p><i>Medium Level - Non-Security Clearance Credential for Standard First Responder Designees Credential Identity Verification Requirements:</i></p> <ul style="list-style-type: none"> • Applicants must have a sponsor (authorizes the need for applicant to obtain physical and logical access to Federal facility) • Applicant must appear in person at Registration or Enrollment Station • Applicant must present 2 forms of Government issued ID Per US Form I-9 or 6 CFR Part 37 , one of which must have a photo. • Applicants fingerprints will be collected electronically index fingers for the sole purpose of tying the identity to the credential. • Applicant must appear in person • Applicant must present 2 forms of Government issued ID Per US Form I-9 or 6 CFR Part 37 , one of which must have a photo. Documents must include information supporting the claim of <ul style="list-style-type: none"> ◦ Date of birth; ◦ Proof of SSN or ineligibility for an SSN; ◦ The applicant's address of principal residence; and ◦ Lawful status in the United States. • Applicants fingerprints will be collected electronically (ten flat or rolled) for identity and adjudication purposes • Applicants pin must be used to complete the transaction
----	-------	--------	---

El	NEW w	(None)	<i>Medium High Level Clinical First Reponder</i> credential issuers must adhere to the Fair Credit and Reporting Act (The FCRA) and other applicable laws, this is to inform all identified job skills/individuals that by giving their approval under the “Clinical Licensure Verification Requirement” and entering their personally identifiable data, they consent and authorize FIX’s and/or third party background screening provider(s) to perform qualifications screenings checks for them that “requires physical or logical access to their job or agency-related activity but do not fall under the category of government employee or government contractor. Must adherer to the Department of Health and Human Services Standard for Early System for Advanced Registration of Volunteer Health Professionals, Standards of the Joint Commission (JAHCO), and any applicable local, County or State Requirements
----	-------	--------	---

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

EI	NEW x	(None)	<p>Medium High Level Clinical First Responder Licensure Verification Requirements:</p> <ul style="list-style-type: none"> • Applicant must appear in person • Applicant must present (dependent on profession); <ul style="list-style-type: none"> ◦ Original copy of a state issued medical license with no restrictions, and or active and unrestricted state issued license to practice with the scope identified by the state ◦ Original copy of MD. DO. PhD. MS. RN. Degree from an educational institution accredited by the authority having jurisdiction referenced under “evidence of credential – explanation of credential elements” from the emergency credentialing standard for that profession as defined in the HHS ESAR-VHP Standard. ◦ Original copy of the DEA Registration Certificate for License Verification ◦ Proof of Active Clinical practice through attestation or other documentation or peer reference from a credential holding peer (with ID reference), affirming that the individual is practicing medicine, or working within the scope of the profession being vetted, in a hospital or non hospital setting. ◦ Proof of Active Clinical Hospital Privileges through attestation or other documentation or peer reference from a credential holding peer (with ID reference) , affirming that the individual is practicing medicine, or works within the scope of the profession being vetted and has privileges in a hospital setting. ◦ Proof of State or National Certification to practice, under medical control, as a pre-hospital car provider • Applicants pin must be used to complete the transaction
AD	NEW a	(None)	<p>Once an Applicant's background check is completed, a trained Adjudicator [Privacy Official] must make a trustworthiness assessment of the Applicant prior to</p>

			the Applicant being enrolled into a FiXs Domain Server.
AD	NEW b	(None)	<p><i>High Level HSPD-12 Compatible Credential and High Level DoD LACS/PACS Credential Identity Vetting Requirements:</i></p> <ul style="list-style-type: none"> • NAC: ◦ Security/Suitability Investigations Index (SII) ◦ Defense Clearance and Investigations Index (DCII) ◦ FBI Name Check ◦ FBI National Criminal History Fingerprint Check • Written inquiries and searches of records: ◦ Employment, going back 5 years ◦ Education, going back 5 years and verifying highest degree ◦ Residence, going back 3 years ◦ References ◦ Law enforcement checks, going back 5 years
AD	NEW c	(None)	<p>No person shall be granted a <i>High Level HSPD-12 Compatible Credential, High Level DoD LACS/PACS Credential, and Medium High Level DoD and Commercial Use PACS/LACS Credential</i> if their background investigation reveals any of the following:</p> <ul style="list-style-type: none"> • Is, or is suspected of being, a terrorist; • Is the subject of an outstanding warrant; • Has deliberately omitted, concealed, or falsified relevant and material facts from any official form used to collect biographic information for the purpose of initiating a background check; • Has presented false or forged identity source documents; • Has been barred from Federal employment; • Is currently awaiting a hearing or trial or has been convicted of a crime punishable by imprisonment of six (6) months or longer; or • Is awaiting or servicing a form of pre-prosecution probation, suspended or deferred sentencing, probation

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

			or parole in conjunction with an arrest or criminal charges against the individual for a crime that is punishable by imprisonment of six (6) months or longer.
AD	NEW d	(None)	<p>Medium High Level DoD and Commercial Use PACS/LACS Credential Background Check Requirements:</p> <ul style="list-style-type: none"> • Terrorist watch list check • Law Enforcement checks, going back five (5) years • FBI Name Check • FBI National Criminal History Fingerprint Check
AD	NEW e	(None)	<p>Medium High Level - Non-Security Clearance Credential for Enhanced First Responder Designees Identity Vetting Requirements:</p> <ul style="list-style-type: none"> • NAC I Commercial Equivalent Check (CEC). ◦ FBI Name and FBI National Criminal History Fingerprint Check ◦ Terrorist Watch List ◦ Local Law Enforcement agency check ◦ Residency verification • Written Inquires and Search of Records ◦ Employment going back 5 years ◦ Education going back 5 years ◦ Residences going back 3 years (Note: Separately, all overseas addresses) ◦ References (3 personal, non-relatives)

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

AD	NEW f	(None)	<p>No person shall be granted a <i>Medium High Level - Non-Security Clearance Credential for Enhanced First Responder Designees</i> if the background check reveals any of the following:</p> <ul style="list-style-type: none"> • Is or is suspected of being a terrorist; • Has been charged or convicted under any provision of the Patriot Act • Is the subject of an outstanding warrant; • Has deliberately omitted, concealed, or falsified relevant or material facts from any official form used to collect biographic information for the purpose of initiating a background check; • Has presented false or forged identity documents; • Has a current Criminal (not civil) restraining order, or has had a criminal restraining order within the last five years, issued due to threat of violence or sexual assault • Is on the Sex Offenders List (level 2or 3) (in the last ten years level 2, life level 3) • Is currently awaiting a hearing or trial or has been convicted of a crime punishable by imprisonment of six (6) months or longer; or • Is awaiting or servicing a form of pre-prosecution probation; suspended or deferred sentencing, probation or parole in conjunction with an arrest or criminal charges against the individual for a crime that is punishable by imprisonment of six (6) months or longer.
----	-------	--------	---

AD	NEW g	(None)	<p><i>Medium Level - Non-Security Clearance Credential for Standard First Responder Designees Credential Identity Vetting Requirements:</i></p> <ul style="list-style-type: none"> • Establish validity of the identity - Identity proofing using administrative/manual methods providing identity proofing criteria from breeder documents required in Federal form I-9, to verify the identity exists, the identity is active (not deceased) and the components are related at a moderate level of assurance. • Criminal History Record Information (CHRI) / Risk Analysis (include a data quality score?) - to include Local, County, State as required by the laws governing the sponsoring authority
AD	NEW h	(None)	The criteria used to adjudicate the background checks for persons requiring <i>Medium Level - Non-Security Clearance Credential for Standard First Responder Designees Credential</i> is determined by the State, County, and Local requirements and laws governing the sponsoring authority.
AD	NEW i	(None)	<i>Medium High Level Clinical First Reponder Credential</i> must meet the requirements of Emergency System for Advanced Registration of Health Professions Volunteers. Title 42, Chapter 6A, Sub-Chapter II, Part B, § 247d-7b

A	NEW j	(None)	<p>Medium High Level Clinical First Reponder Licensure</p> <p>Vetting Requirements:</p> <ul style="list-style-type: none"> • May include, dependent on professional, but not be limited to • Primary Source Verification or delegation to a JCAHO accredited organization that has performed primary source verification of the individual's credentials. • Degree, MD or DO through AAMC, AOA or ECFMG; for all others from an accredited institution • Unencumbered Medical License from State of Issue • Board Certification in recognized specialty or sub specialty from ABMS or AOA • National Practitioner Databank Status • Drug Enforcement Agency (DEA) License Verification with types • Inspector General Status
AD	NEW k	(None)	<p>No person shall be granted a Medium High Level Clinical First Reponder Credential if the licensure check reveals any of the following:</p> <ul style="list-style-type: none"> • Any failure to meet any of the credential elements for the profession as outlined in the Department of Health and Human Services Health resources Services Administrations "Standards and Guidelines for the Early System for the Advanced Registration of Volunteer Healthcare Professionals. • Any Active Sanction on record with any State Inspector General • Any Active disciplinary issue on file with the National Practitioner Databank
CP	NEW g	(None)	<p>Each CA that issues certificates to FiXs credentials shall have an approved CPS corresponding to one or more of the referenced CPs, for the appropriate level of assurance. A FiXs issuer shall only issue credentials with certificates that hold and assert the appropriate level of assurance as defined by this document.</p>

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

CP	NEW h	(None)	Prior to issuance of certificates to a FiXs credential, the issuer will coordinate with the CA/ CMA to ensure that the procedures for authentication of personnel are documented in a Registration Practice Statement (RPS) and comply with the appropriate CP, and submitted to FiXs for approval.
CP	NEW	(None)	<i>High Level DoD LACS/PACS Credential, Medium High Level DoD and Commercial Use PACS/LACS Credential , Medium High Level - Non-Security Clearance Contractor and Commercial Use</i> must capture the contract number under which the FiXs Member Company (or subscriber) employee requires access to DoD resources, and reference to any existing security clearance an Applicant might have.
CP	NEW j	(None)	A color photograph (minimum of 300 dots per inch (dpi) resolution), presenting the individual from the top of the head to the shoulders, is to be placed in the upper left corner of the front of the FiXs Certified Credential card, vertically. Must be in Zone 1 of the front of the card.
CP	NEW k	(None)	For all color photographs, the background color should be uniform throughout an organization's issuance locations
CP	NEW l	(None)	Complete and specific technical requirements for facial image capturing should conform to NIST Special Publication (SP) 800-76, Biometric Data Specification for Personal Identity Verification.
CP	NEW m	(None)	The full legal name of the FiXs Certified Credential card holder's identity is to be printed under the photograph in capital letters. The minimum font size acceptable is 10 point. Must be in Zone 2 of the front of the card.
CP	NEW nn	(None)	The FiXs Certified Credential card holder's affiliation shall be printed in Zone 8 of the front of the card. The required font for the card holder's affiliation is 6 point Bold.

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

CP	NEW o	(None)	The FiXs Certified Credential card holder's organization name shall be printed in Zone 10 of the front of the card. Two lines are available for use, with 6 point Bold being the font requirement.
CP	NEW p	(None)	The FiXs Certified Credential card expiration date is to be printed in a YYYYMMMD format (example: 2007MAR30) in Zone 14 of the front of the card. The expiration date is to be printed in 6 point Bold.
CP	NEW q	(None)	The unique serial number from the agency/organization shall be placed in Zone 1 of the back of the FiXs Certified Credential card. This serial number will be required to be printed in 6 point Bold, left-justified.
CP	NEW r	(None)	Issuer information shall be placed in Zone 2 of the back of the FiXs Certified Credential card and printed in 6 point Bold and right-justified.
CP	NEW s	(None)	The printed information on the FiXs Certified Credential card shall be printed so that the print cannot be rubbed off the actual card material through printing, laminating, and during normal wear and tear throughout the card's life cycle.
CP	NEW t	(None)	The print on the FiXs Certified Credential card is not to be obscured by any images
CP	NEW u	(None)	No manual markings or embossing (unless done during manufacture of the card itself by the manufacturer) are allowed on FiXs Certified Credential cards
CP	NEW v	(None)	No decals or stickers of any type are to be affixed to the FiXs Certified Credential card
CP	NEW w	(None)	No manual markings or embossing (unless done during manufacture of the card itself by the manufacturer) are allowed on PIV cards
CP	NEW x	(None)	Contactless FiXs Certified Credential cards shall be compatible with ISO7819
CP	NEW y	(None)	Contactless FiXs Certified Credential cards shall be compatible with ISO10373

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

CP	NEW z	(None)	Contactless FiXs Certified Credential cards shall be compatible with ISO7816
CP	NEW aa	(None)	Contactless cards FiXs Certified Credential shall be compatible with ISO14443
CP	NEW bb	(None)	<p>FiXs Certified Credential cards should conform to test methods used in ANSI322 regarding:</p> <ul style="list-style-type: none"> • Card flexure • Static stress • Plasticizer exposure • Impact resistance • Card structural integrity • Surface abrasion • Temperature and humidity-induced dye migration • Ultraviolet light exposure • Laundry tests
CP	NEW cc	(None)	FiXs Certified Credential card must be able to withstand up to 2000 hours of southwestern United States sunlight exposure (actual, concentrated, or artificial), as stipulated in ISO 10373
CP	NEW dd	(None)	All FiXs Certified Credential cards shall meet testing requirements in [G90-98] for concentrated sunlight exposure and [G155-00] for accelerated exposure.
CP	NEW ee	(None)	FiXs Certified Credential cards must be able to withstand using a mild soap and water mixture. This should not cause the PIV card to malfunction, nor should it cause the laminate to peel.
CP	NEW ff	(None)	Per ISO 10373, no visible cracks or failures should be experienced following dynamic bending of the FiXs Certified Credential cards.
CP	NEW gg	(None)	FiXs Certified Credential cards must be 27 to 33-mil thick (prior to lamination).
CP	NEW hh	(None)	Hole punching of the FiXs Certified Credential card shall not be done in text and photo areas and any zones that feature machine-readable technology

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

CP	NEW ii	(None)	All security features used on a FiXs Certified Credential card must be in accordance with durability requirements in ISO7810.
CP	NEW jj	(None)	All security features of the FiXs Certified Credential card must be free of defects, such as fading, discoloring, or tampering
CP	NEW kk	(None)	Printed security information on the FiXs Certified Credential is to be legible and not obscured by any images whatsoever
CP	NEW ll	(None)	Electronic contact points on the FiXs Certified Credential card are to be free from printing zones, so that data can be read and written without impediment
CP	NEW mm	(All FiXs Certified Credential cards are required to have at least one of the following security features(Note 2): <ul style="list-style-type: none"> - Optical Varying Structures - Optical Varying Inks - Laser Etching and Engraving - Holograms - Holographic Images - Watermarks - Personal Identification Number - Card Holder Unique Identifier - Biometrics - Encryption

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

CP	NEW nn	(None)	<p>The FiXs barcode will consist of the following data elements (in order):</p> <ol style="list-style-type: none"> 1. Agency Code (within the FASC-N) will be assigned a value, 9999, to indicate that the card has been issued by a non-Federal issuer; 2. System Code (within the FASC-N) will be assigned a unique number ranging between 1 and 9999 to identify the FiXs enrollment and/or issuance system used by a FiXs member organization; 3. Credential Number (within the FASC-N) will be assigned a unique number ranging between 1 and 999,999 to identify the individual credential issued by a particular FiXs enrollment and/or issuance system used by a FiXs member organization; 4. Credential Series (Series Code) - within the FASC-N - will initially be assigned a value, 1, to indicate the first series and incremented up to 9 for additional series; 5. Individual Credential Issue (Credential Code) - within the FASC-N - should always be assigned a value, 1, as recommended by PACS Version 2.3; 6. Organization Category (within the FASC-N) will be assigned a value, 3, to indicate that the card issuer is a commercial organization; 7. Organization Identifier (within the FASC-N) will be assigned a value between 1 and 9999 to identify the lower sixteen bits of the FiXs member's organization identifier;
AI	1	The personalized FiXs Certified Credential Card complies with all the mandatory items on the front of the FiXs Certified Credential Card.	<p>The personalized FiXs Certified Credential Card complies with all the mandatory items on the front of the FiXs Certified Credential Card. Card complies with FiXs Implementation Guidelines Appendix A Smart Card Topology Requirements</p>

AI	1	(i) the FiXs Certified Credential Card meets specific requirements in FIPS 201-1 for (i) photograph; (ii) name; (iii) employee; affiliation; (iv) and expiration date (observe).	(i) the FiXs Certified Credential Card meets specific requirements in FiXs Implementation Guidelines for (i) photograph; (ii) name; (iii) employee; affiliation; (iv) and expiration date. Card complies with FiXs Implementation Guidelines Appendix A Smart Card Topology Requirements (observe).
AI	2	The personalized FiXs Certified Credential Card complies with all the mandatory items on the back of the FiXs Certified Credential Card.	The personalized FiXs Certified Credential Card complies with all the mandatory items on the back of the FiXs Certified Credential Card. Card complies with FiXs Implementation Guidelines Appendix A Smart Card Topology Requirements.
AI	2	(i) the FiXs Certified Credential Card meets specific requirements in FIPS 201-1 for (i) organization card serial number; (ii) and issuer identification. (observe).	(i) the FiXs Certified Credential Card meets specific requirements in FiXs Implementation Guidelines for (i) organization card serial number; (ii) and issuer identification. Card complies with FiXs Implementation Guidelines Appendix A Smart Card Topology Requirements (observe).
MP	7	The organization has completed a life-cycle walk-through at one-year intervals since the last accreditation date and the results are documented in a report to the DAA.	The organization has completed a life-cycle walk-through at one-year intervals since the last accreditation date and the results are documented in a report to the FiXs Organization Authorizing Official .
MP	7	(iii) the results of the Credential Issuer life-cycle walk-through have been documented and reviewed by the DAA (review, interview).	(iii) the results of the Credential Issuer life-cycle walk-through have been documented and reviewed by the FiXs Organization Authorizing Official (review, interview).
MP	6	The organization posts a quarterly report, stating the number of FiXs Certified Credential Cards issued to date, to the organization's website and the link is emailed to OMB.	The organization posts a quarterly report, stating the number of FiXs Certified Credential Cards issued to date, to the organization's website and the link is emailed to FiXs organization and applicable OMB parties .
MP	6	(i) the organization develops and post a quarterly report to the organization's website according to the requirements of the attachment to OMB memorandum 07-06 (review);	(i) the organization develops and post a quarterly report to the organization's website according to the requirements of the attachment to OMB memorandum 07-06 or FiXs provided format (review);

MP	6	(i) the organization develops and post a quarterly report to the organization's website according to the requirements of the attachment to OMB memorandum 07-06 or (review);	(i) the organization develops and provides (makes available) a quarterly report according to the requirements of the attachment to OMB memorandum 07-06 or FiXs provided format (review);
MP	6	(ii) the organization sends the link to the report to OMB on a quarterly basis (review, interview).	(ii) the organization the report to FiXs (and OMB if required) on a quarterly basis (review, interview).

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

PREPARATION & MAINTENANCE OF DOCUMENTATION

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

Item	Req. Id	FiXs	Requirement					Assessment Result	
				I	D	T	O		
1	DO-1	OR: 5	The organization develops and implements an operations plan according to the template in Appendix D of NIST 800-79-1. The operations plan references other documents as needed.	I	D	T	O	The organization has developed an 800-79-1 Operations Plan and is consistent with the CP and CPS.	FS/PS/NS
			(i) the operations plan includes the relevant elements from the template in Appendix D of NIST 800-79-1(review);	X					
			(ii) the operations plan includes the list of Credential Issuer controls and included with each is the Credential Issuer control owner, how they were implemented and whether they are organization or facility specific (review);	X					
			(iii) for any documentation required but not included in the operations plan the name and location is provided (review);	X					
			(iv) the operations plan is reviewed and approved by designated officials within the organization (interview).	X					
2	DO-2	OR: 14, 15, 16, 17, 22, 23, 24, 25, 26, 43, 50, 51, 52, 55, 64, 65, 71	The organization has a written policy and procedures for enrollment/identity proofing which are signed off by the head of the organization.	I	D	T	O	Written policy and procedures for enrollment/identity proofing is consistent with the CP and CPS.	FS/PS/NS
			(i) the organization develops and documents written policy and procedures for identity proofing and enrollment (review);	X					
			(ii) the policy is consistent with the organization's mission and functions, FIPS 201-1 and applicable laws, directives, policies, regulations, standards, and guidance (review);	X					

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

			(iii) the policy and procedures have been signed off by the head of the organization(review);	X				
			(iv) the organization periodically reviews and updates the policy and procedures as required (review, interview).	X	X			
3	DO-3	Registrar = Privacy Official	The organization has a written policy and procedures describing the conditions for FiXs Certified Credential issuance which are signed off by the head of the organization.	I	D	T	O	Written policy and procedures for describing the conditions for FiXs Certified Credential issuance is consistent with the CP and CPS.
			(i) the organization develops and documents a written policy and procedures for issuance (review);	X				
			(ii) the policy is consistent with the organization's mission and functions, FIPS 201-1 and applicable laws, directives, policies, regulations, standards, and guidance (review);	X				
			(iii) the policy and procedures have been signed off by the head of the organization(review);	X				
			(iv) the organization periodically reviews and updates the policy and procedures as required (review, interview)	X	X			
	DO-4		The organization has a written policy and procedures describing the conditions for FiXs Certified Credential Card renewal which are signed off by the head of the organization.	I	D	T	O	Written policy and procedures for describing the conditions for FiXs Certified Credential Card termination is consistent with the CP and CPS.
								FS/PS/NS

			(i) the organization develops and documents a written policy and procedures for card renewal (review);	X				
			(ii) the policy is consistent with the organization's mission and functions, FIPS 201-1 and applicable laws, directives, policies, regulations, standards, and guidance (review);	X				
			(iii) the policy and procedures have been signed off by the head of the organization(review);	X				
			(iv) the organization periodically reviews and updates the policy and procedures as required (review, interview).	X	X			
DO-5			The organization has a written policy and procedures describing the conditions for FiXs Certified Credential termination which are signed off by the head of the organization.	I	D	T	O	Written policy and procedures for describing the conditions for FiXs Certified Credential Card termination is consistent with the CP and CPS. FS/PS/NS
			(i) the organization develops and documents a written policy and procedures for FiXs Certified Credential termination (review);				X	
			(ii) the policy is consistent with the organization's mission and functions, FIPS 201-1 and applicable laws, directives, policies, regulations, standards, and guidance (review);	X				
			(iii) the policy and procedures have been signed off by the head of the organization(review);	X				
			(iv) the organization periodically reviews and updates the policy as required (review, interview).	X	X			

	DO-6		The organization has a written policy and procedures describing the conditions for FiXs Certified Credential re-issuance which are signed off by the head of the organization.	I	D	T	O	Written policy and procedures for describing the conditions for FiXs Certified Credential Card re-issuance is consistent with the CP and CPS.	FS/PS/NS
			(i) the organization develops and documents a written policy and procedures for re-issuance (review);	X					
			(ii) the policy is consistent with the organization's mission and functions, FIPS 201-1 and applicable laws, directives, policies, regulations, standards, and guidance (review);	X					
			(iii) the policy and procedures have been signed off by the head of the organization(review);	X					
			(iv) the organization periodically reviews and updates the policy and procedures as required (review, interview).	X	X				
	DO-7		In cases where a FiXs Certified Credential Card is not required, such as temporary employees and contractors employed for less than 6 months and visitors, the organization has a written policy and procedures describing the conditions for temporary badges.	I	D	T	O		FS/PS/NS
			(i) the organization develops and documents a written policy and procedures for the issuance of temporary badges (review);	X					
			(ii) the policy is consistent with the organization's mission and functions, FIPS 201-1 and applicable laws, directives, policies, regulations, standards, and guidance (review);	X					

			(iii) the organization periodically reviews and updates the policy and procedures as required (review, interview).	X	X				
DO-NEW	OR: 39		Credential Issuers are responsible for maintaining updated FiXs Audit Files. These files must be updated and maintained by the FiXs Member Organization in a timely manner.						
DO-NEW	OR: 60		A revocation process must exist such that an expired or invalidated credential is swiftly revoked						
DO-NEW	OR: 72		All Credential Issuing Organizations must be certified as having Authorization to Operate (ATO) by FiXs Executive Board						
DO-NEW			The Registration Practice Statement must define the process for the periodic FiXs File Updates, in accordance with Section 1.2.7.1 of the FiXs Operating Rules.						

FS - Fully Satisfied

I - Interview

OR - FiXs Operating Rules Compliance Checklist

IG - FiXs Implementation Guidelines Checklist

PS - Partially Satisfied

D - Documentation Review

NS - Not Satisfied

T - Test

O - Observe

Assessment Results

	FS	0
	PS	0
	NS	0
Total		0

ASSIGNMENT OF ROLES & RESPONSIBILITIES

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

C	Req. Id	FiXs	Requirement					Assessment Result	
1	RR-1	OR: 1 <i>Program Manager =SAO</i>	The organization has appointed the role of Senior Authorizing Official (SAO).	I	D	T	O		FS/PS/NS
			(i) the organization has defined the role of Senior Authorizing Official and its responsibilities according to the requirements of SP 800-79-1 (interview);	X					
			(ii) the organization has assigned the role of Senior Authorizing Official (review);		X				
2	RR-2	OR: 1 <i>FiXs Executive Board =DAA</i>	The organization has appointed the role of Designated Accreditation Authority (DAA).	I	D	T	O		FS/PS/NS
			(i) the organization has defined the role of Designated Accreditation Authority and its responsibilities according to the requirements of SP 800-79-1 (interview);	X					
			(ii) the organization has assigned the role of Designated Accreditation Authority (review, interview);	X	X				
3	RR-3	OR: 3 <i>Organization Level Program Manager / Director = OIMO</i>	The organization has appointed the role of Organization Identity Management Official (OIMO).	I	D	T	O		FS/PS/NS
			(i) the organization has defined the role of Organization Identity Management Official and its responsibilities according to the requirements of SP 800-79-1 (interview);	X					
			(iii) the organization has appointed someone to the role of Organization Identity Management Official (interview).						

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

		OR: 4	The Functional Administrator [FOMO] must designate individuals within the organization who have the authority to attest to the applicant's need for a FiXs credential.	X					
3	RR-4	OR: 5 Certification Authority = Assessor	The organization has appointed the role of Assessor.	I	D	T	O		FS/PS/NS
			(i) the organization has defined the role of Assessor and its responsibilities according to the requirements of SP 800-79-1 (review);		X				
			(ii) the organization has assigned the role of Assessor (review);		X				
			(iii) the Assessor is independent of, and organizationally separate from, the persons and office(s) directly responsible for the day-to-day operation of the organization (review, interview).	X	X				
4	RR-5		The organization has appointed the role of Privacy Official (PO).	I	D	T	O		FS/PS/NS
			(i) the organization has defined the role of Privacy Official and its responsibilities according to the requirements of SP 800-79-1 (interview);	X					
			(ii) the organization has assigned the role of Privacy Official in the operations plan (review, interview);	X	X				
			(iii) the Privacy Official does not have any other roles in the Credential Issuer process (review, interview).	X					
6	RR-6	IG: 4, 8, 13, 18	The Credential Issuer Facility employs processes which adhere to the principle of separation of duties to ensure that no single individual has the capability to issue a FiXs Certified Credential Card without the cooperation of another authorized person.	I	D	T	O		FS/PS/NS

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

			(i) the Credential Issuer facility documents in standard operating procedures the principle of separation of duties (review);	X				
			(ii) the Credential Issuer facility's processes demonstrate adherence to the principle of separation of duties (interview, observe).	X		X		
RR-NEW	OR: 2		PM must designate at least one Technical Administrator [Credential Issuer Facility Manager] who has the authority to perform maintenance on the Enrollment System and/or the Authentication System for the Member Organization.					
RR-NEW	OR: 6		A Credential Issuer must designate at least one Facility Administrator Enroller [<i>Operator</i>] per Member facility.					
RR-NEW	OR: 10		A Credential Issuer must designate at least one Facility Verifier per Member facility. Facility Verifiers must be separate personnel from Facility Enrollers.					
RR-NEW	OR: 11		A FiXs Member organization must designate at least one Facility Domain Administrator per Member Facility.					

*Role of Senior Authorizing Official labeled as Program Manager (PM) in FiXs checklist

FS - Fully Satisfied

PS - Partially Satisfied

NS - Not Satisfied

I - Interview

D - Documentation Review

T - Test

O - Observe

OR - FiXs Operating Rules Compliance Checklist

IG - FiXs Implementation Guidelines Checklist

Assessment Results	
FS	0
PS	0
NS	0
Total	0

FACILITY & PERSONNEL READINESS

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

Item	Req. Id	FiXs	Requirement					Assessment Result	
				I	D	T	O		
	FP-1		Minimum physical controls at the Credential Issuer Facility are implemented. These include: (i) use of locked rooms, safes, and cabinets (as appropriate); (ii) physical access to key areas within the facility is restricted to authorized personnel, (iii) security monitoring and automated alarms are implemented, (iv) emergency power and lighting are available, and (v) fire prevention and protection mechanisms are implemented.					FS/PS/NS	
			(i) the OIMO and Credential Issuer Facility Managers(s) are aware of the minimum set of physical controls that need to be in place at the facility(ies) (interview);	x					
			(ii) the minimum physical security controls are implemented by the Credential Issuer Facility (observe).				x		
	FP-2	OR: 69, 70	Credential Issuer Documentation (e.g., operations plan, standard operating procedures, and contracts) are maintained at each Credential Issuer Facility.		I	D	T	O	FS/PS/NS
			(i) the most current versions of the Credential Issuer documentation is available at the Credential Issuer Facility for reference as needed (interview, review);	x	x				
	FP-3		The Credential Issuer Facility Manager(s) has a copy of the contingency/disaster recovery plan for the information systems, which is stored securely.		I	D	T	O	FS/PS/NS
			(i) the contingency plan/ disaster recovery plan is stored securely at the facility (interview, observe);	x			x		
			(ii) the Credential Issuer Facility Manager is knowledgeable on how to restore/reconstitute the information systems in case of system failures (interview).	x					

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

	FP-4		The information systems are managed using a system development life cycle (SDLC) methodology that includes information security considerations	I	D	T	O		FS/PS/NS
			(i) the information system used by the organization has been developed using an SDLC methodology (review, interview);	x	x				
			(ii) information system security is considered as part of the development life cycle (review).		x				
1	FP-5		Enrollment/identity proofing and card activation/issuance workstations are situated in an enclosed area (wall or partition) to provide privacy for an applicant or card holder.	I	D	T	O		FS/PS/NS
			(i) Credential Issuer Facility workstations are situated in an enclosed area (wall or partition) such that other individuals cannot see an applicant or card holder's personal information (observe).		x				
2	FP-6	OR: 8 Facility Enroller = Operator	All operators who perform roles within a Credential Issuer Facility in the areas of enrollment/ identity proofing or card activation/issuance are allowed access to information systems only when authenticated through a FiXs Certified Credential Card.	I	D	T	O		FS/PS/NS
			(i) the requirement that all operators who perform roles within a Credential Issuer Facility in the areas of enrollment/ identity proofing or card activation/issuance are allowed logical access to information systems only when authenticated through a FiXs Certified Credential Card, has been documented in the Credential Issuer Facility's standard operating procedures (review);		x				

			(ii) Operators use FiXs Certified Credential Cards to access information systems in the course of performing their roles in the areas of enrollment/ identity proofing or card activation/issuance access (observe).				X	
3	FP-7	OR: 7, 12 Facility Enroller = Operator	All operators who perform roles within a Credential Issuer Facility in the areas of enrollment/ identity proofing, adjudication and card activation/issuance have undergone training that is specific to their duties prior to being allowed to perform in that function.	I	D	T	O	FS/PS/NS
			(i) The requirement that all operators who perform roles within a Credential Issuer Facility in the areas of enrollment/ identity proofing, adjudication and card activation/issuance are allowed access to information systems only after completing a training course specific to their duties. (interview, review);		X			
			(ii) Records showing that the appropriate training course has been completed by Credential Issuer Facility personnel are stored by the facility for audit purposes (review)				X	
4	FP-8		All pre-personalized and personalized smart card stock received from card vendors and card production facilities are received only by authorized personnel who ensure that the card stock is stored securely in the Credential Issuer Facility.	I	D	T	O	FS/PS/NS
			(i) the Credential Issuer facility has an authorized list of personnel that are responsible for ensuring that smart card stock is received and stored securely in the Credential Issuer Facility (interview);	X				
			(ii) procedures for receiving and storing smart card stock are documented in the Credential Issuer Facility's standard operating procedures (review);		X			

			(iii) the authorized personnel are knowledgeable of the procedures on how to receive and store smart card stock (interview).	X					
	FP-9		The organization maintains a current list of designated point of contacts and alternate point of contacts for all Credential Issuer Facilities used by the organization for enrollment/identity proofing and card activation/issuance.	I	D	T	O		FS/PS/NS
			(i) the organization maintains a current list of designated point of contacts and alternate point of contacts for all Credential Issuer Facilities used by the organization for enrollment/identity proofing and card activation/issuance (review).		X				
	FP-NEW	OR: 18	The Enrollment System must contain an Enrollment Client						
	FP-NEW	OR: 19	The Enrollment System must contain an Enrollment Web Server						
	FP-NEW	OR: 20	The Enrollment System must contain Enrollment Web Software						
	FP-NEW	OR: 21	The Enrollment System must contain Operator Maintenance						
	FP-NEW	OR: 28	The Enrollment System must be available for use 24 hours a day 7 days a week.						
	FP-NEW	OR: 29	The FiXs Domain Server (FDS) must contain enrollment and authentication server software, which interfaces to the FiXs Data Repository, the FiXs Trust Broker, the Enrollment Client, and the Authentication Client.						

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

	FP- NEW	OR: 31	A Hardware Security Module (HSM) must be attached to the FDS. (Note 13)					
	FP- NEW	OR: 32	The Verification System must be operational 24 hours a day, 7 days a week					
	FP- NEW	OR: 33	The Verification System must have an up-time availability of 99.99%.					
	FP- NEW	OR: 34	The FDS must process an Authentication Inquiry and return an Authentication Response in no more than 5 seconds.					
	FP- NEW	OR: 42	Auditing of the FDS must be at a sufficient level to recreate any transaction successfully or unsuccessfully performed within the FiXs system.					
	FP- NEW	OR: 47	The Member Organization must have Encoder Reader Devices.					
	FP- NEW	OR: 48	The Member Organization must subscribe to a document Verification Service.					
	FP- NEW	OR: 66	The FDS must be capable of supporting HTTPS (SSL) protocol. The Member Organization's network and firewall must be configured to allow HTTPS incoming and outgoing transmissions, with outgoing transmissions being limited to the FiXs Trust Broker.					
	FP- NEW	OR: 67	The FDS must be placed within the Organization's firewall.					

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

	FP- NEW		<p>The Credential Issuer must receive periodic updates from the sponsoring FiXs Program Manager [Credential Issuer Facility Manager] or his/her designated agent on behalf of the applicant.</p> <p>Verification shall be in writing and signed or digitally signed with an active FiXs or CAC credential using a Medium Hardware Assurance certificate.</p>							
	FP- NEW	IG: 1	<p>A Credential Issuer must define an acceptable level of risk and then identify standards and procedures that, to the extent possible, support the level of risk. When the risk level and standards are defined by an external organization, such as a government Agency or client, a Credential Issuer must adopt the prescribed processes and requirements.</p>							
	FP- NEW	IG: 3	<p>Members wishing to issue FiXs Credentials must first identify which standards they intend to follow and then meet the requirements of the specified standard(s).</p>							
FS - Fully Satisfied I - Interview		PS - Partially Satisfied D - Documentation Review		NS - Not Satisfied T - Test		O - Observe		Assessment Results		
OR - FiXs Operating Rules Compliance Checklist IG - FiXs Implementation Guidelines Checklist								FS 0		
								PS 0		
								NS 0		
								Total 0		

PROTECTION OF STORED & TRANSMITTED DATA

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

Item	Req-Id	FiXs	Requirement					Assessment Result
				I	D	T	O	
1	SY-1	OR: 5, 27, 30, 35, 36, 37, 38, 40, 41, 43, 44, 45, 46, 54, 55, 56, 61, 68, 69, 70 <i>Facility Enroller = Operator</i>	The Credential Issuer information systems that contain information in identifiable form are handled in compliance with federal laws and policies including the Privacy Act of 1974.	I	D	T	O	FS/PS/NS
			(i) the Credential Issuer Facility does not disclose any record which is contained in the system of records to any person, or to another organization unless written consent has been given by the individual to whom the record pertains unless one of the exceptions for disclosure in the Privacy Act are met (review, interview);	X				
			(ii) individuals are permitted to gain access to their personal record and the information is provided in a form comprehensible to them (review, interview);	X				
			(iii) individuals are able to request amendments to records pertaining to them, corrections are made promptly and if not, the individual is provided with a reason for the refusal and is able to request a review of the refusal (review, interview);	X	X			
			(iv) the organization notifies an individual when their record is made available to any person under a compulsory legal process when such a process becomes a matter of public record (review, interview).	X	X			

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

2	SY-2		The information systems protect the integrity and confidentiality of transmitted information through the use of encryption or other alternate physical protection means.	I	D	T	O		FS/PS/NS
			(i) the integrity of transmitted information is protected by encryption or other alternate physical protection means (interview, test)		X				
			(ii) the confidentiality of transmitted information is protected by encryption or other alternate physical protection means (interview, test)				X		
	SY-NEW		In regard to components used for the issuance of FiXs credential, a network traffic recording, intrusion detection, and forensic analysis system shall be used to monitor intrusion attempts and policy verification (rated at EAL 2 in accordance with Intrusion Detection System Protection Profile (IDSP))						
	SY-NEW		Weekly review of the firewall and network system configurations against installation plans and procedures shall be made to ensure that no unauthorized changes are made to these systems.						
	SY-NEW		Hardware tokens will be stored in a security container.						
	SY-NEW		The CPUs, Redundant Array of Inexpensive Disks (RAID)/ external drives, monitors, keyboards, and mice will be sealed with Tamper Resistant Seals in accordance with paragraph 8-308, ISM and Tab B, Code A, Quantum Information and Computation (QUIC); in order to detect surreptitious entry into the equipment and associated peripherals.						

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

	SY- NEW		The tamper resistance seal will be inspected (and results logged) every month to ensure that it serves its intended use.								
	SY- NEW		Unescorted entry to the facility hosting the CMS or access to any server components (hardware/software) shall be limited to personnel who are cleared for access and whose need to access the components has confirmed.								
	SY- NEW		A FiXs CMS server is to be dedicated to administrating the system and shall only have software installed necessary to perform CMS functions. All upgrades will be from the original equipment manufacturers and software vendors.								
	SY- NEW		Assembly and maintenance of related systems will be accomplished in the controlled environment. Only designated personnel will perform maintenance on the related system.								
FS - Fully Satisfied I - Interview			PS - Partially Satisfied D - Documentation Review	NS - Not Satisfied T - Test			O - Observe			Assessment Results	
OR - FiXs Operating Rules Compliance Checklist IG - FiXs Implementation Guidelines Checklist										FS	0
										PS	0
										NS	0
										Total	0

ENFORCEMENT OF PRIVACY RIGHTS

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

Item	Req-Id	FiXs	Requirement					Assessment Result
				I	D	T	O	
1	PR-1		The organization has developed and posted at the Credential Issuer Facility in multiple locations (e.g., internet site, human resource offices, regional offices, provide at contractor orientation, etc.) privacy act statement/notice or FiXs provided equivalent, complaint procedures, appeals procedures for those denied identification or whose identification cards are revoked, and implements sanctions for employees violating privacy policies. The Credential Issuer collects, stores, processes and controls access and disclosure of personally identifiable information in accordance with applicable Corporate Policy and is in compliance with applicable: national, state, local and foreign laws, FiXs rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information (interview, observe).	I	D	T	O	FS/PS/NS
			(i) the Credential Issuer Facility has developed and posted at the Credential Issuer Facility in multiple locations (e.g., internet site, human resource offices, regional offices, provide at contractor orientation, etc.) privacy act statement/notice or FiXs provided equivalent, complaint procedures, appeals procedures for those denied identification or whose identification cards are revoked, and sanctions for employees violating privacy policies. (interview, observe).		X			
2	PR-2		The organization has conducted a Privacy Impact Assessment of their Credential Issuer information system (s), constituent with FiXs Rules, Guidance and applicable sections of: Section 208 of the E-Government Act of 2002, addresses guidance found in Appendix E of OMB Memorandum 06-06.	I	D	T	O	

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

			(i) the organization has conducted a Privacy Impact Assessment of their Credential Issuer information system (s) which addresses guidance found in Appendix E of OMB Memorandum 06-06 (review);		X				
			(ii) the organization has submitted the Privacy Impact Assessment of their Credential Issuer information system (s) to FiXs Executive Board (interview).		X				
3	PR-3		The organization's FiXs Certification Package are updated to reflect any changes in the disclosure of information to other organizations consistent with FiXs Guidance and applicable sections of the Privacy Act of 1974 and OMB Circular A-130, Appendix 1. If a SORN is required it has been updated with OMB and FiXs.	I	D	T	O		FS/PS/NS
			(i) the organization updates FiXs Certification Package to reflect changes in the disclosure of information policy. If a SORN is required it has been updated with OMB and FiXs. (review, interview).	X	X				
4	PR-4		The applicant is notified of what information in identifiable form is collected, how it will be used, what information will be disclosed and to whom, and what protections are provided to ensure the security of this information.	I	D	T	O		FS/PS/NS
			(i) Before receiving the FiXs Certified Credential Card, the Credential Issuer Facility requires the applicant to be notified of the personally identifiable information that is collected, how it will be used, what information will be disclosed and to whom, and what protections are provided to ensure the security of this information (review, observe)		X		X		
			(ii) the applicant is informed of what personally identifiable information is collected, how it will be used, what information will be disclosed and to whom, and what protections are provided to ensure the security of this information (interview)	X					

5	PR-5	The Credential Issuer Facility employs technologies that allow for continuous auditing of compliance with privacy policies and practices	I	D	T	O		FS/PS/NS
		(i) the Credential Issuer Facility employs technologies that allow for the continuous auditing of compliance with privacy policies and practices. This could include the use of technology to monitor data access, data flows between information systems and the use of Individually Identifiable Information (interview, test).	X		X			
	PR-6	In the case of termination, any personally identifiable information that has been collected from the cardholder is disposed of in accordance with the stated privacy and data retention policies.	I	D	T	O		FS/PS/NS
		(i) as a part of FiXs Certified Credential Card termination, the organization disposes of personally identifiable information in accordance with its privacy and data retention policies (review, interview).	X	X				
	PR- NEW	FiXs members shall adhere to the policy framework governing the public key infrastructure component defined by the policy referenced for each level or higher.						

FS - Fully Satisfied

I - Interview

OR - FiXs Operating Rules Compliance Checklist

IG - FiXs Implementation Guidelines Checklist

PS - Partially Satisfied

D - Documentation Review

NS - Not Satisfied

T - Test

O - Observe

Assessment Results

FS 0

PS 0

NS 0

Total 0

DEPLOYED PRODUCTS & INFORMATION SYSTEMS

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

Item	Req. Id	FiXs	Requirement					Assessment Result	
				I	D	T	O		
1	DP-1		In order to be compliant with the provisions of FiXs to DMDC MOA, (and if applicable: OMB Circular A-130, App III), the Credential Issuer information system(s) are certified in accordance with NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems.						FS/PS/NS
			(i) the organization has a letter showing the current accreditation decision of each information system used to support the Credential Issuer (review).		X				
2	DP-2		Every product utilized by a Credential Issuer facility that it falls within one of the categories listed by the FiXs Evaluation program, shall be listed in the FiXs Approved Product List (APL)		I	D	T	O	FS/PS/NS
			(i) for each product that falls within one of the categories listed within the APL, its make, model and version is compared against the APL (observe); Obtain an Inventory list of approved deployed Items {FiXs ADD-ON Rqmt}		X		X		
3	DP-3		The organization has submitted a personalized FiXs Certified Credential Card from their production system to FiXs (and GSA if applicable) for testing, and it has been approved.		I	D	T	O	FS/PS/NS
			(i) the organization has a letter from the GSA showing their approval of the card (review).		X				
FS - Fully Satisfied I - Interview OR - FiXs Operating Rules Compliance Checklist IG - FiXs Implementation Guidelines Checklist			PS - Partially Satisfied D - Documentation Review			NS - Not Satisfied T - Test O - Observe			Assessment Results FS 0 PS 0 NS 0 Total 0

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

IMPLEMENTATION OF CREDENTIALING INFRASTRUCTURE

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

Item	Req-Id	FiXs	Requirement					Assessment Result	
				I	D	T	O		
1	CI-1		For legacy Public Key Infrastructures (PKI's), the organization's CA shall be cross-certified with the Federal Bridge (FBCA) at Medium-HW or High Assurance Level.		X				FS/PS/NS
			(i) the PKI is listed on the FBCA's website as being cross-certified (review).		X				
2	CI-2		For non-legacy PKI's, the CA that issues certificates to support FiXs Certified Credential Card authentication participates in the hierarchical PKI for the Common Policy managed by the Federal PKI.		X				
			(i) the PKI is listed on the FPKI PA's website as being a shared service provider (review).		X				
3	CI-3		When cards are personalized, card management keys are set to be specific to each FiXs Certified Credential Card. That is, each FiXs Certified Credential Card shall contain a unique card management key.		X				FS/PS/NS
			(i) the CMS Vendor's documentation shows the use of unique card management keys (review);		X				
			(ii) the OIMO indicates that card management keys are unique. (interview).	X					
4	CI-4		Fingerprint images retained by organizations shall be formatted according to SP 800-76-1.		X				FS/PS/NS
			(i) the fingerprint images are formatted according to Table 4 in SP 800-76-1 and INCITS 381 (test).	X	X				
5	CI-5		Facial images collected during enrollment/identity proofing are formatted such that they conform to SP 800-76-1.		X				FS/PS/NS

			(i) the facial images are formatted according to Table 6 in SP 800-76-1 and INCITS 385 (review, test).		X	X				
6	CI-6		The fingerprint templates stored on the FiXs Certified Credential Card are prepared from images of the primary and secondary fingers where the choice of fingers is based on the order of priority, as provided in FIPS 201-1, Section 4.4.1.	I	D	T	O		FS/PS/NS	
			(i) the procedures used to fingerprint the applicant are based on the primary and secondary finger designations as required by the standard (review, observe);		X		X			
			(ii) the fingerprint templates are prepared from images of the primary and secondary fingers (test).		X					
	CI-NEW		Certificates issued on a FiXs credential shall be delivered via a GSA FIPS-201 approved CMS (Card Management System).							
FS - Fully Satisfied I - Interview			PS - Partially Satisfied D - Documentation Review			NS - Not Satisfied T - Test			Assessment Results OR - FiXs Operating Rules Compliance Checklist IG - FiXs Implementation Guidelines Checklist	
						O - Observe				

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

SPONSORSHIP PROCESS

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

Item	Req. Id	FiXs	Requirement	I	D	T	O	Assessment Result	
1	SN-1		A request is created in order to issue a FiXs Certified Credential Card.	I	D	T	O		
			(i) the process for making a request is documented (review);		X				
			(ii) A FiXs Certified Credential Request is created in order to issue a FiXs Certified Credential Card (observe).				X		
2	SN-2		The Credential Issuer Facility collects personal information using only forms approved by FiXs (and if applicable OMB under the Paperwork Reduction Act of 1995.)	I	D	T	O		
			(i) forms used to collect personal information have been approved by FiXs (and if applicable OMB) (review, observe).		X		X		
			(ii) Operators use FiXs Certified Credential Cards to access information systems in the course of performing their roles in the areas of enrollment/ identity proofing or card activation/issuance access (observe).				X		
FS - Fully Satisfied I - Interview		PS - Partially Satisfied D - Documentation Review		NS - Not Satisfied T - Test		O - Observe		Assessment Results	
								FS	0
								PS	0
								NS	0
								Total	0

ENROLLMENT/IDENTITY PROOFING PROCESS

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

Item	Req. Id	FiXs	Requirement	I	D	T	O	Assessment Result
1	EI-1		The Credential Issuer Facility has a process in place to verify the authenticity of the source documents and match them to the identity claimed by the Applicant.	I	D	T	O	FS/PS/NS
			(i) the Credential Issuer Facility has a process in place to verify the authenticity of the source documents and match them to the identity claimed by the Applicant (interview, observe);	X				
			(ii) the Credential Issuer Facility has materials used to train enrollment/identity proofing officials on how to verify the authenticity of the source documents (review).	X				
2	EI-2	OR: 49 IG: 5, 10, 15, 20,	The Credential Issuer Facility requires the Applicant to appear in-person at least once before the issuance of a FiXs Certified Credential Card.	I	D	T	O	FS/PS/NS
			(i) the requirement that an applicant appear in-person at least once before the issuance of a FiXs Certified Credential Card is documented (review);	X				
			(ii) the Applicant appears in-person at least once before the issuance of a FiXs Certified Credential Card (observe).				X	
3	EI-3	IG: 5, 10, 15, 20	Two identity source documents are checked in accordance with the requirements of Form I-9 (one of which must be a photo ID), OMB No. 1115-0136, Employment Eligibility Verification. (FiXs requirement: Applicant must present 2 forms of Government issued ID Per US Form I-9 or 6 CFR Part 37 , one of which must have a photo.)	I	D	T	O	FS/PS/NS
			(i) the requirement to check two identity source documents in accordance with the requirements of Form I-9 is documented (FiXs requirement: Applicant must present 2 forms of Government issued ID Per US Form I-9 or 6 CFR Part 37 , one of which must have a	X				

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

			photo.) (review);					
			(ii) two identity source documents are checked in accordance with the requirements of Form I-9 during enrollment/identity proofing (observe).			X		
			(iii) current proof of citizenship must be checked					
4	EI-4		One of the identity source documents used to verify the claimed identity of the Applicant is a valid Federal or State government issued photo identification.	I	D	T	O	FS/PS/NS
			(i) the requirement that one of the identity source documents is a valid Federal or State government issued photo ID is documented (review);					
			(ii) one of the identity source documents used to verify the claimed identity of the Applicant is a valid Federal or State government issued photo identification (observe).					
5	EI-5		The Credential Issuer Facility performs the entire identity proofing and enrollment/identity proofing process prior to re-issuing a FiXs Certified Credential Card.	I	D	T	O	FS/PS/NS
			(i) the requirement to perform the entire identity proofing and enrollment process prior to re-issuing a FiXs Certified Credential Card is documented (review);	X				
			(ii) the Credential Issuer Facility performs the entire identity proofing and enrollment process prior to re-issuing a FiXs Certified Credential Card (observe).				X	
6	EI-6		A new facial image is collected at the time of renewal.	I	D	T	O	FS/PS/NS

			(i) the requirement to capture a new facial image is documented within the renewal process (review);					
			(ii) a new facial image is collected at the time of renewal (observe).					
7	EI-7		The biometrics (fingerprints and facial image) that are used to personalize the FiXs Certified Credential Card must be captured during the enrollment/identity proofing process.	I	D	T	O	FS/PS/NS
			(i) the requirement to capture biometrics (fingerprints and facial image) that are used to personalize the FiXs Certified Credential Card must be captured during enrollment/identity proofing process is documented (review);	X				
			(ii) The biometrics (fingerprints and facial image) that are used to personalize the FiXs Certified Credential Card must be captured during the enrollment/identity proofing process (observe).				X	
8	EI-8		A cardholder waits until six weeks prior to the expiration of a valid FiXs Certified Credential Card before applying for renewal.	I	D	T	O	FS/PS/NS
			(i) the requirement that a cardholder must wait until six weeks prior to the expiration of a valid FiXs Certified Credential Card before applying for renewal is documented (review);					
			(ii) a cardholder waits until six weeks prior to the expiration of a valid FiXs Certified Credential Card before applying for renewal (interview).					
9	EI-9		The Credential Issuer Facility captures the Applicant's fingerprints in accordance to any of the three imaging modes: (i) plain live scan, (ii) rolled live scan, or (iii) rolled ink card. (FiXs requirement only electronic methods are implemented. Applicants fingerprints will be collected electronically (ten flat or rolled)	I	D	T	O	FS/PS/NS
			(i) the Credential Issuer Facility captures the Applicant's fingerprints in accordance to any of the three imaging modes: (i) plain live scan, (ii) rolled live scan, or (iii) rolled ink card (observe).				X	

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

10	EI-10		The Credential Issuer Facility has an attending official present at the time of fingerprint capture.	I	D	T	O		FS/PS/NS
			(i) the requirement that the Credential Issuer Facility has an attending official present at the time of fingerprint capture is documented (review);		X				
			(ii) the Credential Issuer Facility has an attending official present at the time of fingerprint capture (observe).				X		
11	EI-11		The Credential Issuer Facility acquires fingerprint images in accordance with Table 2 in 800-76-1.	I	D	T	O		FS/PS/NS
			(i) fingers are inspected for the absence of foreign materials (observe);				X		
			(ii) scanner and card surfaces are clean (observe);				X		
			(iii) the presentation of fingers for a plain live scan, rolled live scan, and rolled ink card are based on procedures in Table 1 (observe);				X		
			(iv) multi-finger plain impression images are properly segmented into single finger images (observe).				X		
12	EI-12		The Credential Issuer Facility captures the 10 fingerprints of the Applicant. In the case where less than ten fingers are collected, the missing fingers are labeled before transmitting to the FBI.	I	D	T	O		FS/PS/NS
			(i) the requirement that the Credential Issuer Facility captures the 10 fingerprints of the Applicant and labels any missing fingers is documented (review);		X				
			(ii) the Credential Issuer Facility captures the 10 fingerprints of the Applicant and labels any missing fingers (observe).				X		

	EI-NEW a	OR: 9	In a single session, the Facility Enroller [Operator] must completely and successfully capture and store an applicant's digitized photograph, fingerprint biometrics, and name identification and demographic data. All data must be correctly entered during the single session. All documents should be scanned.				SWITCHED this FiXs requirement from SY-1 It fits better under EI than under ST-1	
	EI-NEW b	OR: 13	Authentication Station Operator [Operator] must log in and authenticate to the system using their FiXs Certified Credential/identification number and biometric prior to processing FiXs Participants, the Authentication Station Operator.					
	EI-NEW c	OR: 58	<p>One of four methods must be provided by Participant to the Authentication Station Operator [Operator] in order for the Authentication Station Operator to access the valid FiXs identifier to initiate the authentication process(Detailed in Section 2.1.5.3):</p> <ul style="list-style-type: none"> 1) No Token/Verbal Communication of Organization and Employee ID 2) Presentation of Company/Organization Badge 3) Presentation of FiXs badge 4) DoD EDI PIN for CAC Cardholders (FiXs PIN for FiXs Holders) 					
	EI-NEW d	OR: 59	All credentials must have an expiration date					
	EI-NEW e	OR: 62	The Credential Issuer is required to process Authentication Inquiries from its Authentication Clients and from Relying Parties.					
	EI-NEW f	OR: 63	The Credential Issuer must return an Authentication Response to the originator of the Authentication Inquiry.					

	EI-NEW g		FiXs member shall insure no FiXs Certified Credential holder shall hold more then one active FiXs Certified Credential.					
	EI-NEW h		TBD					
	EI-NEW i		The DN must include a unique identification string in the CN or as a dnQualifier that will consist of a FiXs Person Designator Identifier (PDI) unique to the credential holder.					
	EI-NEW j		The unique identifier shall be same for all certificates issued to a single credential holder and will be unique to all credentials across the FiXs network.					
	EI-NEW k		TBD					
	EI-NEW l		<p>All FiXs Certified Credential Issuers will comply with uniqueness of names as enforced across the FiXs Network, including X.500 DNs and Card Holder Unique Identifier (CHUID) Data Elements as stipulated in the FiXs implementation requirements. Each FiXs Certified Credential Issuers shall enforce credential uniqueness, as described in Section 1.7 and ensure the following:</p> <ul style="list-style-type: none"> • The applicant does not hold an active FiXs Certified Credential • The name contains the applicant's identity and organization affiliation that is meaningful to humans • The naming convention is as described in the corresponding CP and CPS 					
	EI-NEW m		Each Certified FiXs Certified Credential Issuer will ensure that each individual holds only one active FiXs Certified Credential by verifying that management personnel are authorized to approve the issuance of a credential to an applicant (e.g., contracting officer or contracting officer's technical representative)					

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

	EI- NEW n		Each FiXs Certified Credential Issuer will ensure that each individual holds only one active FiXs Certified Credential by verifying applicant's employment through use of official records.					
	EI- NEW o		The Credential Issuer shall record the process(es) followed for issuance of the certificate.					
	EI- NEW p		The process documentation and authentication shall include the identity of the person performing the identification.					
	EI- NEW q		The process documentation and authentication shall include a signed declaration by that person that he or she verified the identity of the Applicant as required by the CPS using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) and that he or she verified, via the FiXs network that the applicant does not hold another FiXs Certified Credential.					
	EI- NEW r		The process documentation and authentication shall include the date and time of the verification.					
	EI- NEW s		The process documentation and authentication shall include a declaration of identity signed by the applicant using a handwritten signature that includes that assertion that the applicant does not hold another FiXs Certified Credential, performed in the presence of the person performing the identity authentication, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury).					

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

	EI-NEW t	IG: 23, 27	<p>Medium High Level - Non-Security Clearance Credential for Enhanced First Responder Designees and Medium Level - Non-Security Clearance Credentials for Standard First Responder Designees issuers must adhere to the Fair Credit and Reporting Act (The FCRA) and other applicable laws. All identified job skills personnel/individuals must be informed, by the credential issuer, that by giving their approval under the “Identity Verification Requirement” and entering their personally identifiable data into the system, they consent and authorize FiXs and/or third party background screening provider(s) to perform background screenings checks for them that “requires physical or logical access to their job or agency-related activity but do not fall under the category of government employee or government contractor.</p>					
	EI-NEW u	IG: 24	<p>Medium High Level - Non-Security Clearance Credential for Enhanced First Responder Designees Identity Verification Requirements:</p> <ul style="list-style-type: none">• Applicants must have a sponsor (authorizes the need for applicant to obtain physical and logical access to Federal facility)• Applicant must appear in person at Registration or Enrollment Station• Applicant must present 2 forms of Government issued ID Per US Form I-9 or 6 CFR Part 37 , one of which must have a photo.• Individual Information:<ul style="list-style-type: none">ü Date of birth;ü Proof of SSN or ineligibility for an SSN;ü The applicant’s address of principal residence; andü Lawful status in the United States.ü Company-issued Employee Identification Numberü Felony and Misdemeanor convictionsü Outstanding warrantü Terrorist Watch List• Applicants fingerprints will be collected electronically (ten flat or rolled)					

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

		<ul style="list-style-type: none"> • Applicants pin must be used to complete the transaction 					
EI-NEW v	IG: 28	<p><i>Medium Level - Non-Security Clearance Credential for Standard First Responder Designees Credential Identity Verification Requirements:</i></p> <ul style="list-style-type: none"> • Applicants must have a sponsor (authorizes the need for applicant to obtain physical and logical access to Federal facility) • Applicant must appear in person at Registration or Enrollment Station • Applicant must present 2 forms of Government issued ID Per US Form I-9 or 6 CFR Part 37 , one of which must have a photo. • Applicants fingerprints will be collected electronically index fingers for the sole purpose of tying the identity to the credential. • Applicant must appear in person • Applicant must present 2 forms of Government issued ID Per US Form I-9 or 6 CFR Part 37 , one of which must have a photo. Documents must include information supporting the claim of <ul style="list-style-type: none"> o Date of birth; o Proof of SSN or ineligibility for an SSN; o The applicant's address of principal residence; and o Lawful status in the United States. • Applicants fingerprints will be collected electronically (ten flat or rolled) for identity and adjudication purposes • Applicants pin must be used to complete the transaction 					

	EI- NEW w	IG: 32	<p><i>Medium High Level Clinical First Responder</i> credential issuers must adhere to the Fair Credit and Reporting Act (The FCRA) and other applicable laws, this is to inform all identified job skills/individuals that by giving their approval under the “Clinical Licensure Verification Requirement” and entering their personally identifiable data, they consent and authorize FIX’s and/or third party background screening provider(s) to perform qualifications screenings checks for them that “requires physical or logical access to their job or agency-related activity but do not fall under the category of government employee or government contractor. Must adherer to the Department of Health and Human Services Standard for Early System for Advanced Registration of Volunteer Health Professionals, Standards of the Joint Commission (JAHCO), and any applicable local, County or State Requirements</p>						
--	-----------------	--------	--	--	--	--	--	--	--

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

		Medium High Level Clinical First Responder Licensure Verification Requirements: <ul style="list-style-type: none"> • Applicant must appear in person • Applicant must present (dependent on profession); <ul style="list-style-type: none"> ◦ Original copy of a state issued medical license with no restrictions, and or active and unrestricted state issued license to practice with the scope identified by the state ◦ Original copy of MD. DO. PhD. MS. RN. Degree from an educational institution accredited by the authority having jurisdiction referenced under “evidence of credential – explanation of credential elements” from the emergency credentialing standard for that profession as defined in the HHS ESAR-VHP Standard. ◦ Original copy of the DEA Registration Certificate for License Verification ◦ Proof of Active Clinical practice through attestation or other documentation or peer reference from a credential holding peer (with ID reference), affirming that the individual is practicing medicine, or working within the scope of the profession being vetted, in a hospital or non hospital setting. ◦ Proof of Active Clinical Hospital Privileges through attestation or other documentation or peer reference from a credential holding peer (with ID reference) , affirming that the individual is practicing medicine, or works within the scope of the profession being vetted and has privileges in a hospital setting. ◦ Proof of State or National Certification to practice, under medical control, as a pre-hospital car provider • Applicants pin must be used to complete the transaction 						
FS - Fully Satisfied I - Interview	PS - Partially Satisfied D - Documentation Review	NS - Not Satisfied T - Test	O - Observe					Assessment Results
OR - FiXs Operating Rules Compliance Checklist				FS	0			
IG - FiXs Implementation Guidelines Checklist				PS	0			
				NS	0			
				Total	0			

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

ADJUDICATION PROCESS

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

Item	Req. Id	FiXs	Requirement					Assessment Result
				I	D	T	O	
1	AD-1	OR: 53	The organization conducts a National Agency Check with Written Inquiries (NACI), or other Office of Personnel Management (OPM) or National Security community investigation for each Applicant for whom a successfully adjudicated NACI cannot be referenced on file.					FS/PS/NS
			(i) the requirement that the organization conduct a National Agency Check with Written Inquiries (NACI), or other Office of Personnel Management (OPM) or National Security community investigation for each applicant for whom a successfully adjudicated NACI cannot be referenced on file is documented (review);		X			
			(ii) the organization conducts a National Agency Check with Written Inquiries (NACI), or other Office of Personnel Management (OPM) or National Security community investigation for each Applicant for whom a successfully adjudicated NACI cannot be referenced on file (interview).		X			
2	AD-2		The organization successfully adjudicates the FBI National Criminal History Check (fingerprint check) and initiates the National Agency Check with Written Inquires (NACI) before the FiXs Certified Credential Card is issued.					FS/PS/NS
			(i) the requirement that the organization successfully adjudicates the FBI National Criminal History Check (fingerprint check) and initiates the National Agency Check with Written Inquires (NACI) before the FiXs Certified Credential Card is issued is documented (review);		X			
			(ii) the organization successfully adjudicates the FBI National Criminal History Check (fingerprint check) and initiates the National Agency Check with Written Inquires (NACI) before the FiXs Certified Credential Card is issued (interview).	X				
	AD-NEW a	IG: 2	Once an Applicant's background check is completed, a trained Adjudicator [Privacy Official] must make a trustworthiness assessment of the Applicant prior to the Applicant being enrolled into a FiXs Domain Server.					

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

	AD-NEW b	IG : 6, 11	<p><i>High Level HSPD-12 Compatible Credential and High Level DoD LACS/PACS Credential Identity Vetting Requirements:</i></p> <ul style="list-style-type: none"> • NAC: <ul style="list-style-type: none"> ◦ Security/Suitability Investigations Index (SII) ◦ Defense Clearance and Investigations Index (DCII) ◦ FBI Name Check ◦ FBI National Criminal History Fingerprint Check • Written inquiries and searches of records: <ul style="list-style-type: none"> ◦ Employment, going back 5 years ◦ Education, going back 5 years and verifying highest degree ◦ Residence, going back 3 years ◦ References ◦ Law enforcement checks, going back 5 years 					
	AD-NEW c	IG: 7, 12, 17, 22	<p>No person shall be granted a <i>High Level HSPD-12 Compatible Credential, High Level DoD LACS/PACS Credential, and Medium High Level DoD and Commercial Use PACS/LACS Credential</i> if their background investigation reveals any of the following:</p> <ul style="list-style-type: none"> • Is, or is suspected of being, a terrorist; • Is the subject of an outstanding warrant; • Has deliberately omitted, concealed, or falsified relevant and material facts from any official form used to collect biographic information for the purpose of initiating a background check; • Has presented false or forged identity source documents; • Has been barred from Federal employment; • Is currently awaiting a hearing or trial or has been convicted of a crime punishable by imprisonment of six (6) months or longer; or • Is awaiting or servicing a form of pre-prosecution probation, suspended or deferred sentencing, probation or parole in conjunction with an arrest or criminal charges against the individual for a crime that is punishable by imprisonment of six (6) months or longer. 					

	AD-NEW d	IG: 16, 21	<p><i>Medium High Level DoD and Commercial Use PACS/LACS Credential Background Check Requirements:</i></p> <ul style="list-style-type: none"> • Terrorist watch list check • Law Enforcement checks, going back five (5) years • FBI Name Check • FBI National Criminal History Fingerprint Check 							
	AD-NEW e	IG: 25	<p><i>Medium High Level - Non-Security Clearance Credential for Enhanced First Responder Designees Identity Vetting Requirements:</i></p> <ul style="list-style-type: none"> • NAC I Commercial Equivalent Check (CEC). o FBI Name and FBI National Criminal History Fingerprint Check o Terrorist Watch List o Local Law Enforcement agency check o Residency verification • Written Inquires and Search of Records o Employment going back 5 years o Education going back 5 years o Residences going back 3 years (Note: Separately, all overseas addresses) o References (3 personal, non- relatives) 							

		No person shall be granted a <i>Medium High Level - Non-Security Clearance Credential for Enhanced First Responder Designees</i> if the background check reveals any of the following: <ul style="list-style-type: none"> • Is or is suspected of being a terrorist; • Has been charged or convicted under any provision of the Patriot Act • Is the subject of an outstanding warrant; • Has deliberately omitted, concealed, or falsified relevant or material facts from any official form used to collect biographic information for the purpose of initiating a background check; • Has presented false or forged identity documents; • Has a current Criminal (not civil) restraining order, or has had a criminal restraining order within the last five years, issued due to threat of violence or sexual assault • Is on the Sex Offenders List (level 2or 3) (in the last ten years level 2, life level 3) • Is currently awaiting a hearing or trial or has been convicted of a crime punishable by imprisonment of six (6) months or longer; or • Is awaiting or servicing a form of pre-prosecution probation; suspended or deferred sentencing, probation or parole in conjunction with an arrest or criminal charges against the individual for a crime that is punishable by imprisonment of six (6) months or longer. 				
AD-NEW f	IG: 26	<i>Medium Level - Non-Security Clearance Credential for Standard First Responder Designees Credential/ Identity Vetting Requirements:</i> <ul style="list-style-type: none"> • Establish validity of the identity - Identity proofing using administrative/manual methods providing identity proofing criteria from breeder documents required in Federal form I-9, to verify the identity exists, the identity is active (not deceased) and the components are related at a moderate level of assurance. • Criminal History Record Information (CHRI) / Risk Analysis (include a data quality score?) - to include Local, County, State as required by the laws governing the sponsoring authority 				

	AD-NEW h	IG: 30	The criteria used to adjudicate the background checks for persons requiring <i>Medium Level - Non-Security Clearance Credential for Standard First Responder Designees Credential</i> is determined by the State, County, and Local requirements and laws governing the sponsoring authority.							
	AD-NEW i	AG: 31	<i>Medium High Level Clinical First Responder Credential</i> must meet the requirements of Emergency System for Advanced Registration of Health Professions Volunteers. Title 42, Chapter 6A, Sub-Chapter II, Part B, § 247d-7b							
	AD-NEW j	AG: 34	<p><i>Medium High Level Clinical First Responder Licensure Vetting Requirements:</i></p> <ul style="list-style-type: none"> • May include, dependent on professional, but not be limited to • Primary Source Verification or delegation to a JCAHO accredited organization that has performed primary source verification of the individual's credentials. • Degree, MD or DO through AAMC, AOA or ECFMG; for all others from an accredited institution • Unencumbered Medical License from State of Issue • Board Certification in recognized specialty or sub specialty from ABMS or AOA • National Practitioner Databank Status • Drug Enforcement Agency (DEA) License Verification with types • Inspector General Status 							

	AD- NEW k	AG: 35	No person shall be granted a <i>Medium High Level Clinical First Responder Credential</i> if the licensure check reveals any of the following: <ul style="list-style-type: none"> • Any failure to meet any of the credential elements for the profession as outlined in the Department of Health and Human Services Health resources Services Administrations "Standards and Guidelines for the Early System for the Advanced Registration of Volunteer Healthcare Professionals. • Any Active Sanction on record with any State Inspector General • Any Active disciplinary issue on file with the National Practitioner Databank 									
FS - Fully Satisfied I - Interview	PS - Partially Satisfied D - Documentation Review	NS - Not Satisfied T - Test	O - Observe	Assessment Results	FS	0	PS	0	NS	0	Total	0

OR - FiXs Operating Rules Compliance Checklist
IG - FiXs Implementation Guidelines Checklist

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

CARD PRODUCTION PROCESS

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

Item	Req. Id		Requirement					Assessment Result		
1	CP-1		The FiXs Certified Credential Card implements security features that aid in reducing counterfeiting, are resistant to tampering, and provide visual evidence of tampering attempts.	I	D	T	O		FS/PS/NS	
			(i) the FiXs Certified Credential Card contains at least one security feature. Examples of these security features include the following: (i) Optical varying structures, (ii) Optical varying inks, (iii) Laser etching and engraving, (iv) Holograms, (v) Holographic images, (vi) Watermarks (interview, observe).	X			X			
2	CP-2		The FiXs Certified Credential Card is not embossed	I	D	T	O		FS/PS/NS	
			(i) the FiXs Certified Credential Card is not embossed (review, observe)		X		X			
3	CP-3		Decals are not adhered to the FiXs Certified Credential Card.	I	D	T	O		FS/PS/NS	
			(i) decals are not adhered to the FiXs Certified Credential Card (review, observe).		X		X			
4	CP-4		If organizations choose to punch an opening in the card body to enable the card to be worn on a lanyard, all such alterations are closely coordinated with the card vendor and/or manufacturer to ensure the card material integrity is not adversely impacted.	I	D	T	O		FS/PS/NS	
			(i) the integrity of a FiXs Certified Credential Card is not affected by a punched opening (test).			X				
			(ii) Documentation from the FiXs Certified Credential Card vendor shows that durability and operational requirements have not been compromised (review).		X					
	CP-NEW a	OR: 57	The organization must issue the Participant a valid FiXs Identifier that can be used to access the Participant's credentials. (Note 18)							

	CP-NEW b	The CA/ CMA provides Certificate Manufacturing: When notified by the FiXs CMS of a valid enrollment request, the CA/ CMA manufactures the requested certificate(s) for delivery to a FIPS 201 compliant card.					
	CP-NEW c	The CA/CMA provides Certificate Publishing: The CA/ CMA publishes it to a directory. The directory may be accessed via Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS) gateway or via the LDAP protocol.					
	CP-NEW d	The CA/CMA provides Encryption Key Storage: Optional storage of escrowed encryption keys.					
	CP-NEW e	The CA/CMA provides Key Recovery: If encryption key escrow is selected, a Key Recovery Practice Statement (KRPS) shall detail the escrow and recovery processes.					
	CP-NEW f	The CA/CMA provides Certificate Status information: In the form of Certificate Revocation Lists (CRLs) distribution and Online Certificate Status Protocol (OCSP) responses					
	CP-NEW g	Each CA that issues certificates to FiXs credentials shall have an approved CPS corresponding to one or more of the referenced CPs, for the appropriate level of assurance. A FiXs issuer shall only issue credentials with certificates that hold and assert the appropriate level of assurance as defined by this document.					
	CP-NEW h	Prior to issuance of certificates to a FiXs credential, the issuer will coordinate with the CA/ CMA to ensure that the procedures for authentication of personnel are documented in a Registration Practice Statement (RPS) and comply with the appropriate CP, and submitted to FiXs for approval.					

	CP-NEW i	IG: 9	<i>High Level DoD LACS/PACS Credential, Medium High Level DoD and Commercial Use PACS/LACS Credential, Medium High Level - Non-Security Clearance Contractor and Commercial Use</i> must capture the contract number under which the FiXs Member Company (or subscriber) employee requires access to DoD resources, and reference to any existing security clearance an Applicant might have.						
	CP-NEW j	IG: 36	A color photograph (minimum of 300 dots per inch (dpi) resolution), presenting the individual from the top of the head to the shoulders, is to be placed in the upper left corner of the front of the FiXs Certified Credential card, vertically. Must be in Zone 1 of the front of the card.						
	CP-NEW k	IG: 37	For all color photographs, the background color should be uniform throughout an organization's issuance locations						
	CP-NEW l	IG: 38	Complete and specific technical requirements for facial image capturing should conform to NIST Special Publication (SP) 800-76, Biometric Data Specification for Personal Identity Verification.						
	CP-NEW m	IG: 39	The full legal name of the FiXs Certified Credential card holder's identity is to be printed under the photograph in capital letters. The minimum font size acceptable is 10 point. Must be in Zone 2 of the front of the card.						
	CP-NEW n	IG: 40	The FiXs Certified Credential card holder's affiliation shall be printed in Zone 8 of the front of the card. The required font for the card holder's affiliation is 6 point Bold.						
	CP-NEW o	IG: 41	The FiXs Certified Credential card holder's organization name shall be printed in Zone 10 of the front of the card. Two lines are available for use, with 6 point Bold being the font requirement.						
	CP-NEW p	IG: 42	The FiXs Certified Credential card expiration date is to be printed in a YYYYMMDD format (example: 2007MAR30) in Zone 14 of the front of the card. The expiration date is to be printed in 6 point Bold.						

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

	CP-NEW q	IG: 43	The unique serial number from the agency/organization shall be placed in Zone 1 of the back of the FiXs Certified Credential card. This serial number will be required to be printed in 6 point Bold, left-justified.					
	CP-NEW r	IG: 44	Issuer information shall be placed in Zone 2 of the back of the FiXs Certified Credential card and printed in 6 point Bold and right-justified.					
	CP-NEW s	IG: 45	The printed information on the FiXs Certified Credential card shall be printed so that the print cannot be rubbed off the actual card material through printing, laminating, and during normal wear and tear throughout the card's life cycle.					
	CP-NEW t	IG: 46	The print on the FiXs Certified Credential card is not to be obscured by any images					
	CP-NEW u	IG: 47	No manual markings or embossing (unless done during manufacture of the card itself by the manufacturer) are allowed on FiXs Certified Credential cards.					
	CP-NEW v	IG: 48	No decals or stickers of any type are to be affixed to the FiXs Certified Credential card.					
	CP-NEW w	IG: 49	No manual markings or embossing (unless done during manufacture of the card itself by the manufacturer) are allowed on PIV cards.					
	CP-NEW x	IG: 50	Contactless FiXs Certified Credential cards shall be compatible with ISO7819					
	CP-NEW y	IG: 51	Contactless FiXs Certified Credential cards shall be compatible with ISO10373					
	CP-NEW z	IG: 52	Contactless FiXs Certified Credential cards shall be compatible with ISO7816					
	CP-NEW aa	IG: 53	Contactless cards FiXs Certified Credential shall be compatible with ISO14443					

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

	CP-NEW bb	IG: 54	<p>FiXs Certified Credential cards should conform to test methods used in ANSI322 regarding:</p> <ul style="list-style-type: none"> • Card flexure • Static stress • Plasticizer exposure • Impact resistance • Card structural integrity • Surface abrasion • Temperature and humidity-induced dye migration • Ultraviolet light exposure • Laundry tests 					
	CP-NEW cc	IG: 55	FiXs Certified Credential card must be able to withstand up to 2000 hours of southwestern United States sunlight exposure (actual, concentrated, or artificial), as stipulated in ISO 10373					
	CP-NEW dd	IG: 56	All FiXs Certified Credential cards shall meet testing requirements in [G90-98] for concentrated sunlight exposure and [G155-00] for accelerated exposure.					
	CP-NEW ee	IG: 57	FiXs Certified Credential cards must be able to withstand using a mild soap and water mixture. This should not cause the PIV card to malfunction, nor should it cause the laminate to peel.					
	CP-NEW ff	IG: 58	Per ISO 10373, no visible cracks or failures should be experienced following dynamic bending of the FiXs Certified Credential cards.					
	CP-NEW gg	IG: 59	FiXs Certified Credential cards must be 27 to 33-mil thick (prior to lamination).					
	CP-NEW hh	IG: 60	Hole punching of the FiXs Certified Credential card shall not be done in text and photo areas and any zones that feature machine-readable technology					
	CP-NEW ii	IG: 61	All security features used on a FiXs Certified Credential card must be in accordance with durability requirements in ISO7810.					

	CP-NEW jj	IG: 62	All security features of the FiXs Certified Credential card must be free of defects, such as fading, discoloring, or tampering.								
	CP-NEW kk	IG: 63	Printed security information on the FiXs Certified Credential is to be legible and not obscured by any images whatsoever.								
	CP-NEW II	IG: 64	Electronic contact points on the FiXs Certified Credential card are to be free from printing zones, so that data can be read and written without impediment.								
	CP-NEW mm	IG: 65	<p>All FiXs Certified Credential cards are required to have at least one of the following security features(Note 2):</p> <ul style="list-style-type: none"> - Optical Varying Structures - Optical Varying Inks - Laser Etching and Engraving - Holograms - Holographic Images - Watermarks - Personal Identification Number - Card Holder Unique Identifier - Biometrics - Encryption 								

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

		The FiXs barcode will consist of the following data elements (in order): <ol style="list-style-type: none"> 1. Agency Code (within the FASC-N) will be assigned a value, 9999, to indicate that the card has been issued by a non-Federal issuer; 2. System Code (within the FASC-N) will be assigned a unique number ranging between 1 and 9999 to identify the FiXs enrollment and/or issuance system used by a FiXs member organization; 3. Credential Number (within the FASC-N) will be assigned a unique number ranging between 1 and 999,999 to identify the individual credential issued by a particular FiXs enrollment and/or issuance system used by a FiXs member organization; 4. Credential Series (Series Code) - within the FASC-N - will initially be assigned a value, 1, to indicate the first series and incremented up to 9 for additional series; 5. Individual Credential Issue (Credential Code) - within the FASC-N - should always be assigned a value, 1, as recommended by PACS Version 2.3; 6. Organization Category (within the FASC-N) will be assigned a value, 3, to indicated that the card issuer is a commercial organization; 7. Organization Identifier (within the FASC-N) will be assigned a value between 1 and 9999 to identify the lower sixteen bits of the FiXs member's organization identifier; 				
--	--	---	--	--	--	--

FS - Fully Satisfied

I - Interview

PS - Partially Satisfied

D - Documentation Review

NS - Not Satisfied

T - Test

O - Observe

Assessment Results

FS 0

PS 0

NS 0

Total 0

OR - FiXs Operating Rules Compliance Checklist

IG - FiXs Implementation Guidelines Checklist

CARD ACTIVATION/ISSUANCE PROCESS

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

Item	Req-Id	FiXs	Requirement					Assessment Result	
				I	D	T	O		
1	AI-1		The personalized FiXs Certified Credential Card complies with all the mandatory items on the front of the FiXs Certified Credential Card. Card complies with FiXs Implementation Guidelines Appendix A Smart Card Topology Requirements						FS/PS/NS
			(i) the FiXs Certified Credential Card meets specific requirements in FiXs Implementation Guidelines Appendix A Smart Card Topology Requirements for (i) photograph; (ii) name; (iii) employee; affiliation; (iv) and expiration date. Card complies with FiXs Implementation Guidelines Appendix A Smart Card Topology Requirements (observe).				X		
2	AI-2		The personalized FiXs Certified Credential Card complies with all the mandatory items on the back of the FiXs Certified Credential Card. Card complies with FiXs Implementation Guidelines Appendix A Smart Card Topology Requirements.						FS/PS/NS
			(i) the FiXs Certified Credential Card meets specific requirements in FiXs Implementation Guidelines for (i) organization card serial number; (ii) and issuer identification. Card complies with FiXs Implementation Guidelines Appendix A Smart Card Topology Requirements (observe).				X		
3	AI-3		If one or more optional items are printed on the front of the FiXs Certified Credential Card, they comply with the requirements for the optional items on the front on the FiXs Certified Credential Card.						FS/PS/NS

			(i) the FiXs Certified Credential Card meets specific requirements in FIPS 201-1 if it includes optional items on the front of the card such as (i) signature; (ii) organization specific text area; (iii) rank; (iv) portable data file; (v) header; (vi) organization seal; (vii) footer; (viii) issue date; (ix) color-coding employee affiliation; (x) photo border for employee affiliation; (xi) organization specific data (observe).				X		
4	AI-4		If one or more optional items are printed on the back of the FiXs Certified Credential Card, they comply with the requirements for the optional items on the back on the FiXs Certified Credential Card.	I	D	T	O		FS/PS/NS
			(i) the FiXs Certified Credential Card meets specific requirements in FIPS 201-1 if it includes optional items on the front of the card such as (i) magnetic stripe; (ii) return to; (iii) physical characteristics of cardholder; (iv) additional language for emergency responder officials; (v) standard Section 499, Title 18 language; (vi) linear 3 of 9 bar code; (vii) organization specific text (zones 9 & 10) (observe).				X		
5	AI-5		The FiXs Certified Credential Card includes mechanisms to limit the number of PIN guesses an adversary can attempt if a card is lost or stolen.	I	D	T	O		FS/PS/NS
			(i) the FiXs Certified Credential Card limits the number of incorrect PIN guesses (test).			X			
6	AI-6	IG: APA	The FiXs Certified Credential Card is valid for no more than five years.	I	D	T	O		FS/PS/NS

			(i) the expiration date printed on the FiXs Certified Credential Card is no more than five years from the issuance date (observe, test).		X			
			(ii) the expiration date is printed in the CHUID (test)		X			
			(iii) the two dates (printed on the card and the expiration date in the CHUID) are the same (test)		X			
7	AI-7		The Credential Issuer Facility performs a 1:1 biometric match of the applicant against the biometric included in the FiXs Certified Credential Card or in the FiXs Certified Credential enrollment record before releasing the FiXs Certified Credential Card to the applicant.	I	D	T	O	FS/PS/NS
			(i) the requirement that the issuer performs a 1:1 biometric match of the applicant against the biometric included in the FiXs Certified Credential Card or in the FiXs Certified Credential enrollment record is documented (review);		X			
			(ii) the issuer performs a 1:1 biometric match of the applicant against the biometric included in the FiXs Certified Credential Card or in the FiXs Certified Credential enrollment record (observe).				X	
8	AI-8		The Credential Issuer Facility performs a 1:1 biometric match of the FiXs Certified Credential Card holder against the biometric included in the FiXs Certified Credential Card or in the FiXs Certified Credential enrollment record prior to renewal.	I	D	T	O	FS/PS/NS

			(i) the requirement that the Credential Issuer Facility performs a 1:1 biometric match of the FiXs Certified Credential Card holder against the biometric included in the FiXs Certified Credential Card or in the FiXs Certified Credential enrollment record prior to renewal is documented (review);	X				
			(ii) the Credential Issuer Facility performs a 1:1 biometric match of the FiXs Certified Credential Card holder against the biometric included in the FiXs Certified Credential Card or in the FiXs Certified Credential enrollment record prior to renewal (observe).			X		
9	AI-9		The Credential Issuer Facility advises applicants that the PIN on the FiXs Certified Credential Card should not be easily-guess-able or otherwise individually-identifiable in nature.	I	D	T	O	FS/PS/NS
			(i) the requirement that the Credential Issuer Facility advises applicants that the PIN on the FiXs Certified Credential Card should not be easily-guess-able or otherwise individually-identifiable in nature is documented (review);		X			
			(ii) the Credential Issuer Facility advises applicants that the PIN on the FiXs Certified Credential Card should not be easily-guess-able or otherwise individually-identifiable in nature (observe).				X	
10	AI-10		Identity cards issued to individuals without a completed NACI or equivalent are electronically distinguishable from identity cards issued to individuals who have a completed investigation	I	D	T	O	FS/PS/NS
			(i) the Credential Issuer Facility has procedures for how to update the NACI interim indicator extension for identity cards issued to individuals without a completed NACI or equivalent (review, interview);	X	X			

			(ii) for individuals without a completed NACI or equivalent, the NACI interim indicator is set to true (test);		X			
			(iii) for individuals with a completed NACI or equivalent, the NACI interim indicator is set to false (test).		X			
11	AI-11		During a PIN reset on a locked FiXs Certified Credential Card, the Credential Issuer Facility performs a 1:1 biometric match of the FiXs Certified Credential Card holder against the biometric included in the FiXs Certified Credential Card prior to releasing the unlocked FiXs Certified Credential Card back to the Card holder.	I	D	T	O	FS/PS/NS
			(I) the requirement that after PIN reset on the FiXs Certified Credential Card, the Credential Issuer Facility performs a 1:1 biometric match of the FiXs Certified Credential Card holder against the biometric included in the FiXs Certified Credential Card or in the FiXs Certified Credential enrollment record before releasing the FiXs Certified Credential Card is documented (review);		X			
			(ii) after PIN reset on the FiXs Certified Credential Card, the Credential Issuer Facility performs a 1:1 biometric match of the FiXs Certified Credential Card Holder against the biometric included in the FiXs Certified Credential Card or in the FiXs Certified Credential enrollment record before releasing the FiXs Certified Credential Card (observe).				X	
12	AI-12		The Credential Issuer Facility issues an electro-magnetically opaque sleeve or other technology to protect against any unauthorized contactless access to information stored on a FiXs Certified Credential.	I	D	T	O	FS/PS/NS

			(i) the requirement that the Credential Issuer Facility issue an electro-magnetically opaque sleeve with every FiXs Certified Credential Card is documented (review);	X					
			(ii) the Credential Issuer Facility issues an electro-magnetically opaque sleeve with every FiXs Certified Credential Card (interview, observe).	X			X		
AI-13			The organization verifies that the FiXs Certified Credential cardholder remains in good standing, and personnel records are current before renewing/reissuing the card and associated credentials.	I	D	T	O		FS/PS/NS
			(i) the procedures that are followed to determine that the cardholder's records are current are documented (review);		X				
			(ii) the procedures to determine the currency of the cardholder's records are followed by the Credential Issuer facility prior to renewal or reissuance of a FiXs Certified Credential Card (observe)				X		
FS - Fully Satisfied I - Interview			PS - Partially Satisfied D - Documentation Review			NS - Not Satisfied T - Test			Assessment Results FS 0 PS 0 NS 0 Total 0
OR - FiXs Operating Rules Compliance Checklist IG - FiXs Implementation Guidelines Checklist									

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

MAINTENANCE PROCESS

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

Item	Req-Id	FiXs	Requirement					Assessment Result	
1	MP-1		The FiXs Certified Credential FASC-N is not modified post-issuance.	I	D	T	O		FS/PS/NS
			(i) the FiXs Certified Credential FASC-N is not modified post-issuance (review, interview).	X	X				
2	MP-2		In the case of a renewal, re-issuance and termination, the FiXs Certified Credential Card is collected and destroyed whenever possible.	I	D	T	O		FS/PS/NS
			(i) the requirement that in the case of a renewal, re-issuance and termination, the FiXs Certified Credential Card is collected and destroyed whenever possible is documented (review);				X		
			(ii) in the case of a renewal, re-issuance and termination, the FiXs Certified Credential Card is collected and destroyed whenever possible (interview).						
3	MP-3		Normal operational procedures must be in place to ensure proper card revocation during FiXs Certified Credential Card re-issuance and termination: (i) The FiXs Certified Credential Card itself is revoked; (ii) Databases containing Federal Agency Smart Credential Number (FASC-N) values must be updated to reflect the change in status; (iii); and (iv) Online Certificate Status Protocol (OCSP) responders are updated so that queries with respect to certificates on the FiXs Certified Credential Card are answered appropriately.	I	D	T	O		FS/PS/NS
			(i) during card revocation the FiXs Certified Credential Card is revoked (review, interview);	X	X				
			(ii) databases containing Federal Agency Smart Credential Number (FASC-N) values must be updated to reflect the change in status (interview);	X					

			(iii) the CA is informed and the certificates on the FiXs Certified Credential Card are revoked (test);		X			
			(iv) online Certificate Status Protocol (OCSP) responders are updated (test, review).		X	X		
4	MP-4		If the FiXs Certified Credential Card cannot be collected and destroyed, normal operating procedures are completed within 18 hours of notification.	I	D	T	O	FS/PS/NS
			(i) the requirement that FiXs Certified Credential Card cannot be collected and destroyed, normal operating procedures are completed within 18 hours of notification is documented (review);		X			
			(ii) if the FiXs Certified Credential Card cannot be collected and destroyed, normal operating procedures are completed within 18 hours of notification (observe).				X	
5	MP-5		Upon FiXs Certified Credential Card termination, the organization enforces a standard methodology of updating systems of records to indicate employee termination and this status is replicated throughout relying systems used for physical and logical access to organization facilities and resources.	I	D	T	O	FS/PS/NS
			(i) the Credential Issuer Facility has documented its procedures for updating information systems to indicate employee termination (review);		X			
			(ii) the Credential Issuer Facility updates information systems to indicate employee termination (interview, observe).	X			X	
6	MP-6		The organization posts a quarterly report, stating the number of FiXs Certified Credential Cards issued to date, to the organization's website and the link is emailed to FiXs organization and applicable OMB parties.	I	D	T	O	FS/PS/NS

			(i) the organization develops and post a quarterly report to the organization's website according to the requirements of the attachment to OMB memorandum 07-06 or FiXs provided format (review);	X													
			(ii) the organization the report to FiXs (and OMB if required) on a quarterly basis (review, interview).	X	X												
7	MP-7		The organization has completed a life-cycle walk-through at one-year intervals since the last accreditation date and the results are documented in a report to the FiXs Organization Authorizing Official.	I	D	T	O		FS/PS/NS								
			(i) the organization has completed a life-cycle walk-through to cover sponsorship, enrollment/identity proofing, card production, card activation/issuance and maintenance processes (interview);	X													
			(ii) a life-cycle walk-through has been completed at one year intervals since the last accreditation date (interview);	X													
			(iii) the results of the Credential Issuer life-cycle walk-through have been documented and reviewed by the FiXs Organization Authorizing Official (review, interview).	X		X											
FS - Fully Satisfied I - Interview			PS - Partially Satisfied D - Documentation Review			NS - Not Satisfied T - Test			Assessment Results <table border="1" style="margin-left: auto; margin-right: auto;"> <tr><td>FS</td><td>0</td></tr> <tr><td>PS</td><td>0</td></tr> <tr><td>NS</td><td>0</td></tr> <tr><td>Total</td><td>0</td></tr> </table>	FS	0	PS	0	NS	0	Total	0
FS	0																
PS	0																
NS	0																
Total	0																
OR - FiXs Operating Rules Compliance Checklist																	
IG - FiXs Implementation Guidelines Checklist																	

Copyright© 2008
 Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)



The Federation for Identity and
Cross-Credentialing Systems®

Appendix C

FiXS PIV Approval to Operate (ATO) Application

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXS®)

Appendix TBD

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)



The Federation for Identity and
Cross-Credentialing Systems®

Appendix D

FiXs Baseline Security Assessment Checklist

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

This checklist should be used to describe the security policies, processes, procedures and features which have been implemented, documented, and incorporated into the nominated information system. This checklist along with the FiXs ATO Application, Draft SSP, Risk Assessment Report, and PAO&M must be submitted as part of the nominated system's Security Baseline Documentation.

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

RISK ASSESSMENT

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

Item	Control	Requirement	Status	Justification/Comments
1		The organization develops, disseminates, and periodically reviews/updates:	I/NI/P/NA/AR	
	RA-1	(i) a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, and compliance		
		(ii) formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.		
2			I/NI/P/NA/AR	
	RA-2	The organization categorizes the information system and the information processed, stored, or transmitted by the system in accordance with FIPS 199 and documents the results (including supporting rationale) in the system security plan. Designated senior-level officials within the organization review and approve the security categorizations		
3			I/NI/P/NA/AR	
	RA-3	The organization conducts assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency.		
4			I/NI/P/NA/AR	
	RA-4	The organization updates the risk assessment every three years or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system.		

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

5			I/NI/P/NA/AR	
	RA-5	Vulnerability Scanning: Using appropriate vulnerability scanning tools and techniques, the organization scans for vulnerabilities in the information system every six months or when significant new vulnerabilities affecting the system are identified and reported.		
	RA-5.1	Vulnerability scanning tools include the capability to readily update the list of vulnerabilities scanned		
	RA-5.2	Vulnerability Scanning: The organization updates the list of information system vulnerabilities every six months or when significant new vulnerabilities are identified and reported.		
	RA-5.3	Vulnerability scanning procedures include means to ensure adequate scan coverage, both vulnerabilities checked and information system components scanned		

Assessment Results	
I	0
NI	0
P	0
NA	0
AR	0
TOTAL	0

LEGEND
I = Implemented
NI = Not Implemented
P = Partially Implemented
NA = Not Applicable
AR = Accepting Risk

PLANNING

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

Item	Control	Requirement	Status	Justification/Comments
1		The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security planning policy that addresses purpose, scope, roles, responsibilities, and compliance (ii) formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.	I/NI/P/NA/AR	
2	PL-1		I/NI/P/NA/AR	
2	PL-2	The organization develops and implements a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization review and approve the plan.	I/NI/P/NA/AR	
3	PL-3	The organization reviews the security plan for the information system annually and revises the plan to address system/organizational changes or problems identified during plan implementation or security control assessments.	I/NI/P/NA/AR	
4	PL-4	The organization establishes and makes readily available to all information system users a set of rules that describes their responsibilities and expected behavior with regard to information system usage. The organization receives signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system.	I/NI/P/NA/AR	
5	PL-5	The organization conducts a privacy impact assessment on the information system.	I/NI/P/NA/AR	

Assessment Results	
I	0
NI	0
P	0
NA	0
AR	0
TOTAL	0

LEGEND
I = Implemented
NI = Not Implemented
P = Partially Implemented
NA = Not Applicable
AR = Accepting Risk

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

SYSTEM & SERVICES ACQUISITION

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

Item	Control	Requirement	Status	Justification/Comments
1			I/NI/P/NA/AR	
	SA-1	Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.		
2			I/NI/P/NA/AR	
	SA-2	The organization determines, documents, and allocates as part of its capital planning and investment control process the resources required to adequately protect the information system.		
3			I/NI/P/NA/AR	
	SA-3	The organization manages the information system using a system development life cycle methodology that includes information security considerations.		
4			I/NI/P/NA/AR	
	SA-4	The organization includes security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk.		
5			I/NI/P/NA/AR	
	SA-5	The organization ensures that adequate documentation for the information system and its constituent components is available, protected when required, and distributed to authorized personnel.		
	SA-5.1	The organization includes documentation describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.		

	SA-5.2	The organization includes documentation describing the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components).		
6			I/NI/P/NA/AR	
	SA-6	The organization complies with software usage restrictions.		
7			I/NI/P/NA/AR	
	SA-7	The organization enforces explicit rules governing the downloading and installation of software by users.		
8			I/NI/P/NA/AR	
	SA-8	The organization designs and implements the information system using security engineering principles.		
9			I/NI/P/NA/AR	
	SA-9	The organization ensures that third-party providers of information system services employ adequate security controls in accordance with applicable federal laws, directives, policies, regulations, standards, guidance, and established service level agreements. The organization monitors security control compliance.		
10			I/NI/P/NA/AR	
	SA-10	The information system developer creates and implements a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation.		

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

11			I/NI/P/NA/AR	
	SA-11	The information system developer creates a security test and evaluation plan, implements the plan, and documents the results. Developmental security test results may be used in support of the security certification and accreditation process for the delivered information system.		

Assessment Results	
I	0
NI	0
P	0
NA	0
AR	0
TOTAL	0

LEGEND

I = Implemented
 NI = Not Implemented
 P = Partially Implemented
 NA = Not Applicable
 AR = Accepting Risk

CERTIFICATION & ACCREDITATION

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

Item	Control	Requirement	Status	Justification/Comments
1		The organization develops, disseminates, and periodically reviews/updates:	I/NI/P/NA/AR	
	CA-1	(i) formal, documented, security assessment and certification and accreditation policies that address purpose, scope, roles, responsibilities, and compliance.		
		(ii) formal, documented procedures to facilitate the implementation of the security assessment and certification and accreditation policies and associated assessment, certification, and accreditation controls.		
2			I/NI/P/NA/AR	
	CA-2	The organization conducts an assessment of the security controls in the information system annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.		
3			I/NI/P/NA/AR	
	CA-3	The organization authorizes all connections from the information system to other information systems outside of the accreditation boundary and monitors/controls the system interconnections on an ongoing basis. Appropriate organizational officials approve information system interconnection agreements.		
4			I/NI/P/NA/AR	
	CA-4	The organization conducts an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.		
5			I/NI/P/NA/AR	

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

	CA-5	The organization develops and updates quarterly, a plan of action and milestones for the information system that documents the organization's planned, implemented, and evaluated remedial actions to correct any deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.		
6			I/NI/P/NA/AR	
	CA-6	The organization authorizes (i.e., accredits) the information system for processing before operations and updates the authorization every 3 years. A senior organizational official signs and approves the security accreditation.		
7			I/NI/P/NA/AR	
	CA-7	The organization monitors the security controls in the information system on an ongoing basis.		

Assessment Results	
I	0
NI	0
P	0
NA	0
AR	0
TOTAL	0

LEGEND
I = Implemented
NI = Not Implemented
P = Partially Implemented
NA = Not Applicable
AR = Accepting Risk

PERSONNEL SECURITY

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

Item	Control	Requirement	Status	Justification/Comments
1		The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, personnel security policy that addresses purpose, scope, roles, responsibilities, and compliance. (ii) formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.	I/NI/P/NA/AR	
2	PS-1		I/NI/P/NA/AR	
3	PS-2	The organization assigns a risk designation to all positions and establishes screening criteria for individuals filling those positions. The organization reviews and revises position risk designations periodically in accordance with OPM guidance.	I/NI/P/NA/AR	
4	PS-3	The organization screens individuals requiring access to organizational information and information systems before authorizing access.	I/NI/P/NA/AR	
5	PS-4	When employment is terminated, the organization terminates information system access, conducts exit interviews, ensures the return of all organizational information system-related property (e.g., keys, identification cards, building passes), and ensures that appropriate personnel have access to official records created by the terminated employee that are stored on organizational information systems.	I/NI/P/NA/AR	
	PS-5	The organization reviews information systems/facilities access authorizations when individuals are reassigned or transferred to other positions within the organization and initiates appropriate actions (e.g., reissuing keys, identification cards, building passes; closing old accounts and establishing new accounts; and changing system access authorizations).	I/NI/P/NA/AR	

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

6			I/NI/P/NA/AR	
	PS-6	The organization completes appropriate access agreements (e.g., nondisclosure agreements, acceptable use agreements, rules of behavior, conflict-of-interest agreements) for individuals requiring access to organizational information and information systems before authorizing access.		
7			I/NI/P/NA/AR	
	PS-7	The organization establishes personnel security requirements for third-party providers (e.g., service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, network and security management) and monitors provider compliance to ensure adequate security.		
8			I/NI/P/NA/AR	
	PS-8	The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.		

Assessment Results	
I	0
NI	0
P	0
NA	0
AR	0
TOTAL	0

LEGEND
I = Implemented
NI = Not Implemented
P = Partially Implemented
NA = Not Applicable
AR = Accepting Risk

PHYSICAL & ENVIRONMENTAL PROTECTION

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

Item	Control	Requirement	Status	Justification/Comments
1		The organization develops, disseminates, and periodically reviews/updates:	I/NI/P/NA/AR	
	PE-1	(i) a formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, and compliance.		
		(ii) formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.		
2			I/NI/P/NA/AR	
	PE-2	The organization develops and keeps current lists of personnel with authorized access to facilities containing information systems (except for those areas within the facilities officially designated as publicly accessible) and issues appropriate authorization credentials (e.g., badges, identification cards, smart cards). Designated officials within the organization review and approve the access list and authorization credentials once a year.		
3			I/NI/P/NA/AR	
	PE-3	The organization controls all physical access points (including designated entry/exit points) to facilities containing information systems (except for those areas within the facilities officially designated as publicly accessible) and verifies individual access authorizations before granting access to the facilities. The organization also controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.		

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

4			I/NI/P/NA/AR	
	PE-4	The organization controls physical access to information system transmission lines carrying unencrypted information to prevent eavesdropping, intransit modification, disruption, or physical tampering.		
5			I/NI/P/NA/AR	
	PE-5	The organization controls physical access to information system devices that display information to prevent unauthorized individuals from observing the display output.		
6			I/NI/P/NA/AR	
	PE-6	The organization monitors physical access to information systems to detect and respond to incidents. The organization monitors real-time intrusion alarms and surveillance equipment. The organization employs automated mechanisms to ensure potential intrusions are recognized and appropriate response actions initiated.		
	PE-6.1	The organization monitors real-time intrusion alarms and surveillance equipment.		
	PE-6.2	The organization employs automated mechanisms to ensure potential intrusions are recognized and appropriate response actions initiated.		
7			I/NI/P/NA/AR	
	PE-7	The organization controls physical access to information systems by authenticating visitors before authorizing access to facilities or areas other than areas designated as publicly accessible.		

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

	PE-7.1	The organization escorts visitors and monitors visitor activity, when required.		
8		The organization maintains a visitor access log to facilities (except for those areas within the facilities officially designated as publicly accessible. Visitor logs are reviewed at closeout, maintained on file, and available for further review for one year) that includes:	I/NI/P/NA/AR	
	PE-8	(i) name and organization of the person visiting		
		(ii) signature of the visitor		
		(iii) form of identification		
		(iv) date of access		
		(v) time of entry and departure		
		(vi) purpose of visit		
		(vii) name and organization of person visited		
	PE-8.1	The organization employs automated mechanisms to facilitate the maintenance and review of access logs.		
9			I/NI/P/NA/AR	
	PE-9	The organization protects power equipment and power cabling for the information system from damage and destruction.		
	PE-9.1	The organization employs redundant and parallel power cabling paths.		

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

10			I/NI/P/NA/AR	
	PE-10	For specific locations within a facility containing concentrations of information system resources (e.g., data centers, server rooms, mainframe rooms), the organization provides the capability of shutting off power to any information technology component that may be malfunctioning (e.g., due to an electrical fire) or threatened (e.g., due to a water leak) without endangering personnel by requiring them to approach the equipment.		
11			I/NI/P/NA/AR	
	PE-11	The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss. The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.		
	PE-11.1	The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.		
	PE-11.2	The organization provides a long-term alternate power supply for the information system that is selfcontained and not reliant on external power generation.		
12			I/NI/P/NA/AR	

	PE-12	The organization employs and maintains automatic emergency lighting systems that activate in the event of a power outage or disruption and that cover emergency exits and evacuation routes.		
13			I/NI/P/NA/AR	
	PE-13	The organization employs and maintains fire suppression and detection devices/systems that can be activated in the event of a fire.		
	PE-13.1	Fire suppression and detection devices/systems activate automatically in the event of a fire.		
	PE-13.2	Fire suppression and detection devices/systems provide automatic notification of any activation to the organization and emergency responders.		
14			I/NI/P/NA/AR	
	PE-14	The organization regularly maintains within acceptable levels and monitors the temperature and humidity within facilities containing information systems.		
15			I/NI/P/NA/AR	
	PE-15	The organization protects the information system from water damage resulting from broken plumbing lines or other sources of water leakage by ensuring that master shutoff valves are accessible, working properly, and known to key personnel.		
	PE-15.1	The organization employs automated mechanisms to automatically close shutoff valves in the event of a significant water leak.		
16			I/NI/P/NA/AR	

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

	PE-16	The organization controls information system-related items (i.e., hardware, firmware, software) entering and exiting the facility and maintains appropriate records of those items		
17			I/NI/P/NA/AR	
	PE-17	Individuals within the organization employ appropriate information system security controls at alternate work sites.		

Assessment Results	
I	0
NI	0
P	0
NA	0
AR	0
TOTAL	0

LEGEND

I = Implemented
 NI = Not Implemented
 P = Partially Implemented
 NA = Not Applicable
 AR = Accepting Risk

CONTINGENCY PLANNING

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

Item	Control	Requirement	Status	Justification/Comments
1		The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, and compliance.	I/NI/P/NA/AR	
	CP-1	(ii) formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.		
2			I/NI/P/NA/AR	
	CP-2	The organization develops and implements a contingency plan for the information system addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. Designated officials within the organization review and approve the contingency plan and distribute copies of the plan to key contingency personnel.		
	CP2.1	The organization coordinates contingency plan development with organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan).		
3			I/NI/P/NA/AR	
	CP-3	The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training annually.		
	CP-3.1	The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.		

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

	CP-3.2	The organization employs automated mechanisms to provide a more thorough and realistic training.		
4			I/NI/P/NA/AR	
	CP-4	The organization tests the contingency plan for the information system at least annually using to determine the plan's effectiveness and the organization's readiness to execute the plan. System rated as high shall be tested at the alternate processing site. Appropriate officials within the organization review the contingency plan test results and initiate corrective actions.		
	CP-4.1	The organization coordinates contingency plan testing with organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan).		
	CP-4.2	The organization tests the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations.		
	CP-4.3	The organization employs automated mechanisms to more thoroughly and effectively test the contingency.		
5			I/NI/P/NA/AR	
	CP-5	The organization reviews the contingency plan for the information system once per year and revises the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.		
6			I/NI/P/NA/AR	

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

	CP-6	The organization identifies an alternate storage site and initiates necessary agreements to permit the storage of information system backup information. The alternate storage site is geographically separated from the primary storage site so as not to be susceptible to the same hazards.		
	CP-6.1	The alternate storage site is geographically separated from the primary storage site so as not to be susceptible to the same hazards.		
	CP-6.2	The alternate storage site is configured to facilitate timely and effective recovery operations.		
	CP-6.3	The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.		
7			I/NI/P/NA/AR	
	CP-7	The organization identifies an alternate processing site and initiates necessary agreements to permit the resumption of information system operations for critical mission/business functions within 24 hours when the primary processing capabilities are unavailable.		
	CP-7.1	The alternate processing site is geographically separated from the primary processing site so as not to be susceptible to the same hazards.		
	CP-7.2	The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.		
	CP-7.3	Alternate processing site agreements contain priority of-service provisions in accordance with the organization's availability requirements.		

	CP-7.4	The alternate processing site is fully configured to support a minimum required operational capability and ready to use as the operational site.		
8			I/NI/P/NA/AR	
	CP-8	The organization identifies primary and alternate telecommunications services to support the information system and initiates necessary agreements to permit the resumption of system operations for critical mission/business functions within 24 hours when the primary telecommunications capabilities are unavailable.		
	CP-8.1	Primary and alternate telecommunications service agreements contain priority-of-service provisions in accordance with the organization's availability requirements.		
	CP-8.2	Alternate telecommunications services do not share a single point of failure with primary telecommunications services.		
	CP-8.3	Alternate telecommunications service providers are sufficiently separated from primary service providers so as not to be susceptible to the same hazards.		
	CP-8.4	Primary and alternate telecommunications service providers have adequate contingency plans.		
9			I/NI/P/NA/AR	
	CP-9	The organization conducts backups of user-level and system-level information (including system state information) contained in the information system according to backup schedules documented in the system contingency plan and stores backup information at an appropriately secured location.		

	CP-9.1	The organization conducts backups of user-level and system-level information (including system state information) contained in the information system according to backup schedules documented in the system contingency plan and stores backup information at an appropriately secured location.		
	CP-9.2	The organization selectively uses backup information in the restoration of information system functions as part of contingency plan testing.		
	CP-9.3	The organization stores backup copies of the operating system and other critical information system software in a separate facility or in a fire-rated container that is not collocated with the operational software.		
10			I/NI/P/NA/AR	
	CP-10	The organization employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to the system's original state after a disruption or failure.		
	CP-10.1	The organization includes a full recovery and reconstitution of the information system as part of contingency plan testing.		

Assessment Results	
I	0
NI	0
P	0
NA	0
AR	0
TOTAL	0

LEGEND
I = Implemented
NI = Not Implemented
P = Partially Implemented
NA = Not Applicable
AR = Accepting Risk

CONFIGURATION MANAGEMENT

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

Item	Control	Requirement	Status	Justification/Comments
1		The organization develops, disseminates, and periodically reviews/updates:	I/NI/P/NA/AR	
	CM-1	(i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, and compliance		
		(ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.		
2			I/NI/P/NA/AR	
	CM-2	The organization develops, documents, and maintains a current, baseline configuration of the information system and an inventory of the system's constituent components.		
	CM-2.1	The organization updates the baseline configuration as an integral part of information system component installations. Plan includes explicit checks with assigned responsibilities to periodically ensure that the plan is being implemented as intended.		
	CM-2.2	The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration.		
3			I/NI/P/NA/AR	
	CM-3	The organization documents and controls changes to the information system. Appropriate organizational officials approve information system changes in accordance with organizational policies and procedures.		

	CM-3.1	The organization employs automated mechanisms to: (i) document proposed changes to the information system (ii) notify appropriate approval authorities (iii) highlight approvals that have not been received in a timely manner (iv) inhibit change until necessary approvals are received (v) document completed changes to the information system		
4			I/NI/P/NA/AR	
	CM-4	The organization monitors changes to the information system and conducts security impact analyses to determine the effects of the changes.		
5			I/NI/P/NA/AR	
	CM-5	The organization enforces access restrictions associated with changes to the information system.		
	CM-5.1	The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.		
6			I/NI/P/NA/AR	
	CM-6			

Copyright© 2008
 Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

	CM-6.1	The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.		
7			I/NI/P/NA/AR	
	CM-7	The organization configures the information system to provide only essential capabilities and specifically prohibits and/or restricts the use of any protocol or service that is not explicitly permitted.		
	CM-7.1	The organization reviews the information system annually, to identify and eliminate unnecessary functions, ports, protocols, and/or services.		

Assessment Results	
I	0
NI	0
P	0
NA	0
AR	0
TOTAL	0

LEGEND

I = Implemented
 NI = Not Implemented
 P = Partially Implemented
 NA = Not Applicable
 AR = Accepting Risk

MAINTENANCE

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

Item	Control	Requirement	Status	Justification/Comments
1		The organization develops, disseminates, and periodically reviews/updates:	I/NI/P/NA/AR	
	MA-1	(i) a formal, documented, information system maintenance policy that addresses purpose, scope, roles, responsibilities, and compliance		
		(ii) formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.		
2			I/NI/P/NA/AR	
	MA-2	The organization schedules, performs, and documents routine preventative and regular maintenance on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.		
	MA-2.1	The organization maintains a maintenance log for the information system that includes: (i) the date and time of maintenance		
		(ii) name of the individual performing the maintenance		
		(iii) name of escort, if necessary		
		(iv) a description of the maintenance performed		
		(v) a list of equipment removed or replaced (including identification numbers, if applicable).		

	MA-2.2	The organization employs automated mechanisms to ensure that periodic maintenance is scheduled and conducted as required, and that a log of maintenance actions, both needed and completed, is up to date, accurate, complete, and available.		
3			I/NI/P/NA/AR	
	MA-3	The organization approves, controls, and monitors the use of information system maintenance tools and maintains the tools on an ongoing basis.		
	MA-3.1	The organization inspects all maintenance tools (e.g., diagnostic and test equipment) carried into a facility by maintenance personnel for obvious improper modifications.		
	MA-3.2	The organization checks all media containing diagnostic test programs (e.g., software or firmware used for system maintenance or diagnostics) for malicious code before the media are used in the information system.		
	MA-3.3	The organization checks all maintenance equipment with the capability of retaining information to ensure that no organizational information is written on the equipment or the equipment is appropriately sanitized before release; if the equipment cannot be sanitized, the equipment remains within the facility or is destroyed, unless an appropriate organization official explicitly authorizes an exception.		
	MA-3.4	The organization employs automated mechanisms to ensure only authorized personnel use maintenance tools.		
4			I/NI/P/NA/AR	
	MA-4	The organization approves, controls, and monitors remotely executed maintenance and diagnostic activities.		

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

	MA-4.1	The organization audits all remote maintenance sessions, and appropriate organizational personnel review the audit logs of the remote sessions.		
	MA-4.2	The organization addresses the installation and use of remote diagnostic links in the security plan for the information system.		
	MA-4.3	Remote diagnostic or maintenance services are acceptable if performed by a service or organization that implements for its own information system the same level of security as that implemented on the information system being serviced.		
5			I/NI/P/NA/AR	
	MA-5	The organization maintains a list of personnel authorized to perform maintenance on the information system. Only authorized personnel perform maintenance on the information system.		
6			I/NI/P/NA/AR	
	MA-6	The organization obtains maintenance support and spare parts within 48 hours of failure.		

Assessment Results	
I	0
NI	0
P	0
NA	0
AR	0
TOTAL	0

LEGEND
I = Implemented
NI = Not Implemented
P = Partially Implemented
NA = Not Applicable
AR = Accepting Risk

SYSTEM & INFORMATION INTEGRITY

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

Item	Control	Requirement	Status	Justification/Comments
1		The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, and compliance (ii) formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.	I/NI/P/NA/AR	
2	SI-1		I/NI/P/NA/AR	
		(i) a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, and compliance (ii) formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.		
2	SI-2	The organization identifies, reports, and corrects information system flaws	I/NI/P/NA/AR	
	SI-2.1	The organization centrally manages the flaw remediation process and installs updates automatically without individual user intervention.		
	SI-2.2	The organization employs automated mechanisms to periodically and upon command determine the state of information system components with regard to flaw remediation.		
3			I/NI/P/NA/AR	
	SI-3	The information system implements malicious code protection that includes a capability for automatic updates.		
	SI-3.1	The organization centrally manages virus protection mechanisms.		
	SI-3.2	The information system automatically updates virus protection mechanisms.		
4			I/NI/P/NA/AR	

	SI-4	The organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system.		
	SI-4.1	The organization networks individual intrusion detection tools into a system-wide intrusion detection system using common protocols.		
	SI-4.2	The organization employs automated tools to support near-real-time analysis of events in support of detecting system-level attacks.		
	SI-4.3	The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.		
	SI-4.4	The information system monitors outbound communications for unusual or unauthorized activities indicating the presence of malware (e.g., malicious code, spyware, adware).		
5			I/NI/P/NA/AR	
	SI-5	The organization receives information system security alerts/advisories on a regular basis, issues alerts/advisories to appropriate personnel, and takes appropriate actions in response.		
	SI-5.1	The organization employs automated mechanisms to make security alert and advisory information available throughout the organization as needed.		
6			I/NI/P/NA/AR	
	SI-6	The information system verifies the correct operation of security functions periodically every year and notifies system administrator when anomalies are discovered.		

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

	SI-6.1	The organization employs automated mechanisms to provide notification of failed security tests.		
	SI-6.2	The organization employs automated mechanisms to support management of distributed security testing.		
7			I/NI/P/NA/AR	
	SI-7	The information system detects and protects against unauthorized changes to software and information.		
8			I/NI/P/NA/AR	
	SI-8	The information system implements spam and spyware protection.		
	SI-8.1	The organization centrally manages spam and spyware protection mechanisms.		
	SI-8.2	The information system automatically updates spam and spyware protection mechanisms.		
9			I/NI/P/NA/AR	
	SI-9	The organization restricts the information input to the information system to authorized personnel only.		
10			I/NI/P/NA/AR	
	SI-10	The information system checks information inputs for accuracy, completeness, and validity.		
11			I/NI/P/NA/AR	

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

	SI-11	The information system identifies and handles error conditions in an expeditious manner.		
12			I/NI/P/NA/AR	
	SI-12	The organization handles and retains output from the information system in accordance with organizational policy and operational requirements.		

Assessment Results	
I	0
NI	0
P	0
NA	0
AR	0
TOTAL	0

LEGEND

I = Implemented
 NI = Not Implemented
 P = Partially Implemented
 NA = Not Applicable
 AR = Accepting Risk

MEDIA PROTECTION

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

Item	Control	Requirement	Status	Justification/Comments
1		The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, and compliance (ii) formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.	I/NI/P/NA/AR	
2	MP-1		I/NI/P/NA/AR	
		(i) a formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, and compliance		
		(ii) formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.		
2	MP-2	The organization ensures that only authorized users have access to information in printed form or on digital media removed from the information system.	I/NI/P/NA/AR	
	MP-2.1	Unless guard stations control access to media storage areas, the organization employs automated mechanisms to ensure only authorized access to such storage areas and to audit access attempts and access granted.		
3	MP-3	The organization affixes external labels to removable information storage media and information system output indicating the distribution limitations and handling caveats of the information.	I/NI/P/NA/AR	
4	MP-4	The organization physically controls and securely stores information system media, both paper and electronic, based on the highest FIPS 199 security category of the information recorded on the media.	I/NI/P/NA/AR	
5			I/NI/P/NA/AR	

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

	MP-5	The organization controls information system media (paper and electronic) and restricts the pickup, receipt, transfer, and delivery of such media to authorized personnel.		
6			I/NI/P/NA/AR	
	MP-6	The organization sanitizes information system digital media using approved equipment, techniques, and procedures. The organization tracks, documents, and verifies media sanitization actions and periodically tests sanitization equipment/procedures to ensure correct performance.		
7			I/NI/P/NA/AR	
	MP-7	The organization sanitizes or destroys information system digital media before its disposal or release for reuse outside the organization, to prevent unauthorized individuals from gaining access to and using the information contained on the media.		

Assessment Results	
I	0
NI	0
P	0
NA	0
AR	0
TOTAL	0

LEGEND

I = Implemented
 NI = Not Implemented
 P = Partially Implemented
 NA = Not Applicable
 AR = Accepting Risk

INCIDENT RESPONSE

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

Item	Control	Requirement	Status	Justification/Comments
1		The organization develops, disseminates, and periodically reviews/updates:	I/NI/P/NA/AR	
	IR-1	(i) a formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, and compliance		
		(ii) formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.		
2			I/NI/P/NA/AR	
	IR-2	The organization trains personnel in their incident response roles and responsibilities with respect to the information system and provides refresher training at least annually.		
	IR-2.1	The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.		
	IR-2.2	The organization employs automated mechanisms to provide a more thorough and realistic training environment.		
3			I/NI/P/NA/AR	
	IR-3	The organization tests the incident response capability for the information system at least annually using automated mechanisms for high systems to determine the incident response effectiveness and documents the results.		
	IR-3.1	The organization employs automated mechanisms to more thoroughly and effectively test the incident response capability.		
4			I/NI/P/NA/AR	
	IR-4	The organization employs automated mechanisms to support the incident handling process.		
	IR-4.1	The organization employs automated mechanisms to support the incident handling process.		

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

5			I/NI/P/NA/AR	
	IR-5	The organization tracks and documents information system security incidents on an ongoing basis.		
	IR-5.1	The organization tracks and documents information system security incidents on an ongoing basis.		
6			I/NI/P/NA/AR	
	IR-6	The organization promptly reports incident information to appropriate authorities.		
	IR-6.1	The organization employs automated mechanisms to assist in the reporting of security incidents.		
7			I/NI/P/NA/AR	
	IR-7	The organization provides an incident support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The support resource is an integral part of the organization's incident response capability.		
	IR-7.1	The organization employs automated mechanisms to increase the availability of incident response-related information and support.		

Assessment Results	
I	0
NI	0
P	0
NA	0
AR	0
TOTAL	0

LEGEND
I = Implemented
NI = Not Implemented
P = Partially Implemented
NA = Not Applicable
AR = Accepting Risk

AWARENESS & TRAINING

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

Item	Control	Requirement	Status	Justification/Comments
1		The organization develops, disseminates, and periodically reviews/updates:	I/NI/P/NA/AR	
	AT-1	(i) a formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, and compliance		
		(ii) formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.		
2			I/NI/P/NA/AR	
	AT-2	The organization ensures all users (including managers and senior executives) are exposed to basic information system security awareness materials before authorizing access to the system and at least annually thereafter.		
3			I/NI/P/NA/AR	
	AT-3	The organization identifies personnel with significant information system security roles and responsibilities, documents those roles and responsibilities, and provides appropriate information system security training before authorizing access to the system and each year thereafter.		
4			I/NI/P/NA/AR	
	AT-4	The organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training.		

Assessment Results	
I	0
NI	0
P	0
NA	0
AR	0
TOTAL	0

LEGEND
I = Implemented
NI = Not Implemented
P = Partially Implemented
NA = Not Applicable
AR = Accepting Risk

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

IDENTIFICATION & AUTHENTICATION

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

Item	Control	Requirement	Status	Justification/Comments
1		The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, and compliance (ii) formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls	I/NI/P/NA/AR	
2	IA-1		I/NI/P/NA/AR	
2	IA-2	The information system uniquely identifies and authenticates users (or processes acting on behalf of users).	I/NI/P/NA/AR	
	IA-2.1	The information system employs multifactor authentication.		
3			I/NI/P/NA/AR	
	IA-3	The information system identifies and authenticates specific devices before establishing a connection.		
4			I/NI/P/NA/AR	
	IA-4	The organization manages user identifiers by: (i) uniquely identifying each user (ii) verifying the identity of each user (iii) receiving authorization to issue a user identifier from an appropriate organization official (iv) ensuring that the user identifier is issued to the intended party (v) disabling user identifier after 30 days of inactivity (vi) archiving user identifiers		

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

5		The organization manages information system authenticators (e.g., tokens, PKI certificates, biometrics, passwords, key cards) by:	I/NI/P/NA/AR	
	IA-5	(i) defining initial authenticator content		
		(ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators		
		(iii) changing default authenticators upon information system installation.		
6			I/NI/P/NA/AR	
	IA-6	The information system provides feedback to a user during an attempted authentication and that feedback does not compromise the authentication mechanism.		
7			I/NI/P/NA/AR	
	IA-7	For authentication to a cryptographic module, the information system employs authentication methods that meet the requirements of FIPS 140-2.		

Assessment Results	
I	0
NI	0
P	0
NA	0
AR	0
TOTAL	0

LEGEND

I = Implemented
 NI = Not Implemented
 P = Partially Implemented
 NA = Not Applicable
 AR = Accepting Risk

ACCESS CONTROL

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

Item	Control	Requirement	Status	Justification/Comments
1		The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, and compliance (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.	I/NI/P/NA/AR	
2	AC-1		I/NI/P/NA/AR	
	AC-2	The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts annually.		
	AC-2.1	The organization employs automated mechanisms to support the management of information system accounts.		
	AC-2.2	The information system automatically terminates temporary and emergency accounts after 48 hours.		
	AC-2.3	The information system automatically disables inactive accounts after 90 Days.		
	AC-2.4	The organization employs automated mechanisms to ensure that account creation, modification, disabling, and termination actions are audited and, as required, appropriate individuals are notified.		
3			I/NI/P/NA/AR	
	AC-3	The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy.		
	AC-3.1	The information system ensures that access to security functions (deployed in hardware, software, and firmware) and information is restricted to authorized personnel (e.g., security administrators).		
4			I/NI/P/NA/AR	
	AC-4	The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.		

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

5			I/NI/P/NA/AR	
	AC-5	The information system enforces separation of duties through assigned access authorizations.		
6			I/NI/P/NA/AR	
	AC-6	The information system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.		
7			I/NI/P/NA/AR	
	AC-7	The information system enforces a limit of three consecutive invalid access attempts by a user during a 30 minute time period. The information system automatically locks the account/node for 30 minutes for low systems or until an appropriate security administrator manually intervenes to unlocks accounts on moderate and high systems when the maximum number of unsuccessful attempts is exceeded.		
	AC-7.1	The information system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.		
8		The information system displays an approved, system use notification message before granting system access informing potential users:	I/NI/P/NA/AR	
	AC-8	(i) that the user is accessing a U.S. Government information system		
		(ii) that system usage may be monitored, recorded, and subject to audit		
		(iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties		
		(iv) that use of the system indicates consent to monitoring and recording. The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.		
9			I/NI/P/NA/AR	

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

	AC-9	The information system notifies the user, upon successful logon, of the date and time of the last logon, and the number of unsuccessful logon attempts since the last successful logon.		
10			I/NI/P/NA/AR	
	AC-10	The information system does not allow concurrent sessions for systems rated high.		
11			I/NI/P/NA/AR	
	AC-11	The information system prevents further access to the system by initiating a session lock that remains in effect until the user reestablishes access using appropriate identification and authentication procedures.		
12			I/NI/P/NA/AR	
	AC-12	The information system automatically terminates a session after ten minutes of inactivity.		
13			I/NI/P/NA/AR	
	AC-13	The organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls.		
	AC-13.1	The organization employs automated mechanisms to facilitate the review of user activities.		
14			I/NI/P/NA/AR	
	AC-14	The organization identifies specific user actions that can be performed on the information system without identification or authentication.		
	AC-14.1	The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives.		
15			I/NI/P/NA/AR	
	AC-15	The information system marks output using standard naming conventions to identify any special dissemination, handling, or distribution instructions.		

16			I/NI/P/NA/AR	
	AC-16	The information system appropriately labels information in storage, in process, and in transmission.		
17			I/NI/P/NA/AR	
	AC-17	The organization documents, monitors, and controls all methods of remote access (e.g., dial-up, Internet) to the information system including remote access for privileged functions. Appropriate organization officials authorize each remote access method for the information system and authorize only the necessary users for each access method.		
	AC-17.1	The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.		
	AC-17.2	The organization uses encryption to protect the confidentiality of remote access sessions.		
	AC-17.3	The organization controls all remote accesses through a managed access control point.		
18			I/NI/P/NA/AR	
	AC-18	The organization: (i) establishes usage restrictions and implementation guidance for wireless technologies (ii) documents, monitors, and controls wireless access to the information system. Appropriate organizational officials authorize the use of wireless technologies.		
	AC-18.1	The organization uses authentication and encryption to protect wireless access to the information system.		
19			I/NI/P/NA/AR	
	AC-19	The organization: (i) establishes usage restrictions and implementation guidance for portable and mobile devices (ii) documents, monitors, and controls device access to organizational networks. Appropriate organizational officials authorize the use of portable and mobile devices.		
	AC-19.1	The organization employs removable hard drives or cryptography to protect information residing on portable and mobile devices.		

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

20			I/NI/P/NA/AR	
	AC-20	The organization restricts the use of personally owned information systems for official U.S. Government business involving the processing, storage, or transmission of federal information.		

Assessment Results	
I	0
NI	0
P	0
NA	0
AR	0
TOTAL	0

LEGEND

I = Implemented
 NI = Not Implemented
 P = Partially Implemented
 NA = Not Applicable
 AR = Accepting Risk

AUDITING & ACCOUNTABILITY

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

Item	Control	Requirement	Status	Justification/Comments
1		The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, and compliance (ii) formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.	I/NI/P/NA/AR	
2	AU-1		I/NI/P/NA/AR	
	AU-2	The information system generates audit records for events identified in the C29.		
	AU-2.1	The information system provides the capability to compile audit records from multiple components throughout the system into a system-wide (logical or physical), time-correlated audit trail.		
	AU-2.2	The information system provides the capability to manage the selection of events to be audited by individual components of the system.		
3			I/NI/P/NA/AR	
	AU-3	The information system captures sufficient information in audit records to establish what events occurred, the sources of the events, and the outcomes of the events.		
	AU-3.1	The information system provides the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.		
	AU-3.2	The information system provides the capability to centrally manage the content of audit records generated by individual components throughout the system.		

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

4			I/NI/P/NA/AR	
	AU-4	The organization allocates sufficient audit record storage capacity and configures auditing to prevent such capacity being exceeded.		
5			I/NI/P/NA/AR	
	AU-5			
	AU-5.1	The information system provides a warning when allocated audit record storage volume is close to being reached.		
6			I/NI/P/NA/AR	
	AU-6	The organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.		
	AU-6.1	The organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.		
	AU-6.2	The organization employs automated mechanisms to immediately alert security personnel of inappropriate or unusual activities with security implications.		
7			I/NI/P/NA/AR	
	AU-7	The organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.		
	AU-7.1	The information system provides the capability to automatically process audit records for events of interest based upon selectable, event criteria.		
8			I/NI/P/NA/AR	

	AU-8	The information system provides time stamps for use in audit record generation.		
9			I/NI/P/NA/AR	
	AU-9	The information system protects audit information and audit tools from unauthorized access, modification, and deletion.		
	AU-9.1	The information system produces audit information on hardware-enforced, write-once media.		
10			I/NI/P/NA/AR	
	AU-10	The information system provides the capability to determine whether a given individual took a particular action (e.g., created information, sent a message, approved information [e.g., to indicate concurrence or sign a contract] or received a message).		
11			I/NI/P/NA/AR	
	AU-11	The organization retains audit logs in accordance with system owners records retention policies, but at least for one year for high and moderate systems to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.		

Assessment Results	
I	0
NI	0
P	0
NA	0
AR	0
TOTAL	0

LEGEND

I = Implemented
 NI = Not Implemented
 P = Partially Implemented
 NA = Not Applicable
 AR = Accepting Risk

SYSTEMS & COMMUNICATION PROTECTION

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

Item	Control	Requirement	Status	Justification/Comments
1		The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, and compliance.	I/NI/P/NA/AR	
	SC-1	(ii) formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.		
2			I/NI/P/NA/AR	
	SC-2	The information system separates user functionality (including user interface services) from information system management functionality.		
3			I/NI/P/NA/AR	
	SC-3	The information system isolates security functions from nonsecurity functions.		
	SC-3.1	The information system employs underlying hardware separation mechanisms to facilitate security function isolation.		
	SC-3.2	The information system further divides the security functions with the functions enforcing access and information flow control isolated and protected from both non-security functions and from other security functions.		
	SC-3.3	The information system minimizes the amount of nonsecurity functions included within the isolation boundary containing security functions.		
	SC-3.4	The information system security maintains its security functions in largely independent modules that avoid unnecessary interactions between modules.		

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

	SC-3.5	The information system security maintains its security functions in a layered structure minimizing interactions between layers of the design.		
4			I/NI/P/NA/AR	
	SC-4	The information system prevents unauthorized and unintended information transfer via shared system resources.		
5			I/NI/P/NA/AR	
	SC-5	The information system protects against or limits the effects of denial of service attacks on devices within the organization's internal network.		
	SC-5.1	The information system restricts the ability of users to launch denial of service attacks against other information systems or networks.		
	SC-5.2	The information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks		
6			I/NI/P/NA/AR	
	SC-6	The information system limits the use of resources by priority.		
7			I/NI/P/NA/AR	
	SC-7	The information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.		
	SC-7.1	The organization physically allocates publicly accessible information system components (e.g., public web servers) to separate subnetworks with separate, physical network interfaces. The organization prevents public access into the organization's internal networks except as appropriately mediated.		
8			I/NI/P/NA/AR	

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

	SC-8	The information system protects the integrity of transmitted information.		
	SC-8.1	The organization employs cryptographic mechanisms to ensure recognition of changes to information during transmission unless otherwise protected by alternative physical measures (e.g., protective distribution systems).		
9			I/NI/P/NA/AR	
	SC-9	The information system protects the confidentiality of transmitted information		
	SC-9.1	The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless protected by alternative physical measures (e.g., protective distribution systems).		
10			I/NI/P/NA/AR	
	SC-10	The information system terminates a network connection at the end of a session or after ten minutes of inactivity.		
11			I/NI/P/NA/AR	
	SC-11	The information system establishes a trusted communications path between the user and the security functionality of the system.		
12			I/NI/P/NA/AR	
	SC-12	The information system employs automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management.		
13			I/NI/P/NA/AR	

	SC-13	When cryptography is employed within the information system, the system performs all cryptographic operations (including key generation) using FIPS 140- 2 validated cryptographic modules operating in approved modes of operation.		
14			I/NI/P/NA/AR	
	SC-14	For publicly available systems, the information system protects the integrity of the information and applications.		
15			I/NI/P/NA/AR	
	SC-15	The information system prohibits remote activation of collaborative computing mechanisms (e.g., video and audio conferencing) and provides an explicit indication of use to the local users (e.g., use of camera or microphone).		
	SC-15.1	The information system provides physical disconnect of camera and microphone in a manner that supports ease of use.		
16			I/NI/P/NA/AR	
	SC-16	The information system reliably associates security parameters (e.g., security labels and markings) with information exchanged between information systems.		
17			I/NI/P/NA/AR	
	SC-17	The organization develops and implements a certificate policy and certification practice statement for the issuance of public key certificates used in the information system.		
18			I/NI/P/NA/AR	
	SC-18	The organization: (i) establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously		

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

		(ii) documents, monitors, and controls the use of mobile code within the information system. Appropriate organizational officials authorize the use of mobile code.		
19			I/NI/P/NA/AR	
	SC-19	The organization: (i) establishes usage restrictions and implementation guidance for Voice Over Internet Protocol (VOIP) technologies based on the potential to cause damage to the information system if used maliciously		
		(ii) documents, monitors, and controls the use of VOIP within the information system. Appropriate organizational officials authorize the use of VOIP.		

Assessment Results	
I	0
NI	0
P	0
NA	0
AR	0
TOTAL	0

LEGEND

I = Implemented
 NI = Not Implemented
 P = Partially Implemented
 NA = Not Applicable
 AR = Accepting Risk



The Federation for Identity and
Cross-Credentialing Systems®

Appendix E

Risk Assessment Template

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

Appendix TBD

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)



The Federation for Identity and
Cross-Credentialing Systems®

Appendix F

System Security Plan Template

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXS®)

The FiXs Systems Security Plan (SSP) Template provides guidance, content requirements, and direction for preparation of SSPs. The SSP is required during the Initiation Phase of the FiXs C&A Process.

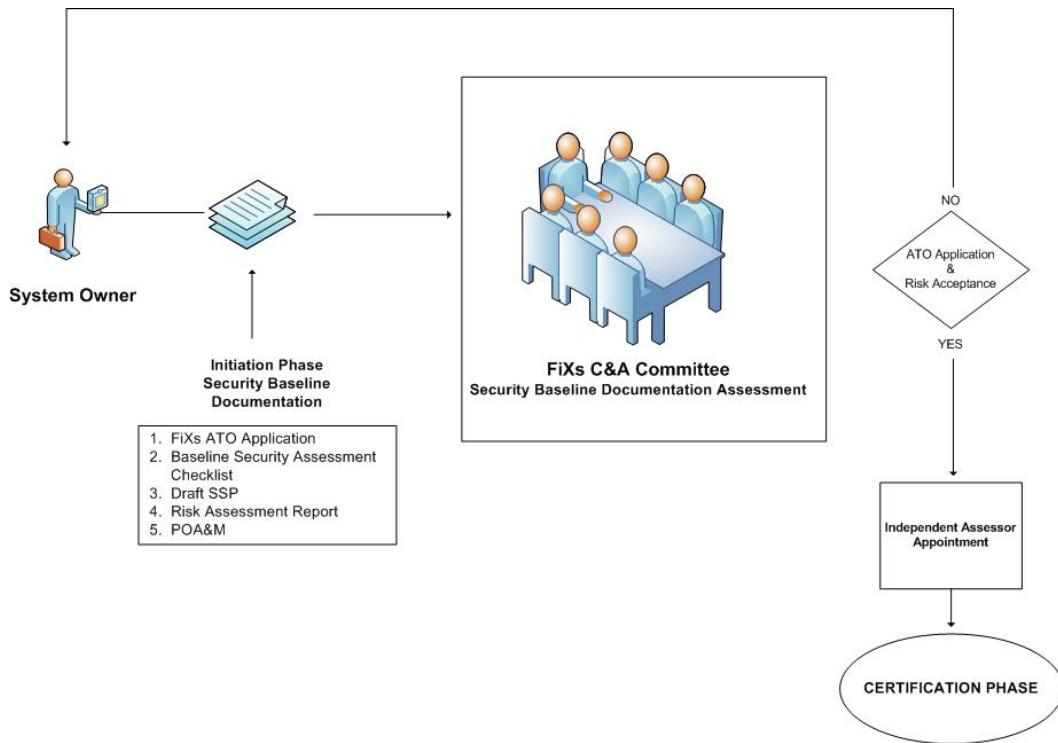


Figure 1, FiXs Initiation Phase Document Review Process



The Federation for Identity and
Cross-Credentialing Systems®

***click here and enter system
name & acronym
SYSTEM SECURITY PLAN (SSP)***

*click here and enter system owner's NAME
click here and enter system owner's Address*

SSP Date *click here and enter date of SSP*

TABLE OF CONTENTS

1. SYSTEM IDENTIFICATION	5
1.1 SYSTEM NAME/TITLE.....	5
1.2 RESPONSIBLE ORGANIZATION.....	5
1.3 INFORMATION CONTACTS.....	5
1.4 ASSIGNMENT OF SECURITY RESPONSIBILITY	6
1.5 SYSTEM OPERATIONAL STATUS.....	7
1.6 GENERAL DESCRIPTION/PURPOSE.....	7
2. MANAGEMENT CONTROLS	14
2.1 RISK ASSESSMENT (RA) AND RISK MANAGEMENT.....	14
2.2 REVIEW OF SECURITY CONTROLS	15
2.3 RULES OF BEHAVIOR (ROB)	15
2.4 PLANNING FOR SECURITY IN THE SDLC.....	15
3. OPERATIONAL CONTROLS.....	15
3.1 PERSONNEL SECURITY CONTROLS	15
3.2 PHYSICAL AND ENVIRONMENTAL PROTECTION CONTROLS	15
3.3 PRODUCTION INPUT/OUTPUT CONTROLS	15
3.4 INCIDENT RESPONSE CAPABILITY	15
3.5 CONTINGENCY PLANNING AND DISASTER RECOVERY PLANNING.....	16
3.6 HARDWARE, OPERATING SYSTEM, AND SYSTEM SOFTWARE MAINTENANCE CONTROLS	16
3.7 DATA INTEGRITY/VALIDATION CONTROLS.....	16
3.8 DOCUMENTATION	16
3.9 SECURITY AWARENESS, AND TRAINING (SAT).....	16
4. TECHNICAL CONTROLS	16
4.1 IDENTIFICATION AND AUTHENTICATION CONTROLS	16
4.2 AUTHORIZATION AND ACCESS CONTROLS	17
4.3 REMOTE USERS AND DIAL-UP CONTROLS	17
4.4 WIDE AREA NETWORKS (WAN) CONTROLS	17
4.5 PUBLIC ACCESS CONTROLS	17
4.6 TEST SCRIPTS/RESULTS	17
4.7 AUDIT TRAILS.....	17
5. APPENDICES AND ATTACHMENTS	17
APPENDIX A - EQUIPMENT LIST.....	17
APPENDIX B - SOFTWARE LIST	17
APPENDIX C – GLOSSARY	17
APPENDIX D - ACRONYMS & ABBREVIATIONS	17

[if needed, modify the attachment(s) list as necessary]

ATTACHMENT 1.....	ATT 1-1
ATTACHMENT 2.....	ATT 2-1

1. SYSTEM IDENTIFICATION

1.1 SYSTEM OVERVIEW

This section should provide a general description of the system and identifies the system's purpose, capabilities, users, and information data flows. This section should also generally discuss the hardware, software firmware, and technologies implemented in support of deployment of the system.

1.2 SYSTEM NAME/TITLE

Official System Name:	click here and enter data
System Acronym:	click here and enter data
System of Records (SOR) #:	This will be supplied by FiXs C&A Committee click here and enter data

1.3 RESPONSIBLE ORGANIZATION

Name of Organization:	click here and enter data
Address:	click here and enter data
City, State, Zip:	click here and enter data
Contract Number:	click here and enter data
Contractor Name:	click here and enter data

1.4 INFORMATION CONTACTS

Name: (System Owner/Manager)	click here and enter data
Title:	click here and enter data
Organization:	click here and enter data
Address:	click here and enter data
Mailstop:	click here and enter data
City, State, Zip:	click here and enter data
Phone:	click here and enter data
E-Mail:	click here and enter data

click here and enter data

Name: (Business Owner/Manager)
Title: click here and enter data
Organization: click here and enter data
Address: click here and enter data
Mailstop: click here and enter data
City, State, Zip: click here and enter data
Phone: click here and enter data
E-Mail: click here and enter data

Name: (System Maintainer Manager)
Title: click here and enter data
Organization: click here and enter data
Address: click here and enter data
Mailstop: click here and enter data
City, State, Zip: click here and enter data
Phone: click here and enter data
E-mail: click here and enter data

Name: (SSP Author)
Title: This Section will be Completed by FiXes Assigned Assessor
Organization: click here and enter data
Address: click here and enter data
Mailstop: click here and enter data
City, State, Zip: click here and enter data
Phone: click here and enter data
E-mail: click here and enter data

1.5 ASSIGNMENT OF SECURITY RESPONSIBILITY

Name: (individual[s] responsible for security) click here and enter data
Title: click here and enter data
Organization: click here and enter data
Address: click here and enter data

Mailstop:	click here and enter data
City, State, Zip:	click here and enter data
Phone:	click here and enter data
E-mail:	click here and enter data
Emergency Contact: (name, phone & email)	click here and enter data
Name: (System/Component Security Manager)	click here and enter data
Title:	click here and enter data
Organization:	click here and enter data
Address:	click here and enter data
Mailstop:	click here and enter data
City, State, Zip:	click here and enter data
Phone:	click here and enter data
E-mail:	click here and enter data
Emergency Contact: (name, phone & email)	click here and enter data

1.6 SYSTEM OPERATIONAL STATUS

✓ (Check Only One) *new*, *operational*, or *undergoing a major modification.*

1.7 GENERAL DESCRIPTION/PURPOSE

This section should provide a technical description of the system and identifies the system's major applications/components, capabilities, users, and information data flows. This should also discuss the hardware, software and firmware implemented in support of deployment of the system.

click here and enter text for this section

The following table(s) identifies the major applications supported by the system or network.

Application Name:	
Function:	
Type of Information:	
Application High Water Mark:	

Table 1-1: Major Application Supported by System Name

The following table(s) identifies the major applications supported by the system or network.

Application Name:	
Function:	
Type of Information:	
Application High Water Mark:	

Table 1-2: Major Application Supported by System Name

{Use as many table as required to describe the system's applications. This section must identify whether the identified system is a component of another General Support System (GSS) or other Major Application (MA)}

1.7.1 System Environment and Special Considerations

click here and enter text for this section

1.7.2 System Accreditation Boundary

An in depth description of the accreditation boundary is required here. This paragraph will determine all the hardware and software that is being Accredited during the C&A effort. If there are multiple sites, buildings, systems and so on, then they should all be included in here. This paragraph should reflect the Network Diagram and Topology.

click here and enter text for this section

1.7.3 System Users

Provide an overview of the type of users for the system with the Security Rating and then provide a table with will identify their Security Level (T1 through T3).

click here and enter text for this section

Type of User	Security Level
(System Administrator, Maintenance Personnel, General Users, etc.,)	(T1, T2, T3)

Table 1-3: System Users

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

1.7.4 System Hardware Description

click here and enter text for this section

Use a table to list the principal hardware components for the system.

Hardware/Operating System	Location	Remarks

Table 1-4: System Hardware

1.7.5 System Software Description

click here and enter text for this section

Use a table to list the principal software components for the system.

Operating System/Application	Location	Remarks

Table 1-5: System Software

(Note: An entire list of the system hardware and software inventory must be maintained per the FiXs C&A Appendix A, CM-2 security control. These lists should be provided as Appendices A & B to the SSP).

1.7.6 System Firmware Description

click here and enter text for this section

Use a table to list the principal firmware components for the system.

Hardware Device	Firmware	Remarks

Table 1-6: System Firmware

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

1.7.7 Encryption/PKI

Provide a high level description of the use of Encryption/PKI if applicable. A more detailed use of encryption will be provided below in Section 4.)

click here and enter text for this section

1.7.8 Network Topology

click here and enter text for this section

Describe the physical network topology implemented by the system.

- Bus Topology
- Mesh Topology
- Ring Topology
- Star Topology
- Tree Topology
- Hybrid Topology – explain

1.7.8.1 Network Configuration

Provide a Network Configuration Diagram and a brief statement that explains the diagram at a high level.

click here and enter text for this section

1.7.8.2 Network Connection Rules

Provide the Policy and Procedures for Network Connections. “This does not include connection by user.” The connection rules are related to systems connections.

click here and enter text for this section

1.7.9 System Environment

click here and enter text for this section

Provide an overview of the system environment based either on it's current environment or the planned environment being certified.

1.7.10 System Interconnection/Information Sharing

Describe policies and procedures that are planned or implemented to manage system interconnections and information sharing between other systems. List, and identify all planned or current connections to external systems. List all agreements that are planned or currently in place which outline the agreements for identified system interconnections.

click here and enter text for this section

1.7.11 Information Flow

Provide an overview of the how the information flows from point A to B and back if necessary. This is normally at a high level view and if the information crosses organizational boundaries, the appropriate interconnection agreement(s) must be referenced.

click here and enter text for this section

1.7.12 Mobile Code

If Mobile Code is used, explain where and how it is used. Explain why it is required to support the operation of the system. Identify how the use of mobile code was approved and identify the approval authority.

click here and enter text for this section

1.7.13 Ports, Protocols, and Services

Provide a table which lists the Ports, Protocols, and Services enabled in the system.

click here and enter text for this section

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

Keyword	Decimal	Description	Used By

Table 1-7: System Port, Protocols, and Services

1.7.14 Applicable Laws/ Regulations Affecting the System

The following is a generic listing of documents that should have been used to develop and reference during the C&A process. This listing should be tailored to meet the organization(s) in question during the C&A effort. As a minimum the following references should be listed:

- a. *FiXs By-Laws, Version 2.2, 26 Nov 2007*
- b. *FiXs Security Guidelines, Version 2.0, 29 Mar 07*
- c. *FiXs Implementation Guidelines, Version 3.0, 29 Mar 2007*
- d. *FiXs Policy Document , Version 2.0, 29 Mar 2007*
- e. *FIXS Operating Rules, Version 2.0, 29 Mar 2007*
- f. *FIXS Operating Rules, Addendum*
- g. *FiXs Trust Model, Version 2.0, 29 Mar 2007*
- h. *FiXs Certification and Accreditation Process, 22 Aug 2008*

(Add any other pertinent references)

click here and enter text for this section

1.7.15 System Categorization

Using the security controls for Confidentiality, Integrity and Availability from Appendix A of the FiXs C&A Process in conjunction with the FiXs Security Guidelines, FiXs Operating Rules, and FiXs Logical Operating Rules, identify the baseline security categorization for the system. Use the guidelines and methodologies described in NIST SP 800-60 to develop system categorization.

Note that impacts may be tailored higher or lower depending upon the system's overall system posture and conditions outlined in the SSP and Risk Assessment Report.

{Enter System Categorization Table here.)

Information System Name: SCADA System [and Agency specific identifier]			
Business and Mission Supported: The SCADA (supervisory control and data acquisition) system provides real-time control and information supporting the main power plant. The power plant provides critical distribution of electric power to the military installation.			
Information Types			
[D.7.1] Energy Supply	Sensor data monitoring the availability of energy for the Military installation and its soldiers and command authority. This function includes control of distribution and transfer of power. The SCADA remote control capabilities can take action such as initiating necessary switching actions to alleviate an overloading power condition. The impacts to this information and the SCADA system may affect the installation's critical infrastructures.		
[C.2.8.12]General Information	The SCADA information system processes routine administrative information.		
Step 1 Identify Information Types	Step 2 [Provisional] / Step 3a [Adjustments]		
	Confidentiality Impact	Integrity Impact	Availability Impact
Step 3b- Impact Adjustment Justification			
Energy Supply	L / M	L / H	L / H
	Disclosure of sensor information may seriously impact the missions if indications & warnings of overall capability are provided to an adversary.	Severe impacts or consequences may occur if adversarial modification of information results in incorrect power system regulation or control actions.	Due to loss of availability, severe impact to the mission capability may result and may in-turn have overall catastrophic consequences for the facility's critical infrastructures and possible loss of human life.
General Information	L	L	L
	No adjustments	No adjustments	No adjustments
Step 4 System Categorization:	Moderate	High	High
	Overall Information System Impact: High		

Sample Security Categorization Table

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

The following section of the SSP provides a description of the Risk Management approach and applicable security controls and security measures that have been implemented and or incorporated into the system's design. Using the terminology described in Appendix A to the FiXs C&A Process, the system sponsor must address the Risk Management Approach and the security controls and security measures which have been factored or incorporated into the system's design. Information contained in this section should also address how the selected controls have been implemented. The paragraphs included in this section may be supplemented by information provided in the accompanying Security Baseline Document, Risk Management Report, and separate stand alone policies, plans, or procedures. Copies of supporting policies, plans, or procedures should be attached as appendices to the SSP.

2. MANAGEMENT CONTROLS

2.1 RISK ASSESSMENT (RA) AND RISK MANAGEMENT

Information provided in this paragraph should include a high level summary risks and the risk management approach outlined in the accompanying Risk Management Report.

The following table provides an example of the high level Risk management data which is required in this section.

RISK ASSESSMENT				RISK MANAGEMENT	
Vulnerability	Risk Level	Recommended Safeguard	Residual Risk	Status of Safeguard	Updated Risk
click here and enter data					
click here and enter data					

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

click here and enter text for this section

2.2 REVIEW OF SECURITY CONTROLS

click here and enter text for this section

2.3 RULES OF BEHAVIOR (ROB)

click here and enter text for this section

2.4 PLANNING FOR SECURITY IN THE SDLC

2.4.1 Pre-Development Phase

click here and enter text for this section

2.4.2 Development Phase

click here and enter text for this section

2.4.3 Post-Development Phase

click here and enter text for this section

3. OPERATIONAL CONTROLS

3.1 PERSONNEL SECURITY CONTROLS

click here and enter text for this section

3.2 PHYSICAL AND ENVIRONMENTAL PROTECTION CONTROLS

click here and enter text for this section

3.3 PRODUCTION INPUT/OUTPUT CONTROLS

click here and enter text for this section

3.4 INCIDENT RESPONSE CAPABILITY

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

click here and enter text for this section

3.5 CONTINGENCY PLANNING AND DISASTER RECOVERY PLANNING

click here and enter text for this section

3.6 HARDWARE, OPERATING SYSTEM, AND SYSTEM SOFTWARE MAINTENANCE CONTROLS

3.6.1 Configuration Management (CM)

click here and enter text for this section

3.6.2 Environmental System Software Management

click here and enter text for this section

3.6.3 Application Software Management

click here and enter text for this section

3.7 DATA INTEGRITY/VALIDATION CONTROLS

click here and enter text for this section

3.8 DOCUMENTATION

click here and enter text for this section

3.9 SECURITY AWARENESS, AND TRAINING (SAT)

click here and enter text for this section

4. TECHNICAL CONTROLS

4.1 IDENTIFICATION AND AUTHENTICATION CONTROLS

click here and enter text for this section

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

4.2 AUTHORIZATION AND ACCESS CONTROLS

click here and enter text for this section

4.3 REMOTE USERS AND DIAL-UP CONTROLS

click here and enter text for this section

4.4 WIDE AREA NETWORKS (WAN) CONTROLS

click here and enter text for this section

4.5 PUBLIC ACCESS CONTROLS

click here and enter text for this section

4.6 TEST SCRIPTS/RESULTS

click here and enter text for this section

4.7 AUDIT TRAILS

click here and enter text for this section

5. APPENDICES AND ATTACHMENTS

5.1 APPENDIX A - EQUIPMENT LIST

click here and enter text for this section

5.2

5.3 APPENDIX B - SOFTWARE LIST

click here and enter text for this section

5.4

5.5 APPENDIX C – GLOSSARY

click here and enter text for this section

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

5.6

5.7 APPENDIX D - ACRONYMS & ABBREVIATIONS

click here and enter text for this section

ATTACHMENT 1 (if needed)

click here and enter text for this section

ATTACHMENT 2 (if needed)

click here and enter text for this section



The Federation for Identity and
Cross-Credentialing Systems®

Appendix G

Plan of Action and Milestones (POA&M) Template

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXS®)

The FiXs Plan of Actions & Milestones (PAO&M) Template provides guidance, content requirements, and direction for preparation of the system security risks and deficiencies. The POA&M Template is required during the Initiation Phase of the FiXs C&A Process.

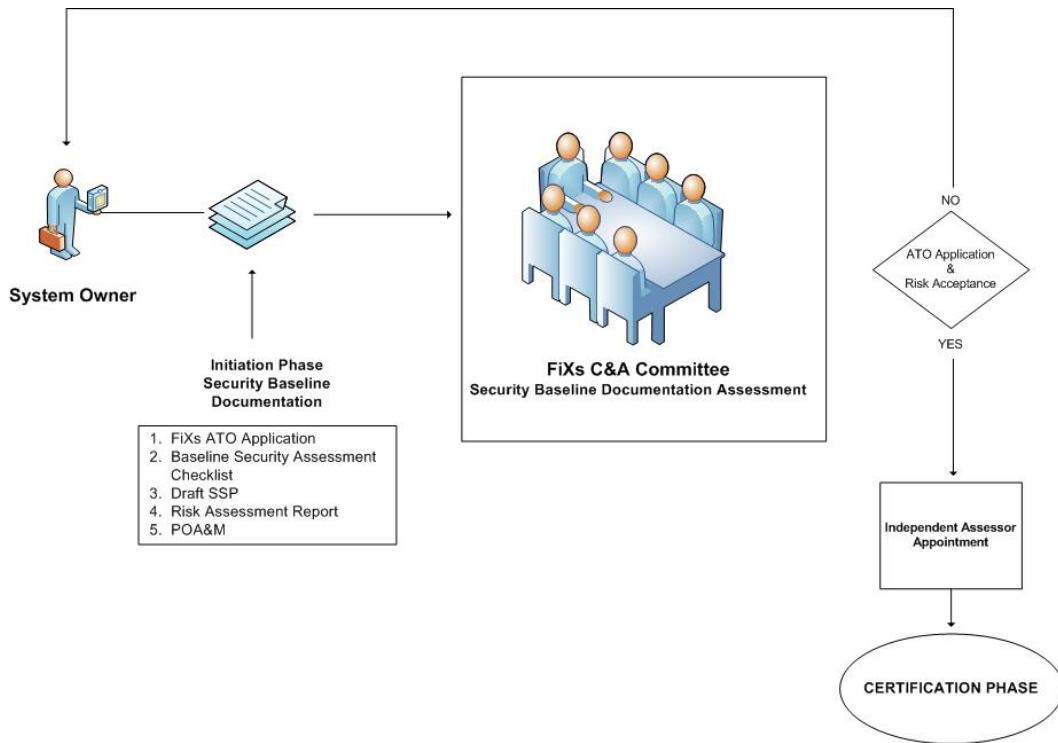


Figure 1, FiXs Initiation Phase Document Review Process

FiXs Plan of Action and Milestones (POA&M) Template

Date: _____ POC Name: _____ FiXs Certification Agent Name: _____
 System Component Name: _____ POC Phone: _____ Security Costs: _____
 System/Project Name: _____ POC E-mail: _____
 FiXs SORN Identifier: _____

Number	Security Control	Weakness	Risk Rating	POC	Resources Required	Scheduled Completion Date	Milestones with Completion Dates	Milestone Changes	Status	Comments
Enter sequential number for each identified deficiency or Risk	Enter the IA Control number from the C&A Checklist that was marked as "No Supported" or "Not Fully Supported"	Provide description of IA Control that was marked as "No Supported" or "Not Fully Supported"	Provide High, Medium or Low impact assessment which correlates with System Risk Assessment	Enter the system POC role (i.e. PM, ISSO, ISSM, I etc.)	Enter the estimated staffing & monetary amount required to eliminate identified deficiency or Risk	Enter the scheduled completion date in the form Day Month Year	If applicable enter each milestone date and the associated milestone otherwise enter N/A	If changes to the Milestone Dates occur enter each new milestone date and the associated milestone	Enter Ongoing or Completed,	For non-compliant IA Controls that have received FiXs DAA Risk Acceptance; enter document name and date of the Document which provided DAA Risk Acceptance



The Federation for Identity and
Cross-Credentialing Systems®

Appendix H

Security Requirements Traceability Matrix (SRTM) Example – Trusted Gateway Broker

Copyright© 2008
Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXS®)

Appendix TBD

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)



The Federation for Identity and
Cross-Credentialing Systems®

Appendix I

FiXS PIV Card Issuer (PCI) Operation Plan Template

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXS®)

This appendix provides a template for developing a NIST 800-79-1 compliant PIV Operations Plan. The following is a suggested outline for the PCI operations plan. It is highly recommended that an organization follow this template to document its PCI operations comprehensively and to the full extent as needed to support a successful accreditation.

Background

<Provide a brief background on HSPD-12, FIPS 201-1 and PIV, as well as how the organization has planned to meet the Directive. >

II. Purpose and Scope

<Describe the purpose and scope of the operations plan.>

III. Applicable Laws, Directives, Policies, Regulations & Standards

<Identify all Laws, Directives, Policies, Regulations and Standards that govern PIV Card issuance at the Organization.>

IV. PCI Roles and Responsibilities

<Identify the accreditation-related roles and responsibilities of all key personnel within the PCI.>

V. Assignment of Roles

<Document how the various roles that have been identified in the section above are appointed. These can be either specific individuals or positions within the organization. Provide contact information for all the roles assigned.>

VI. PCI Description

<Provide a description of the organization's PCI. Details such as structure and geographic dispersion should be included.>

VII. PCI Facility Details

<Identify all the PCI Facilities that are included within the PCI that are part of the accreditation boundary. Provide details such as the location, PIV Card functions performed (e.g. enrollment and/or registration) at the facility, and the approximate number of PIV Cards supported at each facility.>

VIII. PCI Management

<This section discusses various management aspects of the PCI.>

Coordination and Interaction

<Describe management interactions within the PCI, both at an organization level and between the organization and the facility(ies).>

Staffing

<Describe the procedures employed to make sure that adequate staff is available for performing PIV Card related functions.>

Training

<Describe the procedures employed to ensure that the staff is properly trained to perform their respective duties.>

Procurement

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

<Describe the mechanism typically used for procuring products/services related to the organization's HSPD-12 implementation.>

Outsourcing

<Describe the PIV Card functions being outsourced at the PCI (if applicable).>

IX. PCI Policies and Procedures

<Describe in this section the various policies and procedures that apply for (i) sponsorship, (ii) Enrollment and Identity proofing, (iii) Adjudication, (iv) card production, (v) card activation and issuance, and (vi) maintenance. Also discuss the procedures for temporary badges, as well as for non-PIV badges employed by the organization.>

- a. Sponsorship
- b. Enrollment/Identity Proofing
- c. Adjudication
- d. Card Production
- e. Card Activation/Issuance
- f. Maintenance
 - Card Termination
 - Card Renewal
 - Card Re-issuance
- g. Temporary/Non-PIV Badges

X. PCI Information System(s) Description

<Provide a description of the technical aspects of the organization's PIV system, including system architecture, network connectivity, connections to external system and information shared both internally and externally, and the PKI provider as well as the information system accreditation status.>

Architecture

Interconnections and Information Sharing
Information System Inventory
Public Key Infrastructure
SP 800-37 C&A Information

XI. Card Personalization & Production

<Describe the organization's PIV Card graphical layout(s), as well the optional data containers being used. Provide details if there are any PIV Card expiration date requirements levied by the organization. Also describe the mechanisms in place for securing both pre-personalized and personalized PIV Card stock.>

PIV Card Graphical Topology

PIV Card Electronic Data Elements

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)

Expiration Date Requirements
Card Inventory Management

XII. Card Reporting Requirements

<Describe how the organization collects information from its facilities relating to the number of PIV Cards issued and background investigations completed etc., as required by OMB. Also provide details on how the organization consolidates this information and provides its report to OMB on the status of their HSPD-12 implementation.>

XIII. PCI Controls

<This section documents the PCI Controls and provides the following information for each: (i) PCI control identifier and description, (ii) control owner, (iii) whether the control is organization-specific or facility- specific, and (iv) a description of how the PCI control has been implemented by the organization.>

PCI Control Identifier and Description

PCI Control Owner

Organization/Facility Specific

How the PCI control is implemented

Appendix A - Memoranda of Appointment

<Attach copies of signed memoranda-of-appointment that record the various roles that have been assigned and the personnel fulfilling these roles that have accepted the position and its associated responsibilities.>

Appendix B - Privacy Requirements

<Attach copies of the privacy-related information as identified below.>

- a. Privacy Policy
- b. Privacy Impact Assessment
- c. System of Record Notice
- d. Privacy Act Statement/Notice
- e. Rules of Conduct
- f. Privacy Processes
 - Requests to review personal information
 - Requests to amend personal information
 - Appeal procedures
 - Complaint procedures

Appendix C – Service Level Agreements, Memoranda of Understanding (MOU)

<Attach copies of any service level agreements and memoranda of understanding executed between the organization and any external service provider that has been contracted to provide certain PIV related functions.>

Copyright© 2008

Proprietary Information of the Federation for Identity and Cross-Credentialing Systems, Inc.® (FiXs®)