United States Federal PKI X.509 Certification Practice Statement (CPS) for the Federal Public Key Infrastructure (FPKI) Trust Infrastructure

Federal Bridge Certification Authority (FBCA)
Federal Common Policy Certification Authority (FCPCA)

14 December 2022

Version 6.2

Signature Page

_____   _____

Program Manager, Federal PKI Management Authority   DATE

Table of Contents

Contents

List of Tables

RECORD OF CHANGES

CHANGE DESCRIPTION	VERSION NUMBER	DATE OF CHANGE
Updated CPS to RFC 3647 Format.	2.0	2 February 2008
Updated CPS to reflect new location of FPKI and changes made for deployment of the Target Architecture (planned deployment in September 2010).	3.0	21 May 2010

Minor updates to CPS to clarify archiving procedures.	3.1	27 May 2010
Updated to incorporate changes to the FBCA CP in regards to PIV-I and to enhance the description of CPS activities to meet policy.	3.2	19 July 2010
Updated to address comments from the Day 0 Audit, September 2010.	3.3	29 September 2010
Updated to include the SHA1 FRCA.	3.4	15 November 2010
Combined CPS for FBCA and Common Policy into a single document. Updated to remove information for Legacy CAs and to address findings and recommendations from final Audit of Legacy CAs.	4.0	28 November 2011
Revisions in response to annual PKI audit findings and recommendations. Audit conducted in January 2012.	4.1	26 March 2012
Revisions in response to FPKI Systems Compliance Audit Report Triennial Audit Year 1 findings and recommendations. Audit conducted March 2013.	4.2	27 June 2013
Revisions in response to FPKIPA Chair review	4.3	16 October 2013
Updated for production site relocation	4.4	22 April 2014
Revisions in response to FPKI Compliance Audit Report Triennial Audit Year 2 findings and recommendations. Audit conducted May 2014.	4.5	4 August 2014
Revisions in response to FPKI Compliance Audit Report Triennial Audit Year 3 findings and recommendations. Audit conducted May 2015.	4.6	30 June 2015
Operational updates and revisions in response to FPKI Compliance Audit Report Triennial Audit Year 1 findings and recommendations. Audit conducted June 2016.	4.7	30 July 2016
Operational updates and revisions in preparation for upcoming FPKI Compliance Audit Report Triennial Audit Year 2 to be conducted June 2017.	4.8	30 April 2017
Operational updates and revisions in response to FPKI Compliance Audit Report Triennial Audit Year 2 findings and recommendations. Audit conducted June 2017.	4.9	7 August 2017
Operational updates and revisions in response to the FPKI Compliance Audit Report findings and recommendations. Audit conducted June 2018. Incorporated Common CP CR# 2017-02, 2017-03, 2017-04, 2018-01, 2018-02, 2018-03, 2018-04.	4.10	13 July 2018

Incorporated Bridge CP CR# 2017-02, 2017-03, 2017-04, 2017-05, 2018-01, 2018-02, 2018-03, 2018-04.		
Incorporated Common CP CR# 2018-05 Incorporated Bridge CP CR# 2018-05	4.11	10 December 2018
Incorporated FCPCA CP CR #2018-07 Incorporated FBCA CP CR #2019-01 CR reviewed with no impact: FCPCA #2018-06, FCPCA #2018-08, FBCA #2018-06 Editorial Updates Incorporated feedback from FY19 FPKI Compliance Audit Created Unredacted Version	5.0	01 October 2019
Operational updates and revisions in response to the FPKI Compliance Audit Report findings and recommendations. Audit conducted July 2019 Editorial updates.	5.1	05 May 2020
Revisions based on new FCPCA CP v2.0 published September 2020 and in response to FPKI Compliance Audit Report findings and recommendations. Audit completed August 30, 2020.	6.0	28 June 2021
Incorporated feedback from FY21 FPKI Compliance Audit. Audit and Archive revisions based on updated FCPCA CP. Removed text matching CP which is only relevant for subscriber certificates which are not in scope for this CPS Changed cross certificate to CA certificate when relevant for both FCPCA & FBCA issued certificates	6.1	15 March 2022
Incorporated feedback from FY22 Compliance Audit Updates due to FBCA CP rewrite & new archive procedures	6.2	14 December 2022

1   FPKI TRUST INFRASTRUCTURE CPS INTRODUCTION

The Federal Public Key Infrastructure Management Authority (FPKIMA) operates the certification authorities (CAs) that comprise the FPKI Trust Infrastructure. This FPKI Certification Practice Statement (CPS) documents the internal practices and procedures used by the FPKIMA for certificate lifecycle services including issuance, certificate management (including publication and archiving), revocation, and renewal or re-keying. In addition, this CPS covers the operation of systems and the management of facilities, which includes FPKI Repository functionality used to post CA certificates and certificate revocation lists (CRLs) issued by FPKI Trust Infrastructure CAs.

The scope of this CPS is limited to the two FPKI Trust Infrastructure CAs that operate in compliance with *X.509 Certificate Policy for the Federal Bridge Certification Authority* [FBCA CP] and *X.509 Certificate Policy for The U.S. Federal PKI Common Policy Framework* [FCPCA CP]. The two FPKI Trust Infrastructure CAs are:

1.   **The Federal Bridge Certification Authority (FBCA)** – facilitates interoperability between the PKIs of the U.S. Federal Government and other Entity PKI domains. The FBCA enables interoperability among Entity PKI domains in a peer-to-peer fashion. The FBCA issues certificates only to CAs designated by the Entity operating that PKI. FBCA certificates issued to Entity CAs act as a conduit of trust. The FBCA extends interoperability with non-Federal entities only when the FPKI Policy Authority (FPKIPA) has determined it is beneficial to the Federal Government.

2.   **The Federal Common Policy Certification Authority (FCPCA)** – acts as the trust anchor for the Federal Government PKI domains. The FCPCA issues certificates to Shared Service Providers (SSPs)[1] CAs approved by the FPKIPA. The Federal Legacy PKIs mapped to the FBCA at mediumHardware may also be approved to issue certificates in compliance with the FCPCA CP. Therefore, the Federal Legacy PKIs mapped to the FBCA at mediumHardware may choose to cross-certify in a peer-to-peer fashion directly with the FCPCA rather than with the FBCA. FCPCA certificates issued to Entity CAs act as a conduit of trust.

This CPS is consistent with the Internet Engineering Task Force (IETF) Request for Comments (RFC) 3647, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* [RFC 3647].

1.1   OVERVIEW

1.1.1   Certification Practice Statement

This CPS documents the practices and procedures used by the FPKIMA to operate the FBCA and FCPCA. Practices include the operation of systems, the FPKI Repository function, and management of facilities.

---

[1] The SSP program is designed to facilitate outsourcing of PKI services by Federal agencies.

1.1.2 Relationship Between the CP and the CPS

[FBCA CP] states the requirements for certificate policies that can be placed in certificates issued by the FBCA and mapped to policies defined in FPKI member CPs. [FCPCA CP] states the requirements for the issuance and management of certificates issued by the FCPCA, and requirements for the operation of the CA. This CPS states how the FPKIMA meets the specified requirements.

1.1.3 Scope

The generic term "Entity" applies equally to Federal organizations and other organizations owning or operating PKI domains (e.g., a PKI provided by a commercial service, or a bridge CA serving a community of interest).

An SSP is an Entity that issues Personal Identity Verification (PIV) credentials in addition to other types of certificates to Federal users in compliance with the [FCPCA CP].

This CPS covers CA certificates issued by the FPKI Trust Infrastructure CAs to Entity CAs including SSPs CAs. The FPKI Trust Infrastructure CAs do not issue subscriber certificates to end users, and therefore do not operate Card Management Systems or Key Escrow and Recovery systems.

1.1.4 Interoperation with CAs Issuing under Different Policies

Interoperation between CAs that issue under different policies is achieved through policy mapping with the FBCA CP and cross-certification after formal mapping and approval by the FPKIPA. The FCPCA is cross-certified with the FBCA. Legacy Federal PKI CAs mapped to id-fpki-certpcy-mediumHardware may be directly cross-certified with the FCPCA instead of the FBCA. A legacy Federal PKI is a PKI managed by a Federal agency which received approval to cross-certify with the FBCA prior to the 12/31/2005 mandate to use SSP services. No matter which FPKI Trust Infrastructure CA issues the cross-certificate to an Entity that operates in accordance to its own CP, the entity CP is mapped to the FBCA CP.

1.2 DOCUMENT NAME AND IDENTIFICATION

This document is referred to as the FPKI CPS.

The FCPCA and FBCA only issue CA certificates and certificates required for the support of the CAs. Cross-certificates issued from the FBCA in accordance with this CPS shall assert in the certificate policy extension at least one of the OIDs listed in Table 1.2-1.

The FPKI CPS supports twelve policies specified at six levels of assurance in [FBCA CP]. Each policy has an OID, to be asserted in certificates issued by the FBCA. Entity CAs may assert these OIDs in policyMappings extensions of certificates issued to the FBCA. Table 1.2-1 lists the FBCA policy OIDs registered in the NIST Computer Security Objects Register (CSOR).

Table 1.2-1. id-fpki-certpcy Policy OIDs

FBCA Policy	OID
csor-certpolicy OBJECT IDENTIFIER	::= { 2.16.840.1.101.3.2.1 }
fbca-policies OBJECT IDENTIFIER	::= { 2.16.840.1.101.3.2.1.3 }

2

id-fpki-certpcy-rudimentaryAssurance	::= { 2.16.840.1.101.3.2.1.3.1 }
id-fpki-certpcy-basicAssurance	::= { 2.16.840.1.101.3.2.1.3.2 }
id-fpki-certpcy-mediumAssurance	::= { 2.16.840.1.101.3.2.1.3.3 }
id-fpki-certpcy-mediumHardware	::= { 2.16.840.1.101.3.2.1.3.12 }
id-fpki-certpcy-medium-CBP	::= { 2.16.840.1.101.3.2.1.3.14 }
id-fpki-certpcy-mediumHW-CBP	::= { 2.16.840.1.101.3.2.1.3.15 }
id-fpki-certpcy-mediumDevice	::= { 2.16.840.1.101.3.2.1.3.37}
id-fpki-certpcy-mediumDeviceHardware	::= { 2.16.840.1.101.3.2.1.3.38 }
id-fpki-certpcy-highAssurance	::= { 2.16.840.1.101.3.2.1.3.4 }
id-fpki-certpcy-pivi-hardware	::= { 2.16.840.1.101.3.2.1.3.18 }
id-fpki-certpcy-pivi-cardAuth	::= { 2.16.840.1.101.3.2.1.3.19 }
id-fpki-certpcy-pivi-contentSigning	::= { 2.16.840.1.101.3.2.1.3.20 }

The High Assurance policy is reserved for U.S. Federal government entity PKI operation and use.

This CPS provides substantial assurance concerning identity of certificate subjects.

Subordinate CA certificates issued from the FCPCA in accordance with this CPS shall assert in the certificate policy extension at least one of the ten OIDs listed in Table 1.2-2.

CA certificates issued from the FCPCA may also assert one or more of the OIDs listed in Table 1.2-1.

Table 1.2-2. id-fpki-common Policy OIDs

FCPCA Policy	OID
id-fpki-common-policy	::= {2.16.840.1.101.3.2.1.3.6}
id-fpki-common-hardware	::= {2.16.840.1.101.3.2.1.3.7}
id-fpki-common-devices	::= {2.16.840.1.101.3.2.1.3.8}
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}
id-fpki-common-cardAuth	::= {2.16.840.1.101.3.2.1.3.17}
id-fpki-common-devicesHardware	::= {2.16.840.1.101.3.2.1.3.36}
id-fpki-common-piv-contentSigning	::= {2.16.840.1.101.3.2.1.3.39}
id-fpki-common-derived-pivAuth	::= {2.16.840.1.101.3.2.1.3.40}
id-fpki-common-derived-pivAuth-hardware	::= {2.16.840.1.101.3.2.1.3.41}

Certificates issued to CAs may contain any or all of these OIDs.

The following 3 policies will not be asserted in the certificate policies extension of certificates issued by the FCPCA, but may be mapped to the equivalent PIV-I policies in the policy mapping extension.

Table 1.2-3. id-fpki-common PIV-I Policy OIDs

FCPCA Policy	OID
id-fpki-common-pivi-authentication	::= {2.16.840.1.101.3.2.1.3.45}
id-fpki-common-pivi-cardAuth	::= {2.16.840.1.101.3.2.1.3.46}
id-fpki-common-pivi-contentSigning	::= {2.16.840.1.101.3.2.1.3.47}

Table 1.2-4. id-fpki-common PIV-I Policy OID Mapping

Issuer Domain	Subject Domain
id-fpki-certpcy-pivi-hardware	id-fpki-common-pivi-authentication
id-fpki-certpcy-pivi-cardAuth	id-fpki-common-pivi-cardAuth
id-fpki-certpcy-pivi-contentSigning	id-fpki-common-pivi-contentSigning

1.3   PKI PARTICIPANTS

The following roles are relevant to the administration and operation of the FPKI Trust Infrastructure. The responsibilities of each of the Trusted Roles are further defined in Section 5.2.1.

1.3.1 PKI Authorities

Table 1.3-1. FPKI Roles

FPKI Role	Description
Federal Chief Information Officers Council	The Federal CIO Council comprises the Chief Information Officers of all cabinet level departments and other independent agencies. The Federal CIO Council has established the framework for Federal PKI interoperability which includes overseeing the operation of the organizations responsible for governing and promoting its use. In particular, the Federal CIO Council delegates policy and practice responsibilities to the Federal PKI Policy Authority.
Federal PKI Policy Authority (FPKIPA)	The FPKIPA is a group of U.S. Federal government agencies (including cabinet-level Departments) established pursuant to the Federal CIO Council. The FPKIPA includes representatives of the Agencies that execute a Memorandum of Agreement (MOA) with the FBCA and representatives of agencies that use SSP services for their PIV credentials but have committed the resources to actively participate in the governance of the FPKI. The FPKIPA is responsible for: ● [FBCA CP] and [FCPCA CP]; ● Approving the FPKI CPS; ● Accepting applications from Entities desiring to cross-certify with the FBCA; ● Determining the mappings between certificates issued by applicant Entity CAs and the certificate policy OIDs set forth in [FBCA CP], which includes objective and subjective evaluation of the respective CP contents, and any other facts deemed relevant by the FPKIPA; ● Approving the CPS for each SSP that issues certificates under [FCPCA CP]; ● Identifying and authenticating an Entity, as well as identifying individuals authorized to represent that Entity; ● Approving the compliance audit report for each Entity CA issuing certificates under either [FCPCA CP] or an Entity CP which has been mapped to [FBCA CP]; and ● After an Entity is authorized to cross-certify with the FBCA or FCPCA, ensuring continued conformance of that Entity with applicable requirements as a condition for allowing continued interoperability using the FPKI Trust Infrastructure. The FPKIPA executes an MOA with an Entity setting forth the respective responsibilities and obligations of both parties, and the mappings between the certificate policy OIDs contained in [FBCA CP] and those in the Entity CP. When the Entity belongs to a sovereign nation, the United States Department of State may execute the MOA or delegate the authority to execute the MOA on its behalf.
FPKI Management Authority (FPKIMA)	The FPKIMA is the organization that operates and maintains the FPKI Trust Infrastructure CAs in accordance with the practices and procedures identified in this CPS on behalf of the U.S. Government under the General Services

	Administration (GSA). The FPKIMA issues certificates to external entities as authorized by the FPKIPA.is subject to the direction of the FPKIPA In addition, the FPKIMA is responsible for validating that the individuals representing an Entity in the certificate issuance process have been authorized by the FPKIPA. The FPKIMA will notify the FPKIPA of any planned change to the infrastructure that has potential to affect the FPKI operational environment at least two weeks prior to implementation.
FPKIMA Program Manager	The Program Manager is the individual within the FPKIMA who has principal responsibility for overseeing the proper operation of the FPKI Trust Infrastructure including the FPKI Repository and selecting the FPKIMA Staff. The FPKIMA Program Manager must hold a Top Secret security clearance.
FPKIMA Trusted Roles	Individuals within the FPKIMA who operate the FPKI Repository and FPKI Trust Infrastructure CAs and the FPKI Repository, including issuance of executing FPKIPA direction to issue CA certificates to Entity CAs from the FBCA or FCPCA.
Entity CA	CA within a PKI that has been designated to cross-certify directly with one of the FPKI Trust Infrastructure CAs. The Entity CA issues either end-entity certificates, or CA certificates to other Entity or external-party CAs, or both. Where the Entity operates a hierarchical PKI, the CA is typically the Entity Root CA. Where the Entity operates a mesh PKI, the CA may be any CA designated by the Entity for cross-certification with one of the FPKI Trust Infrastructure CAs. The FPKIMA issues cross-certificates to Entity CA's as authorized by the FPKIPA. This may include issuing to more than one CA for the same Entity.
Federal Bridge Certification Authority (FBCA)	The FBCA is the entity operated by the FPKIMA that is authorized by the FPKIPA to create, sign, and issue public key certificates to Entity CAs. The FPKIMA is responsible for all operational aspects of the issuance and management of cross-certificates including: - The certificate manufacturing process; - Publication of certificates; - Revocation of certificates, - Generation and destruction of FBCA signing keys; and - Ensuring that all aspects of FBCA services and FBCA operations and infrastructure related to certificates issued under [FBCA CP] are performed in accordance with the requirements, representations, and warranties of [FBCA CP].
Federal Common Policy Certification Authority (FCPCA)	The FCPCA is operated by the FPKIMA and authorized by the FPKIPA. The FCPCA includes the collection of hardware, software, and operating personnel that create, sign, and issue public key certificates to Subscribers. The FCPCA is responsible for the issuing and managing of certificates including:

6

	- The certificate manufacturing process; - Publication of certificates; - Revocation of certificates; - Generation and destruction of FCPCA signing keys; and - Ensuring that all aspects of FCPCA services, operations, and infrastructure related to certificates issued under [FCPCA CP] are performed in accordance with the requirements, representations, and warranties of [FCPCA CP].
Shared Service Provider Certification Authority (SSP CA)	An SSP CA is operated by an SSP authorized by the FPKIPA to operate under the SSP program. The SSP program is designed to facilitate outsourcing of PKI services by federal agencies.
Certificate Status Servers (CSS)	Certificate Status Servers are not currently supported in the FPKI Trust Infrastructure.

1.3.2 Registration Authorities

The FPKIMA does not operate a Registration Authority. FPKI Trust Infrastructure CAs issue CA certificates only to participating PKI CAs. The FPKIPA collects and validates the authenticity of the participating PKI CA and the identity information about the participating organization including Point of Contact (POC) information for those individuals authorized to act on behalf of the Entity in the cross-certification process. The FPKIMA verifies the information to be included in the cross-certificate and validates that the individual(s) representing the participating PKI CA matches the POC information in the Letter of Authorization (LOA) provided by the FPKIPA.

1.3.3 Subscribers

A Subscriber is the entity whose name appears as the subject in a certificate, who asserts that it uses its key and certificate in accordance with the CP asserted in the certificate, and who does not use it to issue certificates. CAs are sometimes technically considered "Subscribers" to a PKI. However, the term "Subscriber" as used in this CPS refers only to those who request certificates for uses other than signing and issuing certificates, or certificate status information. Therefore, the FPKIMA does not issue any Subscriber certificates from FPKI Trust Infrastructure CAs. Certificates issued in support of the FPKI Trust Infrastructure are only used to issue certificates and are not defined as subscribers in the context of this CPS.

1.3.4 Affiliated Organizations

FPKI Trust Infrastructure CAs issue CA certificates and certificates that support the FPKI Trust Infrastructure.

1.3.5   Relying Parties

A Relying Party is the entity that relies on the validity of the binding of the Subscriber's name to a public key. Although [FBCA CP] and [FCPCA CP] contain some helpful guidance, which Relying Parties may consider in making their decisions, Relying Parties are outside the scope of this CPS and are not controlled by the FPKIPA or the FPKIMA.

1.3.6 **Other Participants**

FPKIMA operation of FPKI Trust Infrastructure CAs under the [FBCA CP] and [FCPCA CP] requires the services of security, community, and application authorities not specifically mentioned in the CPs. The Government Information Systems Security Manager (ISSM) is assigned in writing by the appropriate GSA Authorizing Official (AO) and serves as the focal point for overseeing the implementation of adequate security within the system, including ways to prevent, detect, and recover from security problems. These functions are performed through the assessment and accreditation (A&A) process, and delegation of tasks to the Information System Security Officer (ISSO) (e.g., day-to-day monitoring of FPKIMA system security).

The ISSO is assigned in writing by the appropriate GSA AO on the recommendation of the ISSM, and is the focal point for ensuring implementation of adequate system security in order to prevent, detect, and recover from security breaches.

1.4 CERTIFICATE USAGE

1.4.1 **Appropriate Certificate Uses**

.The FBCA is intended to support applications involving unclassified information, which can include sensitive unclassified data protected pursuant to federal statutes and regulations. Each Entity-specific MOA identifies the certificate policies associated with that Entity. As described in [FBCA CP], the high certificate policy assurance level is appropriate for use where the threats to data are high, or the consequences of the failure of security services are high. This may include very high-value transactions or high levels of fraud risk. Note that the data in such transactions never traverse the FBCA infrastructure.

The FBCA issues cross-certificates to Entity CAs, and issues CRLs and Certification Authority Revocation Lists (CARLs) relating to those certificates. The FBCA issues at least one cross-certificate that asserts the id-fpki-certpcy-highAssurance OID, so the FBCA is operated at the assurance level that meets the requirements for that policy as defined in the [FBCA CP].

The FCPCA issues at least one certificate that asserts id-fpki-common-High OID, so the FCPCA is operated at the assurance level that meets the requirements for that policy.

The FCPCA is intended to support applications involving unclassified information, which can include sensitive unclassified data protected pursuant to federal statutes and regulations. Note that the data in such transactions never traverse the FCPCA infrastructure. Each SSP-specific MOA identifies the certificate policies associated with that SSP.

The FCPCA issues CA certificates to SSP and legacy Federal PKI CAs, and issues CRLs relating to those certificates.

The FPKI Trust Infrastructure may issue internal certificates to Trusted Roles and/or Trust Infrastructure devices in support of CA operations.

1.4.2 **Prohibited Certificate Uses**

FPKI Trust Infrastructure CAs do not issue certificates to end-entity Subscribers, and do not restrict the usage of certificates issued by any Entity CAs.

1.5 POLICY ADMINISTRATION

1.5.1 **Organization Administering the Document**

The FPKIMA is responsible for maintaining this CPS.

1.5.2 **Contact Person**

Questions regarding this CPS shall be directed to the FPKIMA Program Manager at fpki dash help at gsa dot gov.

1.5.3 **Person Determining CPS Statement Suitability for the Policy**

This CPS must conform to [FBCA CP] and [FCPCA CP]. The FPKIPA is responsible for asserting whether this CPS conforms to [FBCA CP] and [FCPCA CP]. The FPKIPA is also responsible for approving this CPS.

Entities must designate the person or organization that asserts that their CPS(s) conforms to their CP(s).

In each case, the determination of suitability shall be based on an independent compliance auditor's results and recommendations. See Section 8 for further details.

1.5.4 **CPS Approval Procedures**

The FPKIMA submits the FPKI CPS and the results of a compliance audit to the FPKIPA for approval. The FPKIPA votes to accept or reject the FPKI CPS and accompanying compliance audit. If rejected, the FPKIMA Program Manager will task the required FPKIMA resources to resolve the identified discrepancies. When the resolutions are documented, a compliance audit will be conducted, and the results resubmitted to the FPKIPA for review and approval.

1.6 DEFINITIONS AND ACRONYMS

1.6.1 Definitions

Note: these definitions come from the FBCA and FCPCA CPs and will be updated when the CPs are updated.

Access	Ability to make use of an information system (IS) resource.
Access Control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems.
Accreditation	Formal declaration by an Designated Approving Authority that an IS is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk
Activation Data	Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).
Applicant	The Subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed.
Archive	A collection of documents created or gathered by the CA and selected for long-term preservation as evidence of their activities.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.
Audit Log	A chronological record of information system activities, including records of system accesses and operations performed in a given period.
Audit Record	An individual entry in an audit log related to an audited event.
Authenticate	To confirm the identity of an entity when that identity is presented.

Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.
Backup	Copy of files and programs made to facilitate recovery, if necessary.
Binding	Process of associating two related elements of information.
Biometric	A physical or behavioral characteristic of a human being.
Certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its Subscriber, (3) contains the Subscriber's public key, (4) identifies its operational period, and (5) is digitally-signed by the certification authority issuing it. [ABADSG]. As used in this CPS, the term "Certificate" refers to certificates that expressly reference one or more of the OIDs of this CPS in the "Certificate Policies" field of an X.509 v.3 certificate.
Certification Authority (CA)	An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CRLs.
Certification Authority Revocation List (CARL)	A signed, time-stamped list of serial numbers of CA public key certificates, including cross-certificates that have been revoked.
CA Facility	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.
Certification Authority Software	Key Management and cryptographic software used to manage certificates.
Certificate Policy (CP)	A Certificate Policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-

based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.

Certification Practice Statement (CPS)	A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in the corresponding CP, or requirements specified in a contract for services).
Certificate Revocation List (CRL)	A list maintained by a Certification Authority of the certificates which it has issued that are revoked prior to their stated expiration date.
Common Criteria	A set of internationally-accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products.
Component Private Key	Private key associated with a function of the certificate-issuing equipment, as opposed to being associated with an operator or administrator.
Certificate Status Server (CSS)	A trusted entity that provides on-line verification to a relying party of a subject certificate's revocation status
Compromise	Disclosure of information to unauthorized individuals or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.
Computer Security Objects Register (CSOR)	Computer Security Objects Register operated by the National Institute of Standards and Technology.
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes.
Containerization	A form of operating system virtualization, through which applications are run in isolated user spaces called containers, all using the same shared operating system (OS).

Cross-Certificate	A certificate used to establish a trust relationship between two Certification Authorities.
Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS140-2]
Device	A non-person entity, i.e., a piece of hardware or a software application
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a Relying Party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate; and (2) whether the message has been altered since the transformation was made.
Discretionary Access Control	Means of restricting access to objects based on user identity.
Employee	Any person employed by an Entity as defined below.
End-entity	Relying Parties and Subscribers.
Entity	The generic term "entity" applies equally to Federal organizations and other organizations owning or operating PKI domains.
FPKI Management Authority (FPKIMA)	The FPKIMA is the organization responsible for operating the Federal Common Policy Certification Authority and the Federal Bridge Certification Authority.
Federal Public Key Infrastructure Policy Authority (FPKIPA)	The FPKIPA is the Federal Government body responsible for setting, implementing, and administering policy decisions regarding the Federal PKI Architecture.

FPKI Trust Infrastructure	The CAs and supporting Repositories managed by the FPKIMA. In this CPS, the FPKI Trust Infrastructure refers only to the FBCA, and FCPCA.
Firewall	Gateway that limits access between networks in accordance with local security policy.
Hypervisor	Computer software, firmware, or hardware that creates and runs virtual machines. A hypervisor uses native execution to share and manage hardware, allowing for multiple environments which are isolated from one another, yet exist on the same physical machine. Also known as an isolation kernel or virtual machine monitor.
Information System Security Officer (ISSO)	Individual responsible to the ISSM for ensuring the appropriate operational security of an information system throughout its life-cycle, from design through disposal.
Information System Security Manager (ISSM)	Individual responsible for a program, organization, system, or enclave's information assurance program.
Integrity	Protection against unauthorized modification or destruction of information. [NS4009]. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.
Intellectual Property	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.
Intermediate CA	A CA that is subordinate to another CA, and has a CA subordinate to itself.
Key Escrow	A deposit of the private key of a Subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the Subscriber, the terms of which require one or more agents to hold the Subscriber's private key for the benefit of the Subscriber, an employer, or other party, upon provisions set forth in

the agreement. [adapted from ABADSG, "Commercial key escrow service"]

Key Generation Material	Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.
Key Pair	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.
Letter of Authorization	Written instructions signed (manually or digitally) by the FPKIPA Chair to issue a cross-certificate to an Entity.
Memorandum of Agreement (MOA)	Agreement between the FPKIPA and an Entity allowing interoperability between the Entity CA and the FBCA.
Modification (of a certificate)	The act or process by which data items bound in an existing public key certificate are changed by issuing a new certificate
Mutual Authentication	Occurs when parties at both ends of a communication activity authenticate each other (see Authentication).
Non-Repudiation	Assurance that the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data. [NS4009]. Technical non-repudiation refers to the assurance a Relying Party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key..
Object Identifier (OID)	A specialized formatted number that is registered with an internationally recognized standards organization. The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the Federal PKI OIDs are used to uniquely identify certificate policies and cryptographic algorithms.

Offline CA	An offline certification authority is a certification authority isolated from network access, and is often kept in a powered-down state.
Out-of-Band	Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring online).
Physically Isolated Network	A network that is not connected to entities or systems outside a physically controlled space.
Privacy	Restricting access to Subscriber or Relying Party information in accordance with federal law and Entity policy.
Private Key	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.
Public Key	(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an authorized CA).
Re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate that contains the new public key.

Relying Party	A person or entity who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them.
Renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
Repository	A system containing data relating to certificates or revocation data as specified in this CPS. May refer to a directory, web server.
Revoke a Certificate	To prematurely end the operational period of a certificate effective at a specific date and time.
Risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
Secret Key	A "shared secret" used in symmetric cryptography, wherein users are authenticated based on a password, PIN, or other information shared between the user and the remote host or server. A single key is shared between two parties: the sender, to encrypt a transmission, and the recipient, to decrypt the transmission, with the shared key being generated with an algorithm agreed to beforehand by the transacting parties.
Server	A system entity that provides a service in response to requests from clients.
Signature Certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.

Structural Container	An organizational unit attribute included in a distinguished name solely to support local directory requirements, such as differentiation between Human Subscribers and devices
Subordinate CA	In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA. (See superior CA).
Subscriber	A Subscriber is an entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual, an application or network device
Superior CA	In a hierarchical PKI, a CA that has certified the certificate signature key of another CA, and that constrains the activities of that CA. (See subordinate CA).
System Equipment Configuration	A comprehensive accounting of all system hardware and software types and settings.
System Software Layer	A layer of software that manages lower layer hardware and software resources and provides services through well-defined interfaces to the higher layers of software. Examples of system software layers are virtual machines, hypervisors, operating systems, and any containerized architectures.
Technical non-repudiation	Technical non-repudiation refers to the assurance a relying party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key.
Threat	Any circumstance or event with the potential to cause harm to an IS in the form of destruction, disclosure, adverse modification of data, and/or denial of service.
Trust List	Collection of Trusted Certificates used by relying parties to authenticate other certificates
Trusted Certificate	A certificate that is trusted by the relying party on the basis of secure and authenticated delivery. The public keys included in trusted

certificates are used to start certification paths. Also known as a "trust anchor".

Trusted Timestamp	A digitally-signed assertion by a trusted authority that a specific digital object existed at a particular time.
Two-Person Control	Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed, and each familiar with established security and safety requirements.
Zeroize	A method of erasing electronically stored data, cryptographic keys, and CSPs by altering or deleting the contents of the data storage to prevent recovery of the data. [FIPS1402]

1.6.2 **Acronyms**

A&A	Assessment and Authorization
AIA	Authority Information Access
AO	Authorizing Official
CA	Certification Authority
CARL	Certificate Authority Revocation List
CD	Compact Disc
CDN	Content Delivery Network
CIO	Chief Information Officer
CISA	Certified Information System Auditor
CM	Configuration Management
CMS	Card Management System
CP	Certificate Policy
CPS	Certification Practice Statement
CPWG	Certificate Policy Working Group

CRL	Certificate Revocation List
CSOR	Computer Security Object Register
CSS	Certificate Status Server
DN	Distinguished Name
DNS	Domain Name System
EDP	Electronic Data Processing
FBCA	Federal Bridge Certification Authority
FCPCA	Federal Common Policy Certification Authority
FCPF	Federal Common Policy Framework
FIPS	(US) Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FPKI	Federal Public Key Infrastructure
FPKIMA	Federal Public Key Infrastructure Management Authority
FPKIPA	Federal PKI Policy Authority
GSA	General Services Administration
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
HVAC	Heating, Ventilation, and Air Conditioning
ICAMSC	Identity Credentialing and Access Management Steering Committee
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPS	Information Processing System
ISO	International Organization for Standardization
ISSM	Information Systems Security Manager

ISSO	Information Systems Security Officer
KVM	Keyboard-Video-Mouse
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LOA	Letter of Authorization
MOA	Memorandum of Agreement (as used in the context of this CPS, between an Entity and the FPKIPA allowing interoperation between the FPKI Trust Infrastructure CAs and an Entity CA)
N/A	Not Applicable
NARA	National Archives and Records Administration
NAS	Network Attached Storage
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OJT	On-the-Job Training
OMB	Office of Management and Budget
OS	Operating System
PACS	Physical Access Control System
PDF	Portable Document Format
PII	Personal Identifying Information
PIN	Personal Identification Number
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification Interoperable
PKCS	Public Key Certificate Standard

PKCS#10	Public Key Certificate Standard Certificate Request
PKI	Public Key Infrastructure
POC	Point of Contact
RA	Registration Authority
RFC	Request For Comments
RSA	Rivest-Shamir-Adelman (encryption algorithm)
SC	Secure Container
SHA	Secure Hash Algorithm
SHA-256	Secure Hash Algorithm, 256 bit length
SFTP	Secure File Transfer Protocol
SIR	Security Incident Report
SKI	Subject Key Identifier
SOP	Standard Operating Procedure
SP	Special Publication
SSP	Shared Service Provider
TCP	Transmission Control Protocol
TOC	Trusted Operations Center
TSEL	Transport Selector
UPS	Uninterruptible Power Supply
URI	Universal Resource Identifier
URL	Uniform Resource Locator
U.S.	United States
U.S.C.	United States Code

UUID	Universally Unique IDentifier
WWW	World Wide Web

2   PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1   REPOSITORIES

The FPKIMA operates and uses a variety of mechanisms for posting information into a Repository as required by [FBCA CP] and [FCPCA CP]. The mechanisms supported and operated include:

- Maintaining an online X.500 Directory Service System supporting Lightweight Directory Access Protocol (LDAP) v3, which allows anonymous access and retrieval of the certificate information including all cross-certificates issued by and to Federal Common Policy CA and the CRLs it issued;
- Maintaining HTTP services provided by a Content Delivery Network (CDN), which allows anonymous access and retrieval of certificate information via HTTP. This includes all cross-certificates issued by, and to, the FPKI Trust Infrastructure CAs; and the CRLs issued by the FPKI Trust Infrastructure; and
- Providing administrative access control mechanisms when needed to protect FPKI Repository information as described in later sections.

2.2   PUBLICATION OF CERTIFICATION INFORMATION

2.2.1   Publication of Certificates and Certificate Status

The FPKIMA publishes information concerning FPKI Trust Infrastructure CAs as necessary to support their use and operation described in Section 2.1. This includes

- The cross-certificates they issue and receive;
- The CRLs and CARLs they issue; and
- The self-signed root certificate for the FCPCA so it can be used as a trust anchor for the FPKI.

These repositories are available for anonymous access 24 hours a day, 7 days a week, with a minimum of 99% availability overall per year, and scheduled downtime not to exceed 0.5% annually.

The FPKIMA publishes CA certificates issued by, and to, the FPKI Trust Infrastructure in p7c files made available through a CDN.

When issued, CRLs and CARLs are published to both the FPKI X.500/LDAP directories and the CDN for the FCPCA. CRLs are published only to the CDN for the FBCA and FCPCAG2.

2.2.2   Publication of CA Information

The FPKIMA will deliver this FPKI CPS to the FPKIPA for publication.. The FPKIPA utilizes idmanagement.gov to post FPKI-related documentation and certificate activity notification information.

1) [FBCA CP], [FCPCA CP], and FPKIPA procedural documents - https://www.idmanagement.gov/governance/fpkiaudit/
2) Certificate Activity Notification on the System Notification page of the FPKI Guides website –   https://playbooks.idmanagement.gov/fpki/notifications/#notifications

The FPKIMA will notify the FPKIPA of any certificate activity at least two weeks in advance through either a pull request to the Certificate Activity Notification on the System Notification page, or sending an email to the FPKIPA at fpki at gsa dot gov. The FPKIPA then informs the FPKI Community by approving and posting the official notification to the Certificate Activity Notification on the System Notification page. The idmanagement.gov site is separate from the FPKI Repositories maintained by the FPKIMA.

2.2.3 **Interoperability**

The FPKI LDAP Directory, in the FPKI Repository, uses a standards-based schema for Directory objects and attributes. X.500-based directories are deprecated and are being replaced by HTTP-based repositories.

2.3 *FREQUENCY OF PUBLICATION*

Updates to [FBCA CP] or [FCPCA CP] are made by the FPKIPA and published to the FPKIPA web site, after updates have been made to the documents, reviewed and approved by the FPKIPA chairs. The FPKIPA is responsible for publishing the updated document within 30 days as required in the CP. Review and updates, if appropriate, are made to this CPS on an annual basis, or as needed, and are provided to the FPKIPA Chair for approval. The CPS will be posted within 30 days of being signed. Certificates are published to the FPKI repository upon acceptance of the certificate from the entity or SSP, and removed when replaced or upon revocation or expiration.

2.4 *ACCESS CONTROLS ON REPOSITORIES*

The FPKI repositories include an online Directory Service supporting LDAP V3 for publishing CRLs and certificates issued to/by the old FCPCA.

The CDN provides HTTP access to CRLs and certificate-only CMS message files with an extension of ".p7c" that contain cross-certificates issued to, and by, the current FPKI Trust Infrastructure CAs.

The FPKI online repositories reside behind a firewall protecting the FPKI from the Internet. Public anonymous read access to the FPKI Directory and web servers is allowed. Only authorized FPKIMA personnel can update the information stored on these servers.

The FPKI Trust Infrastructure CAs are enabled to generate periodic CRLs. Anonymous access is provided via LDAP (port TCP/389) and HTTP (port TCP/80) to the public.

Table 2.4-1 provides network addresses for LDAP and X.500 Directories, as well as the FPKI Repository.

Table 2.4-1. FPKI Repository Addresses

Purpose	Network Address
LDAP v3 or better	LDAP access to repositories is: ldap.fpki.gov (port 389)
FPKI HTTP	HTTP access to the CDN begins with: http://http.fpki.gov/ or http://repo.fpki.gov/. Artifacts can only be downloaded with the full URL. A list of full URLs is available in the References section under "FPKI HTTP Site Map"

3   IDENTIFICATION AND AUTHENTICATION

This Section contains the practices the FPKIMA follows in registering, identifying, and authenticating Entity CAs and sponsors involved in the certification request process.

3.1   NAMING

3.1.1   Type of Names

FPKI Trust Infrastructure CAs only generate and sign certificates that contain a non-null subject Distinguished Name (DN).

Certificates issued by the FBCA after 2019 contain the issuer DN of: C=US, O=U.S. Government, OU=FPKI, CN=Federal Bridge CA G4.

Certificates issued by the FCPCA after October 2020 contain the issuer DN of C=US, O=U.S. Government, OU=FPKI, CN=Federal Common Policy CA G2.

FPKI Trust Infrastructure CAs generate and sign certificates where the subject DN matches the DN of the CA identified in the LOA from the FPKIPA and the subject DN in the certificate request - Public Key Certificate Standard (PKCS)#10 - received from the Entity CA. These DNs contain X.520 naming elements (at least C, O, and OU), the domain component naming element (DC), or a combination of the two. The FPKI Trust Infrastructure CAs only issue CA certificates.

The certificates issued to Entity and SSP CAs have an assurance level equal to the highest level of assurance contained in the certificate policies as agreed between the FPKIPA and the CA.

3.1.2   Need for Names to Be Meaningful

The FPKI CAs support the generation and publication of cross-certificates with Entity CAs. Names used in the certificates identify the Entity CA to which they are assigned in a meaningful way. The Entity assigns the name to their CA, and the FPKIPA states that they agree that the name identifies the Entity CA in a meaningful way by including it in the LOA issued to the FPKIMA. The subjectDN in a CA certificate matches the issuerDN in the certificates that subject CA issues.

The LOA provided by the FPKIPA and the PKCS#10 request received from the Entity CA will contain the name to be used as the subject of the certificate issued by the FPKI Trust Infrastructure CA.

FPKI Trust Infrastructure CAs may issue certificates with name constraints asserted, limiting the name space of the Entity CAs to that appropriate for their domains. The appropriate name constraints will be as agreed to between the FPKIPA and Entity and specified in the LOA provided by the FPKIPA.

3.1.3   Anonymity or Pseudonymity of Subscribers

The FPKI Trust Infrastructure CAs do not issue anonymous, pseudonymous, or any other Subscriber certificates.

3.1.4   Rules for Interpreting Various Name Forms

[FBCA CP] and [FCPCA CP] contain the rules for interpreting subscriber certificate name forms.

Rules for interpreting DN forms are specified in X.501, *Information Technology – Open Systems Interconnection – The Directory: Models.*

3.1.5 Uniqueness of Names

Entities are responsible for creating meaningful names that uniquely identify their CAs. The FPKIPA manages the name uniqueness for certificates issued by the FPKI Trust Infrastructure CAs by assuring the CA names provided by the Entity appropriately identifies the relationship with the Entity. The name uniqueness verification is a manual process. Names, whether X.500 DNs or other name forms (e.g., an electronic mail address, DNS name), are approved by the FPKIPA and confirmed as being unique.

3.1.6 Recognition, Authentication, and Role of Trademarks

The FPKIPA resolves any name collisions or disputes regarding certificates issued by an FPKI Trust Infrastructure CA brought to its attention. Consistent with Federal policy, the FPKIMA will not issue a certificate knowing that it infringes upon the trademark of another.

3.2 INITIAL IDENTITY VALIDATION

An Entity registration to the FBCA service is initiated by applying to the FPKIPA[2] to obtain a cross-certificate from the FBCA to the Entity CA. This application is done using the Application for Cross-Certification, which must be filled in and signed by an Entity-authorized official. The application contains how the Entity proposes to map its CP certificate policies to the policies defined in the [FBCA CP], and how the Entity's certificate profile conforms to the [FPKI-Prof], and [PIV-I-Prof] if applicable. The application also describes how the applicant Entity's PKI has been independently audited to ensure conformance by the applicant to its own CP and CPS.

The FPKIPA evaluates the application, and either accepts the policy mapping proposed by the applicant or proposes an alternative mapping. As part of the application evaluation, the FPKIPA vets the identity of the Entity organization and the authority of the POCs to participate in the cross-certification process on behalf of the Entity organization. The FPKIPA may use one of the following methods to establish the applicant's authorization:

- Verify application information against a corporate website or corporate information website
- Public records search
- Digitally signed document of the application
- Digitally signed document of a Federal employee sponsor

If the applicant accepts the evaluated mapping, the FPKIPA executes an MOA with the applicant that reflects the respective responsibilities of the FPKIPA and the Entity along with the policy mappings. After the MOA is signed by the parties, the FPKIPA notifies the FPKIMA with an LOA to initiate the process for issuing cross-certificates to the Entity CA. The LOA issued by the FPKIPA to issue an FBCA certificate contains the ID proofing method of the entity organization and the authority of the POCs to participate in the cross-certification process on behalf of the Entity organization.

---

[2] Application for Cross-Certification -The FPKIPA may limit future cross-certifications to Bridges; the current application is in the Bridge Application Process document.

An SSP registration to the FCPCA service is initiated by an SSP applicant applying to the FPKIPA. During this process, the FPKI attorney vets the identity of the SSP applicant organization and the authority of the POCs to represent the organization. Upon successful completion of the application process, the organization is added to the Certified PKI SSP List and may be listed on the GSA Multiple Award Schedule (MAS) under Special Item Number (SIN) 541519PKI, Public Key Infrastructure (PKI) Shared Service Providers (PKI SSP) Program. After the SSP is approved, the FPKIPA notifies the FPKIMA with an LOA to initiate the process for issuing a subordinate CA certificate to the SSP CA. The LOA issued by the FPKIPA to issue an FCPCA certificate contains the ID proofing method of the entity organization and the authority of the POCs to participate in the cross-certification process on behalf of the Entity organization.

3.2.1 Method to Prove Possession of Private Key

The FPKIMA verifies that an Entity CA possesses the private key corresponding to the public key submitted with the application by using the CA application software to verify the signature on the PKCS#10 certificate request received from the Entity. The Entity should supply the subject key identifier (SKI) independently from the email or CD that contains the PKCS#10. When available, the SKI is provided on the certificate request form that accompanies the LOA. When the LOA coincides with a rekey of the Entity CA, this may not be possible. The FPKIMA will verify that the SKI in the PKCS#10 and resulting certificate match the SKI provided by the Entity. All transactions involved in cross-certificate issuance are recorded as part of the security audit data, as described in Section 5.4.1.

The FPKI does not provide hardware tokens to CAs. The FPKIMA generates a certificate based on the PKCS#10, and returns the certificate as described in *FPKIMA Standard Operating Procedures—Certificate Issuance*.

3.2.2 Authentication of Organization Identity

The FPKIMA issues cross-certificates to Entity CAs as authorized by the FPKIPA in an LOA. The FPKIPA authenticates the organization identity as part of the application and MOA processes. For non-government Applicants, the FPKIPA Attorney advises the FPKIPA on the legitimacy and authority of the Applicant organization and representation. The legal review can entail online research and verification of the authorization of the individual submitting the application and is recorded as part of the application process. For non-U.S. Applicant PKIs, the Department of State may be involved in the creation of an MOA or equivalent (i.e., advises the FPKIPA on the legitimacy and authority of the Applicant organization and its representation, advises on the need for an international treaty and may aid in that regard).

The FPKIMA will issue certificates to SSPs as directed by the FPKIPA in an LOA. The FPKIPA vets the identity of the SSP applicant organization and the authority of the POCs to represent the organization using methods described in Section 3.2.

The LOA issued by the FPKIPA to the FPKIMA contains the organization name and address, as well as point-of-contact information for individuals authorized to act on behalf of the organization during the cross-certification process. Changes to the LOA's list of authorized individuals require at least a digitally-signed email or document from an authorized POC in order to add or remove people from the list. In the event someone is unavailable, the FPKIPA validates the legitimacy and authority of the new individual.

3.2.2.1 *Authentication of Entity CAs*

3.2.2.1.1 *Entity CAs are established by the Applicant Entity*

The FPKIMA will verify that they are communicating with an Entity's authorized official by verifying that all communications are with points of contacts (POCs) listed in the LOA. In addition, the FPKIMA will verify the existence of the CA by checking that the certificate request file (PKCS#10) contains the public key specified in the certificate request form submitted and signed by an authorized individual from the CA's organization.

3.2.3 **Authentication of Individual Identity**

The only certificates the FPKI Trust Infrastructure CAs issue to individuals are those required by Trusted Roles for their responsibilities in operation of the CAs. A Trusted Role's identity is verified as part of the background investigation performed per Section 5.3.2. The Trusted Role assignment is recorded and archived per section 5.5.1.

The only device certificates issued are those required for operation of the FPKI Trust Infrastructure CAs.

3.2.4 **Non-verified Subscriber Information**

All information in cross-certificates issued by the FPKI Trust Infrastructure CAs matches information in the LOA and the Entity PKCS#10 (an Entity can send additional extensions in the PKCS#10 that are not specified in the LOA). Extension values containing URIs in the resulting certificate are validated by FPKIMA trusted roles to ensure the extension values only include URIs that are accessible or will be accessible when populated with the resulting certificate.

3.2.5 **Validation of Authority**

The FPKIMA confirms a person's authorization to act on behalf of the Entity by validating that the person is listed as a POC in the LOA. The FPKIPA validates individuals who are authorized to represent the Entity while authenticating the identity of the organization as detailed in Section 3.2.2.

3.2.6 **Criteria for Interoperation**

The FPKIPA determines the criteria for cross-certification with the FPKI Trust Infrastructure. Where certificates and CRLs are published in directories, standards-based schemas for FPKI Directory objects and attributes are used. Detailed information is available in technical guidance from the FPKIMA. The FPKIPA will ensure Participating CAs only have one trust path to the FBCA, irrespective of extension processing.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 **Identification and Authentication for Routine Re-key**

Re-keying a certificate means that a new certificate is created that has the same characteristics and certificate policies as the old one, except that the new certificate has a new, different public key (corresponding to a new, different private key), a different serial number, and maybe a different validity period. (The term re-key is sometimes used in reference to CAs with a new key and DN due to the CA not doing re-key according to the X.509 definition). CA certificates issued will have a maximum validity of 10 years, with the exception of self-signed CA certificates which may have a maximum validity period of 20 years.

New cross-certificates are issued to Entity CAs by the FBCA when the FBCA re-keys, and when Entity CAs re-key. Upon Entity CA re-key, the FPKIMA confirms with the FPKIPA that the MOA between the FPKIPA and Entity is still in good standing, and requests authorization to issue a new cross-certificate to the Entity CA. Authorization is received in the form of a digitally-signed LOA document or a digitally-signed email from the FPKIPA Chair. If a wet signature or other mechanism is used, the FPKIMA will verify the request in a secure manner with the FPKIPA Chair. Prior to issuing the LOA to the FPKIMA, the FPKIPA will verify POC information for individuals authorized to participate in the cross-certification process on behalf of the Entity. This information is verified with the individual(s) who participate in the FPKIPA on behalf of the Entity PKI.

When it is time to re-key one of the FPKI TI CAs, the FPKIMA documents the proposed plan they will follow and requests authorization to proceed from the FPKIPA. Authorization is provided in the form of an LOA from the FPKIPA Chair.

3.3.2 Identification and Authentication for Re-key after Revocation

After a certificate has been revoked other than as a result of quality control during a certificate issuance action, the initial registration process is repeated as detailed in Section 3.2. The FPKIMA must receive a new LOA before issuing a new cross-certificate to an Entity CA.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

Revocation requests can come from an authorized Entity POC or the FPKIPA. Revocation requests must be authenticated. Authentication of a revocation request from the FPKIPA or Entity is done by validating that the digital signature on the request is from the FPKIPA Chair or an authorized Entity POC, and is subordinate to the Entity CA. Revocation requests can also be authenticated by the FPKIMA contacting the authorized Entity POC using the POC information in the LOA.

If the revocation request comes from the Entity, the FPKIMA will notify the FPKIPA Chair. In this case, the revocation can take place first, followed by notification to the FPKIPA.

If the revocation request comes from the FPKIPA Chair, the FPKIMA will notify the Entity using the POC information on the corresponding LOA.

4   CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1   CERTIFICATE APPLICATION

The procedures an Entity should use to apply for one or more Entity CA certificates were developed and approved by the FPKIPA. These procedures as follows:

1. The applicant Entity completes a Cross Certification Application template, which is signed by an Entity-authorized official. The application describes how the Entity proposes to map the certificate policies present in the Entity CA CP to the certificate policies expressed in [FBCA CP], and how the Entity certificate profile conforms to [FPKI-Prof], and [PIV-I-Prof] if applicable. The application also describes how the applicant Entity PKI will be independently audited, prior to cross-certification, to ensure conformance by the applicant to its own CP and CPS. The Entity application will include the Entity CP and CPS written in [RFC 3647] format. For an SSP CA, the SSP will complete the application provided by the FPKIPA.

2. The FPKIPA acts on the application and determines whether to issue a certificate and execute an MOA with the applicant. The FPKIPA establishes the applicant's authorization to obtain a certificate and establish and record the applicant's identity per Sections 3.2 and/or 3.2.2.

3. The FPKIPA authorizes the FPKIMA to issue the certificate to the applicant CA via an LOA, signed by the FPKIPA Chair, detailing the certificate contents and authorized POCs. A certificate request form signed by the application authorized official may be included with the LOA. The FPKIPA may include a compliance statement with the LOA delivered to the FPKIMA for certificate issuance.

4. Based on the LOA provided by the FPKIPA, the FPKIMA team verifies the authenticity of the LOA and included information and then inserts the certificate contents (including policy OIDs and policy mappings) into the certificate or cross-certificate. Role or authorization information requested for inclusion is verified through the digitally-signed LOA, CRF, and/or MOA. All information inserted into a certificate is verified before inclusion and issuance.

5. Applicant CA public keys are delivered to the FPKIMA in a digitally-signed electronic certificate request (i.e., PKCS#10) message from a POC identified in the LOA via one of the following secure means:
   - Email or document with valid digital signature (certification path validates up to the FCPCA, the subject CA that has been approved for certification or cross-certification, or a root distributed by a trusted root program)
   - Secure File Transfer Protocol (SFTP) application
   - In-person: Identity credentials required are either one Federal Government-issued Picture I.D., or two Non-Federal Government I.D.s, one of which shall be a photo I.D. (e.g., driver's license)
   - CD delivered by registered mail or courier, packaged with a memo on Entity CA letterhead identifying the appropriate CA DN and the details of the request, and signed by a POC identified in the LOA (tracking numbers are exchanged via email or telephone)
   - Or other transfer methods and tools validating to FIPS 140-2

6. Identity checking and proof of possession of the private key is accomplished as described in Section 3.2.1 and Section 4.3.1.

7. If the application is authorized by the FPKIPA and requests a two-way cross-certification, the applicant-authorized official can request that the FPKIMA issue the Entity CA a PKCS#10 from the FPKI Trust Infrastructure CA prior to the applicant authorized official sending the Entity CA PKCS#10 to the FPKIMA.
8. After a certificate is issued by the FPKIMA, it is checked to ensure each field and extension is populated with the correct information before it is delivered to the applicant and posted in the FPKI Repository.

The FPKI Trust Infrastructure CAs operated under this CPS do not issue end-entity certificates.

4.1.1 Submission of Certificate Application

An Entity-authorized official submits the certificate application to the FPKIPA.

4.1.2 Enrollment Process and Responsibilities

Entities applying for cross-certification are responsible for providing accurate information on their certificate applications.

All communication among PKI Authorities supporting the certificate application and issuance process are authenticated and protected from modification. Communications may be via digitally-signed email, SFTP, or out-of-band. When electronic communications are used, digital signatures may be used to authenticate the identity of the signer and detect modifications. The digital signature must validate to the FCPCA, an FPKI affiliate Root, the subject CA of the applicant, or other root distributed by a trusted root program. When digital signature is not available, POC information supplied in the LOA is used to authenticate Entity officials. When postal or other physical means of transit are used, tracking numbers are exchanged via email or telephone. If passwords or shared secrets are used to protect electronic communications, they will be communicated in-person or via other out-of-band mechanisms.

4.2 CERTIFICATE APPLICATION PROCESSING

The FPKIPA verifies that information in certificate applications is accurate before certificates are issued. The process of verifying the information is detailed in the [BRIDGE PROCESS]. The process includes mapping CPs, technical testing, and verification of information with the Entity POC for cross-certificates. For subordinate CA certificates, information is verified with the SSP POC. The verified information is provided to the FPKIMA in the form of an LOA.

1. The FPKIMA Officer verifies that the information in the LOA is consistent with information contained in the MOA for Entities cross-certifying with the FPKI Trust Infrastructure.
2. The FPKIMA verifies the information in cross-certificates issued by the FPKI Trust Infrastructure CAs against the information specified in the LOA.
3. The FPKIMA verifies the information in cross-certificates issued by Entities to the FPKI Trust Infrastructure CAs against the information specified in the MOA.

For FPKI Trust Infrastructure certificates:

1. The FPKIMA Administrator and Officer verify the trusted role is approved by the FPKIMA Program Manager through a trusted role authorization letter.

4.2.1 **Performing Identification and Authentication Functions**

The FPKIPA performs identification and authentication of the applicant Entity following the procedures detailed in [BRIDGE PROCESS] or during the SSP acceptance process, and sends Entity POC information in the form of an LOA to the FPKIMA. The FPKIMA only corresponds with those POCs listed in the LOA, or as directed by the listed POC.

4.2.2 **Approval or Rejection of Certificate Applications**

The FPKIPA may approve or reject a certificate application.

4.2.3 **Time to Process Certificate Applications**

The time to process FBCA certificate applications requires completion of the following steps: (1) perform Entity CP to [FBCA CP] mapping to determine the appropriate policy mappings, (2) perform technical testing, (3) FPKIPA vote to approve the Entity's application, (3) obtain a signed MOA between the FPKIPA and the Entity, and (4) the FPKIPA provides an LOA to the FPKIMA.

The time to process FCPCA certificate applications requires completion of the following steps: (1) the SSPWG approves the SSP application and (2) the FPKIPA votes to approve the SSP, and (3) the FPKIPA provides an LOA to the FPKIMA.

The FPKIMA will process and issue certificates within 30 days of applicant identity verification. To complete identity verification, the FPKIMA shall have a signed LOA from the FPKIPA Chair or designee, a digitally-signed certificate request file from an authorized POC identified in the LOA, and a PKCS#10 from the Entity or SSP. All issuance artifacts are securely delivered according to Section 4.1.2.

4.3 CERTIFICATE ISSUANCE

4.3.1 **CA Actions During Certificate Issuance**

The FPKIMA issues cross-certificates to the Entity CA by the following procedure:

1. Upon receiving a signed request message (PKCS#10 message) from the Entity CA, the designated FPKI Trust Infrastructure CA software verifies the signature to prove possession of the private key and checks the PKCS#10 against the signed LOA from the FPKIPA. Then, after all requirements criteria have been satisfied, the FPKI Trust Infrastructure CA will sign and issue the cross-certificate to the Entity CA.
2. Each certificate issued by the FPKIMA is manually checked to ensure each field and extension is populated with the correct information as well as if the new certificate creates multiple trust paths, before the certificate is delivered to the Entity CA.
3. The certificate issued by the FPKIMA will be delivered to the Entity CA in a p7b file (for FCPCA issued certificates) or DER encoded .crt file (for FBCA certificates), via secure means (e.g., secure file transfer, CD delivered by registered mail or courier, or digitally-signed email).
4. If two-way cross-certification is authorized:
   a. The FPKI Trust Infrastructure CA will generate a digitally-signed certificate request message and deliver it to the Entity CA in a PKCS#10 certificate request message, via secure means.
   b. The Entity CA will sign and issue a certificate to the FPKI Trust Infrastructure CA and deliver it to the FPKIMA via secure means.

The FPKIMA will post cross-certificates in p7c files on the HTTP server. In the case of two-way cross-certificates, both cross-certificates are posted in the appropriate p7c file.

FPKI Trust Infrastructure CAs do not generate Subscriber private keys and are not in possession of Entity CA private signature keys.

4.3.2   Notification to Entity of Issuance of Certificate

The FPKIMA will notify and deliver the certificate to the Entity in a secure manner. The FPKIPA and FPKI Community will also be notified by methods included in Section 2.2.2.

4.4   CERTIFICATE ACCEPTANCE

The MOA specifies responsibilities that an Entity and the FPKIPA must perform before the FPKIPA can authorize issuance of an FPKI Trust Infrastructure CA certificate to the Entity CA. Once a CAcertificate has been issued and accepted by the Entity, interoperability with the FPKI Trust Infrastructure begins when the FPKI and Entity repositories have been updated, as appropriate. This begins the Entity's obligations under the MOA and this CPS.

4.4.1 Conduct Constituting Certificate Acceptance

For the FPKI Trust Infrastructure, failure to object to the requested certificate or its contents constitutes acceptance of the certificate.

4.4.2 Publication of the Certificate by the CA

As specified in Section 2.2.1, all CA certificates are published in FPKI and Entity Repositories.

4.4.3   Notification of Certificate Issuance by the CA to Other Entities

When an LOA is received from one of the FPKIPA co-chairs, the FPKIMA notifies the FPKI community of intent to issue a certificate to a participating PKI CA via methods included in Section 2.2.2.

The FPKIPA is notified of newly-issued participating PKI CA certificates including if the issuance creates multiple trust paths via methods included in Section 2.2.2.

4.5   KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

FPKI Trust Infrastructure CAs do not issue subscriber certificates.

4.5.2 Relying Party Public Key and Certificate Usage

Certificates issued by FPKI Trust Infrastructure CAs specify restrictions on use through critical certificate extensions, including the basic constraints and key usage extensions. Some certificate extensions that RFC5280 states must be critical, (i.e., inhibitAnyPolicy and policyConstraints) may not be marked critical by the FPKI Trust Infrastructure CAs due to known limitations in some relying party applications. The FPKI Trust Infrastructure CAs issue CRLs specifying the current status of all revoked and unexpired certificates issued by FPKI Trust Infrastructure CAs. It is recommended that Relying Parties process and comply with this information whenever using FPKI certificates in a transaction. However, enforcement of that recommendation is outside the scope of this CPS.

4.6 CERTIFICATE RENEWAL

4.6.1 **Circumstance for Certificate Renewal**

A certificate may be renewed if the public key has not reached the end of its validity period, the associated private key has not been compromised, and the subject name and attributes are unchanged. The new validity period of the renewed certificate will not extend past the maximum lifetime of the original key. Certificates may also be reissued when a CA re-keys.

If the FBCA or FCPCA performs a key rollover, the FPKIMA may issue renewed certificates for all issued CA certificates.

4.6.2 **Who May Request Renewal**

For the FBCA, the Entity or FPKIMA may request renewal of an Entity CA's cross-certificate.

An Entity CA may perform renewal of its cross-certificate with the FBCA without a corresponding request, such as when the CA re-keys by signing the previous PKCS#10 and sending the resulting certificate by agreed-upon means to the FPKIMA. Alternatively, the FPKIMA may request a renewal of the FBCA cross-certificate from the Entity CA, by sending a new PKCS#10 by agreed-upon means to the Entity.

For all Entity CAs operating under [FCPCA CP], the Entity authorizing official may request renewal of its own certificate. For the FCPCA, the FPKIMA may also request renewal of FPKI Trust Infrastructure CAs certificates. For the FCPCA, certificate renewal for reasons other than FCPCA or Entity CA re-key is approved by the FPKIPA issuing a new digitally-signed LOA from the FPKIPA Chair. The FPKIMA follows the same new issuance procedures in Section 4.3.1 to renew a certificate with the added step to verify the new certificate does not extend past the lifetime of the subject's key lifetime.

4.6.3 **Processing Certificate Renewal Requests**

Certificate renewal for reasons other than re-key of the FBCA, FCPCA, or Entity CA is approved by the FPKIPA issuing a new LOA or confirming authorization by a digitally-signed email from the FPKIPA Chair. The procedures to issue a certificate renewal are the same as for issuing a new certificate (see Section 4.3.1).

4.6.4 **Notification of New Certificate Issuance to Subscriber (i.e., Entity CA)**

See Section 4.3.2.

4.6.5 **Conduct Constituting Acceptance of a Renewal Certificate**

Failure to object to a certificate issued by an FPKI Trust Infrastructure CA constitutes acceptance of the certificate.

4.6.6 **Publication of the Renewal Certificate by the CA**

All CA certificates are published in the FPKI and Entity Repositories (see Section 2.2.1).

4.6.7 **Notification of Certificate Issuance by the CA to Other Entities**

Notification of certificate issuance is provided to all Entities by methods included in Section 2.2.2.

4.7 CERTIFICATE RE-KEY

Re-keying a certificate means that a new certificate is created that has the same characteristics and certificate policies as the old one, except that the new certificate has a new, different public key (corresponding to a new, different private key) and a different serial number, sometimes a new DN, and it may be assigned a different validity period. FBCA cross-certificates issued under this CPS to Entity CAs have a three-year maximum validity.

After certificate re-key, revocation or expiration of the old certificate is coordinated with the Entity.

4.7.1 Circumstance for Certificate Re-key

New cross-certificates need to be issued to Entity CAs by the FPKI CA when the FPKI CA re-keys, and when Entity CAs re-key.

Before an FPKI TI CA can no longer issue a CA certificate for the maximum allowed time, 10 years for SSP CA certificates in the case of the FCPCA, or 3 year cross-certificates for the FBCA, the FPKIMA will establish a new replacement CA. This may be referred to as an "FPKI CA re-key".

4.7.2 Who May Request Certification of a New Public Key

After the FPKI CA performs a re-key, the FPKIMA issues a request for a new cross-certificate (PKCS#10) from each Entity CA currently two-way cross-certified with the FBCA or FCPCA[3].

After an Entity CA performs a re-key, an Entity-authorized official issues a request for a new cross-certificate (PKCS#10) from the FPKI Trust Infrastructure CA.

4.7.3 Processing Certificate Re-keying Requests

The Entity CA's authorized officials are authenticated for the purpose of re-keying in the same manner as was used for the initial application. The FPKIMA will verify that the individuals named in the LOA are still current. Additionally, the FPKIMA verifies with the FPKIPA that the MOA between the FPKIPA and the Entity remains in good standing by receiving a new LOA from the FPKIPA or a digitally-signed email from the FPKIPA Chair confirming authorization to issue the certificate to the Entity CA.

4.7.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

For the FPKI Trust Infrastructure, failure to object to the certificate or its contents constitutes acceptance of the certificate.

4.7.6 Publication of the Re-keyed Certificate by the CA

As specified in Section 2.2.1, all CA certificates will be published in FPKI and Entity Repositories.

---

[3] Fed legacies are allowed to directly, two-way cross-certify with FCPCA.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Notification of certificate issuance is provided to all Entities by methods included in Section 2.2.2.

4.8 CERTIFICATE MODIFICATION

Certificate modification consists of creating new certificates with subject or extension information (e.g., policy mappings or subject information access) that differs from the old certificate. The new certificate may have the same or different subject public key.

After certificate modification, the old certificate may remain active if requested by the Entity or SSP. Otherwise, the original certificate is revoked upon Entity or SSP confirmation.

4.8.1 Circumstance for Certificate Modification

For cross-certificates issued by the FPKI Trust Infrastructure, certificate modification is performed if an authorized Entity POC requests a new cross-certificate because of a change to the CA or if there is a need to correct extension information.

4.8.2 Who May Request Certificate Modification

The FPKIMA or authorized POCs for the Entity CA may request certificate modification for currently cross-certified Entity CAs by sending a digitally-signed email or by using POC information from the LOA or MOA. The FPKIPA may request a certificate modification by providing a new LOA to the FPKIMA.

4.8.3 Processing Certificate Modification Requests

Certificate modification can be requested by the FPKIPA or the Entity CA for the following reasons:

- Modification of the subjectInfoAccess (SIA) extension;
- Minor name changes (e.g., change CA1 to CA2) as part of key rollover procedures; or
- If an error is discovered in a certificate.

If a certificate is modified to make a correction, the new certificate validity period retains the expiration date of the certificate being corrected. If the modification is directed by the FPKIPA, the LOA states any limitation on the validity period; if it does not, the default validity period of 3 or 10 years is used. Whenever the FPKIPA approves a new certificate for a currently cross-certified Entity, the FPKIPA and Entity perform a review of the current MOA for necessary corrections.

It is understood that modifying the certificate involves revoking the old certificate after issuing the new certificate. If the modification of the certificate is approved, so is the revocation of the old certificate.

Either a new PKCS#10 or the previous PKCS#10 can be used to process a certificate modification request.

4.8.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

For the FPKI Trust Infrastructure, failure to object to the certificate or its contents constitutes acceptance of the certificate.

4.8.6 Publication of the Modified Certificate by the CA

As specified in Section 2.2.1, all CA certificates are published in the FPKI and Entity repositories.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Notification of certificate issuance is provided to all Entities by methods included in Section 2.2.2.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

FPKI Trust Infrastructure CAs issue CRLs covering all revoked and unexpired certificates. These CRLs are published in publicly-available repositories, accessible by HTTP. The crlDistributionPoint (CDP) extension in certificates includes at least one URI indicating a location to find the current CRLs. In addition, the FPKIPA web site contains a [FPKI HTTP Site Map] that provides the HTTP locations of the latest CRLs. FPKI Trust Infrastructure CAs do not issue OCSP responder certificates. Any [FBCA CP] or [FCPCA CP] requirements related to OCSP operations are not applicable to the FPKI Trust Infrastructure CAs. The FPKIPA is notified of any revocation via methods included in Section 2.2.2 or following emergency revocation procedures in Section 5.7.

FPKI Trust Infrastructure CAs authenticate revocation requests. Revocation requests may be authenticated using the private key associated with the certificate to be revoked, regardless of whether or not the private key has been compromised.

4.9.1 Circumstances for Revocation

The FPKI Trust Infrastructure CA may revoke a certificate under the following circumstances:

1. When a certificate has been made obsolete or information in the certificate becomes invalid. This can occur when a modified certificate has been requested or an error is discovered in a certificate resulting in the FPKIMA issuing a correct certificate and revoking the certificate with the error.
2. When the privileges or mapped policies in a certificate are removed or reduced.
3. When the Entity CA has shown a violation of the MOA.
4. Private key, CA component compromise, or other emergency that may impact the integrity of the certificate or the FPKI Trust Infrastructure as determined by the FPKIMA personnel.
5. By request of the Entity CA.
6. When the Entity CA fails to adhere to the requirements of its CP or approved CPS.
7. By request of the FPKIPA.

If it is determined a private key used to authorize the issuance of one or more certificates issued by the FPKIMA may have been compromised, all certificates directly or indirectly authorized by that private key since the date of actual or suspected compromise shall be revoked or verified as appropriately issued.

4.9.2 **Who Can Request Revocation**

A certificate issued by the FPKI Trust Infrastructure to an Entity CA is revoked (1) upon direction of the FPKIPA, (2) upon an authenticated request by a previously designated Entity-authorized official (officials are specified in the MOA and/or LOA as authorized to make such a request), or (3) when the FPKIMA personnel determine that an emergency has occurred that may impact the integrity of the certificates issued by the FPKI Trust Infrastructure (see Section 4.9.1).

Requests are verified by contacting an Entity POC using POC information on the associated LOA and when possible, by validating the digital signature on a digitally-signed email or PDF file   .

CA certificates may also be revoked after a modified certificate is issued and accepted by the Entity POC. Permission to issue the modified certificate provides permission to revoke the obsolete certificate (no additional authorization is required).

To request a CA certificate issued by one of the FPKI Trust Infrastructure CAs be revoked, an authorized individual should send a digitally signed email to fpki at gsa dot gov or by reaching out to POCs in the FPKIMA or FPKIPA to begin the request process.

To request a revocation due to a suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to certificates, send an email to fpki at gsa dot gov or by reaching out to POCs in the FPKIMA or FPKIPA to begin the request process.

4.9.3 **Procedure for Revocation Request**

When the revocation request is not due to a perceived emergency, the revocation can be at a time mutually-agreed upon by the Entity authorized official and the FPKIMA. In this case, the FPKIMA notifies the FPKIPA and FPKI community of intent to revoke a certificate issued to a participating PKI CA via methods included in Section 2.2.2.

Revoked certificates are included on all new publications of the certificate status information until one CRL posting period past the expiration date of the revoked certificate.

The FPKIMA posts the CRL to the FPKI Repository (see Section 2.2.1) within 6 hours of the revocation. Certificates are removed from the CRL and/or CARL after the expiration date of the certificate. However, the revoked certificate must appear on at least one published CRL and/or CARL past the expiration date of the certificate.

If it is determined a private key used to authorize the issuance of one or more certificates issued by the FPKIMA may have been compromised, all certificates directly or indirectly authorized by that private key since the date of actual or suspected compromise shall be revoked or verified as appropriately issued.

If a revocation is due to a certificate or systems compromise or an Entity CA violation of the MOA with the FPKIPA, the FPKIMA will notify previously designated officials in all entities having a CA to which the FBCA has issued a certificate.

The FPKIMA will review all revocation requests to ensure that the revocation requests are legitimate and will then revoke the certificate, as follows:

1. An Entity-authorized official or the FPKIPA co-chairs draft an authenticated request to revoke a certificate. The individual may notify the FPKIMA Administrative Help desk

via e-mail to fpki dash help at gsa dot gov identifying the certificate to be revoked, explaining the reason for revocation

2. Upon receipt of a revocation request, the FPKIMA authenticates the request by making direct contact (call back or challenge/response telephone conversation) with the Entity POC, or a FPKIPA co-chair.
3. In the event the revocation request originates from an individual, the FPKIMA apprises the FPKIPA co-chairs and Entity CA of the request. One or both FPKIPA co-chairs will evaluate and verify the need for revocation expressed in the request. If the revocation appears to be valid, a FPKIPA co-chair will direct the FPKIMA to proceed with revocation.
4. In the event the request to revoke originates from the Entity CA, the FPKIMA apprises the FPKIPA co-chairs of the revocation request. After receiving approval from the FPKIMA PM, the FPKIMA will revoke the certificate at a mutually agreed upon time with the Entity CA.
5. In the event the revocation request originates from the FPKIPA co-chairs, the FPKIMA apprises the Entity CA of the request for revocation. After receiving approval from the FPKIMA PM, the FPKIMA will revoke the certificate at a mutually agreed upon time with the FPKIPA.
6. The FPKIMA will revoke the certificate, which automatically generates and adds a CRL entry for that certificate, within 6 hours of notification of approval by a FPKIPA co-chair, or at a mutually agreed upon time with a FPKIPA co-chair or Entity CA.
7. The FPKIMA ensures the new CRL is posted in the FPKI Repository within 6 hours of certificate revocation.
8. The Entity CA also revokes the certificate issued to the FPKI Trust Infrastructure and generates and posts a new CARL/CRL.

The FPKIMA may affect revocation of a certificate prior to notification and approval of a FPKIPA co-chair by following emergency revocation procedures consisting of the following steps:

1. Notify all identified POCs in the emergency list of FPKIMA (i.e., FPKIMA POC, Entity POCs, CPWG POC). This can be done by either:
    - Telephone (using one of callback or challenge/response protocols); or
    - Signed e-mail.
2. Revoke the cross-certificate and post the new CRL.

Once the incident has been investigated and documented, issue a new cross-certificate to replace the one that has been revoked, if directed by the FPKIPA co-chairs.

4.9.4 Revocation Request Grace Period

There is no revocation grace period for the FPKI Trust Infrastructure. The FPKIMA will revoke certificates as quickly as practical upon receipt of a proper revocation request, or at an agreed time as long as the revocation is not due to a compromise or emergency. When the revocation request is due to a compromise, the request will be processed before the next CRL is published, except for those requests received within 2 hours of CRL issuance. Revocation requests for compromise received within 2 hours of CRL issuance are processed before the following CRL is published.

4.9.5 Time Within Which CA must Process the Revocation Request

Revocation of an FPKI Trust Infrastructure CA-issued cross-certificate is accomplished by the generation and publication into the FPKI Repository of a CRL citing the cross-certificate as revoked. The updated CRL is posted within 6 hours of notification of approval by the FPKIPA, or at an agreed upon time, or in accordance with emergency procedures provided in Section 4.9.3.

Further, and separate from the publication of the CRL, prompt oral and/or electronic notification is given by the FPKIMA to all Entity POCs.

4.9.5.1 Revocation of a Cross-Certificate Issued by the Entity CA

Revocation takes effect upon the publication of status information for the cross-certificate issued to an FPKI Trust Infrastructure CA. Information about a revoked cross-certificate remains in the status information (CRL) until after the cross-certificate expires.

4.9.6 Revocation Checking Requirements for Relying Parties

Relying parties should never place any assurance in FPKI certificates that have not been validated against valid revocation status data. Use of revoked certificates could have damaging or catastrophic consequences. The matter of how often new revocation data should be obtained is a determination to be made by the Relying Party, considering the risk, responsibility, and consequences for using a certificate whose revocation status cannot be guaranteed.

4.9.7 CRL Issuance Frequency

To ensure timeliness of information, FPKI Trust Infrastructure CAs operated offline issue CRLs after performing revocations and update within 32 days from the date of previous CRL issuance if no changes were required. Certificate status information is posted within 4 hours of revocation or immediately in accordance with emergency revocation procedures provided in Section 4.9.3. The current CRL will be removed and replaced with the updated CRL.

4.9.8 Maximum Latency of CRLs

The FPKI operates offline CAs; CRLs are published the same day they are generated. All CRLs are transferred securely from the offline CA and published within 4 hours of generation.

4.9.9 On-line Revocation/Status Checking Availability

The FPKIMA has no current plans to support the Online Certificate Status Protocol (OCSP) capability for issued certificates.

4.9.10 On-line Revocation Checking Requirements

The FPKI Trust Infrastructure does not provide on-line revocation status checking services other than posting CRLs.

4.9.11 Other Forms of Revocation Advertisements Available

The FPKI Trust Infrastructure does not support any other forms of revocation advertisements.

4.9.12 Special Requirements Related To Key Compromise

In the event of an Entity CA private key compromise or loss, a CRL is published by the FPKIMA as soon as possible and always within 6 hours of notification of approval by the FPKIPA for an Entity CA cross-certified at High, 18 hours for an Entity CA cross-certified at

Medium, or within 24 hours for an Entity CA cross-certified at Basic, in accordance with procedures described in Section 4.9.3.

If one of the FPKI Trust Infrastructure CA keys is compromised, the FPKIMA will notify the FPKIPA and authorized officials of Entity CAs. If it is not a self-signed certificate, the compromised certificate will be added to the CRL and a CRL either with no nextUpdateTime or a nextUpdateTime of the expiration time of the certificate will be posted. Additionally, if the FCPCA key is compromised, all vendors with agreements to distribute the FCPCA root certificate in their commercial trust stores will be notified.

A replacement CA certificate and key pair will be generated and all cross-certified or subordinate CAs of the compromised FPKI Trust Infrastructure CA will be issued new certificates. The new certificate and new cross-certificates will be securely distributed to all Entity CAs.

4.9.13 Circumstances for Suspension

Suspension is not used by the FPKI Trust Infrastructure.

4.10 CERTIFICATE STATUS SERVICES

The FPKI Trust Infrastructure does not provide a Certificate Status Service other than posted CRLs.

4.11 END OF SUBSCRIPTION

The FPKIMA will notify Entity POCs of the pending expiration of a cross-certificate thirty (30) days prior to the expiration of that cross-certificate. If an authorized Entity POC does not initiate the process to request a new cross-certificate, the relationship terminates when the cross-certificate expires.

4.12 KEY ESCROW AND RECOVERY

4.12.1 Key Escrow and Recovery Policy and Practices

The FPKIMA does not perform any encryption key recovery functions involving Entity CAs and does not store any information encrypted by the FPKI Trust Infrastructure CAs private keys that may require key recovery capabilities. Therefore, key escrow and recovery is not used by the FPKI Trust Infrastructure.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

The FPKI Trust Infrastructure does not perform any session key encapsulation recovery functions; no subscriber key management keys are issued or used within the FPKI Trust Infrastructure.

5   FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1   PHYSICAL CONTROLS

The FPKIMA imposes physical security requirements that provide the protections specified below. All physical control requirements apply to all FPKI Trust Infrastructure CAs.

At each facility, the FPKIMA team is immediately supported by the facility team in the event of any incident that could impact facility operations or procedures, or the operation of the FPKI.

FPKI Trust Infrastructure CA equipment is housed in a locked GSA-approved container and is protected from unauthorized access while the cryptographic module is installed and activated. The cryptographic module activation information is stored on secure devices kept in a multi-party controlled security container (safe) drawer separate from the security container containing the CA.

5.1.1   Site Location and Construction

The FPKIMA operates from data centers in the United States.

At all times, all personnel gaining access to the facility must pass through the building's security checkpoint using a facility or government-issued badge. FPKIMA personnel are granted authorization for building access through a PACS system. Only specific Trusted Roles are granted cage access through those same PACS systems. Escorted access is enforced for all personnel not on a cage access list and must sign a Visitor or Personnel Sign-in Log.

FPKIMA operational sites are consistent with facilities used to house high-value, sensitive information consistent with the required physical access controls in the GSA CIO-IT Security-12-64 and designed to protect the FPKI TI CAs to the same level as the material that will be protected by the public key certificates issued by FPKI Entity CAs.

5.1.2   Physical Access

The FPKIMA only issues CA certificates and therefore does not operate any equipment dedicated to RA, CSS, CMS or Key Escrow and Recovery Services.

5.1.2.1   Physical Access for CA Equipment

FPKI Trust Infrastructure CA equipment is always protected from unauthorized access. Physical access controls are implemented to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. Every individual gaining access to the facility must pass through the facility's security checkpoint. The FPKI Trust Infrastructure CAs are secured in a two-person controlled environment. A locked safe contains the FPKI Trust Infrastructure CA system and the cryptographic module requires multi-party control to access.

When accessing the CA, the Trusted Roles sign a CA Security Container Access Log, which is checked by Trusted Roles during the monthly audits. It is retained onsite as part of the logs and reviewed by a Qualified Auditor on an annual basis.

All access into and out of the room is recorded in a manual log. In addition, the Physical Access Control System (PACS) logs those individuals who have unescorted access. The Trusted Roles accessing the FPKI Trust Infrastructure CAs record the event in both the Personnel Sign-In Log

and in the CA Security Container Access Log. The facility security guards monitor the campus physically and electronically (via video recorders), for any intrusions (authorized and unauthorized) at all times.

Access to the FPKI Trust Infrastructure CAs and private signing keys requires multi-party access. When not in use, all key material is returned to the secure container. Trusted Roles or the ISSO perform a security check of the FPKIMA spaces located in the Data Center and complete the appropriate logs (Personnel Sign-in Log, Visitors Log, Secured Container Access Log, CA IPS Secure Container Log, and others when needed), ensuring all systems are in the appropriate state, and that all sensitive material has been secured appropriately before the last authorized individual leaves the area.

5.1.3 Power and Air Conditioning

FPKIMA operational sites have backup power that will allow FPKIMA Trust Infrastructure to be powered on in case power to the facility is interrupted. The backup power will allow sufficient operating power to perform any standard CA procedures. If commercial power will be unavailable longer than the backup power capacity, the facility will notify the FPKIMA with enough time to perform any needed Trust Infrastructure operations. Backup power shall provide a minimum of six hours operation in the absence of commercial power to maintain availability and avoid denial of service.

5.1.4 Water Exposures

All servers are located on a raised platform or above floor level and away from any water. There are floor drains and below-floor water sensing devices. Master shut-off valves are located in secured areas and can be accessed by key facility members in the event of an emergency.

5.1.5 Fire Prevention and Protection

The facilities are equipped with fire detection and suppression equipment that meet local building codes.

5.1.6 Media Storage

Any media that has been digitally connected to (e.g., inserted in) a system in the FPKI Trust Infrastructure CA zone is stored at the FPKI sites or kept under two-party control when transferred between sites to protect it from unauthorized physical access, in accordance with the SOPs. Media containing data from an FPKI Trust Infrastructure system is stored in the SC to protect it from accidental damage (water, fire, electromagnetic).

5.1.7 Waste Disposal

The disposal of sensitive information is handled in accordance with the GSA Federal Acquisition Service procedures for disposal of such material.

5.1.8 Off-Site Backup

Backups sufficient to recover from a system failure are stored at each site. This is sufficient to allow the CA to be restored to its current state from a fresh installation in case of system failure. Offline CAs are backed up after every certificate issuance or revocation. The entire Offline CA, including OS, are backed up to an encrypted hard drive, and stored offline.

5.2   PROCEDURAL CONTROLS

5.2.1 **Trusted Roles**

A Trusted Role is one whose incumbent performs functions that can introduce security or operational incidents if not carried out properly, whether accidentally or maliciously. At least two people are assigned to each Trusted Role. The people selected to fill these roles are responsible for the integrity of the FPKI Trust Infrastructure CAs. The functions performed in these roles form the basis of trust for all uses of the FPKI Trust Infrastructure. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person.

Trusted Roles are officially appointed or removed through either an authorization letter or email from the FPKIMA Program Manager. There are four Trusted Roles in the FPKIMA.

1) The **Administrator** role does not issue certificates and is responsible for:
   - Installation, configuration, and maintenance of the Operating Systems (OS) and Directory, and CA Software;
   - Establishing and maintaining OS, CA, and FPKI Directory system accounts;
   - Assisting in generating and backing up FPKI Trust Infrastructure CA keys; and
   - Configuring certificate profiles or templates and audit parameters for the OS and the CA; and
   - Restarting OS and services in case of system failures.

2) The **Officer** role is responsible for issuing certificates, including:
   - Registering new Subscribers (i.e. Entity or SSP CAs) and requesting the issuance of certificates;
   - Verifying the accuracy of information included in certificates;
   - Executing the issuance of certificates;
   - Requesting, approving and executing the revocation of certificates;
   - Configuring certificate profiles or templates and audit parameters for FPKI Trust Infrastructure CA software; and
   - Generating and backing up FPKI Trust Infrastructure CA keys.

3) The **Auditor** role is responsible for:
   - Collecting, reviewing, maintaining, and archiving audit logs; and
   - Performing or overseeing internal compliance audits to ensure that the FPKI Trust Infrastructure CAs are operating in accordance with this CPS.

4) The **Operator** role does not currently exist in the CA Zone. There are no plans to utilize an Operator function in the CA Zone.

5.2.2 **Number of Persons Required per Task**

To best ensure the integrity of FPKI Trust Infrastructure equipment and operation, individuals may only assume one of the Officer, Administrator or Auditor roles, but any individual except the Auditor may assume the Operator Role. The separation provides a set of checks and balances over FPKI Trust Infrastructure CA operation. Where multi-party control is enforced, which includes all operational activities involving a CA, the participants will be at a minimum an

Administrator and an Officer.   Under no circumstances does any FPKI Trusted Role perform its own auditor function.

5.2.3 Identification and Authentication for Each Role

The individual Trusted Role shall identify and authenticate themselves using a unique credential assigned to a single individual before being permitted to perform any actions set forth above for that Trusted Role. Trusted Roles with operating system access are given role-based access control on the system enforced by security groups. Multi-party control to physically access CA systems is enforced while logical access to perform CA functions requires multi-party or multi-factor authentication.

5.2.4   Separation of Roles

The FPKI Trust Infrastructure CA, which is operated at the high CP assurance level, enforces separation of roles. FPKIMA personnel are individually assigned to a Trusted Role defined in Section 5.2.1. Individuals may only assume one of the Officer, Administrator, and Auditor Roles. The FPKIMA ensures no individual shall have more than one identity or can:

- Assume both the Administrator and Officer roles; or
- Assume the Auditor and any other role.

Audit log data is generated automatically by FPKI Trust Infrastructure CAs for all access to FPKI Trust Infrastructure CA activities.

5.3 PERSONNEL CONTROLS

5.3.1 Qualifications, Experience, and Clearance Requirements

The FPKIPA and the FPKIMA are responsible and accountable for the operation of the FPKI Trust Infrastructure.

All persons filling Trusted Roles are selected on the basis of loyalty, trustworthiness, and integrity, and are U.S. citizens. The FPKIMA PM and program management team are responsible for evaluating the qualification of each individual selected for a trusted role. The ISSO has oversight of the security training provided to trusted roles, and the Operations Team Lead provides oversight of functional role training.

Personnel security procedures are in place, which include separation of duties (in compliance with the CP), least privilege, and individual accountability to mitigate internal security risks due to the actions of personnel.

5.3.2 Background Check Procedures

FPKIMA Trusted Roles hold Top Secret clearances that require extensive background checks by Government Security personnel. Top Secret clearances are further subject to periodic reviews at least every five years.

5.3.3 Training Requirements

All Trusted Roles undergo security awareness training prior to their appointment to a Trusted Role and on a periodic basis. They are also trained on the operations of the system.

All personnel performing duties with respect to the operation of the FPKI Trust Infrastructure receive comprehensive training. Training (including On-The-Job-Training (OJT) and review of procedures) is conducted in the following areas by systems engineers:

- CA/RA security principles and mechanisms;
- All PKI software versions in use for the FPKI Trust Infrastructure CAs;
- All PKI duties they are expected to perform; and
- Disaster recovery and business continuity procedures.

Training in the overall security procedures of the FPKI Trust Infrastructure is conducted for all personnel at the initial full-operation capability of the FPKI Trust Infrastructure. When a person is assigned to a new FPKI Trusted Role, they receive training in all the operational duties for that role; including a period of shadowing another in that role and then a period of reverse shadowing. In addition, training and review of security procedures is conducted at the time a change in procedures occurs and/or annually. Personnel are required to sign acknowledgements that they have received this training. All personnel training records are maintained by the ISSO and Operations Team Lead.

5.3.4 Retraining Frequency and Requirements

Any significant change to the operations is documented, and personnel are informed and made aware of changes in accordance with the personnel training procedures defined in the SOPs. All FPKIMA personnel participate in mandatory refresher training annually to ensure all affected personnel are aware of new changes to procedures and configuration changes. In addition, immediate OJT is conducted when any changes occur within FPKI Trust Infrastructure operations. Examples of such changes are FPKI Trust Infrastructure CA software or hardware upgrades, changes in automated security systems, and relocation of equipment. The ISSO maintains a record of the training received by each person assigned to an FPKI Trusted Role.

5.3.5 Job Rotation Frequency and Sequence

Any rotation or termination of FPKIMA personnel shall not impact the continuity and integrity of the FPKI services. Since there are multiple people fulfilling each trusted role, there is time to identify and train a replacement any time one individual rotates or terminates his/her position within the FPKIMA.

5.3.6 Sanctions for Unauthorized Actions

The FPKIPA takes appropriate administrative and disciplinary actions against personnel who have performed unauthorized actions involving the FPKI Trust Infrastructure or its Repository. In the event of an unauthorized action, the ISSO immediately investigates the incident. After the investigation, the ISSO and ISSM determine if the action warrants disciplinary actions based on severity and the recurring frequency of the indiscretion. If the unauthorized action is a significant indiscretion, it is reported to the FPKI Program Manager and the FPKIPA. If the incident is not severe, immediate remedial training is conducted to ensure the offending party is made aware of his/her action and trained on the correct actions to prevent further indiscretions.

5.3.7 Independent Contractor Requirements

Contractor personnel employed to perform functions pertaining to the FPKI Trust Infrastructure will have the necessary experience, as determined by their supervisor and Program Manager, to be able to fulfill the required functions of their assigned role when given appropriate training on FPKIMA operational procedures. All personnel assigned to the FPKIMA will be U.S. citizens.

All personnel assigned to FPKIMA Trusted Roles will hold an active U.S. Government Top Secret clearance. FPKIMA contractors and subcontractors are contractually obligated to perform their duties in accordance with this CPS.

5.3.8 Documentation Supplied To Personnel

The FPKIMA makes available to all of its personnel the [FBCA CP], [FCPCA CP], this FPKI CPS, FPKIMA standard operating procedures (SOPs), and any relevant statutes, policies or contracts when an individual is first assigned to an FPKIMA role.

When these documents are revised, FPKIMA personnel are notified of the changes and updated documents are provided in electronic format via SFTP or a secure file storage site.

5.4 AUDIT LOGGING PROCEDURES

The objective of audit log processing is to ensure that all actions are being made by authorized parties and for legitimate reasons.

The FPKIMA generates audit log files for all events (identified in Section 5.4.1) relating to the security of the FPKI Trust Infrastructure CAs, and makes these files available to Auditors during monthly audits as well as for third-party audits. Audit logs are collected for physical machines, virtual machines (VM), and hypervisors. In addition to the audit logs detailed below, information relevant to certificate issuance and certificate revocation events is captured on certificate issuance and certificate revocation forms. Where this is not possible, a logbook, paper form, PDF, or other physical or electronic mechanism is used to capture the data. Paper records are scanned to PDF and stored by Auditors at each monthly audit.

Audit record reviews are performed using an automated process to identify relevant events and anomalies; reviews include verification that the logs have not been tampered with, an inspection of log entries, and a root cause analysis for any alerts or irregularities. Reviews are performed manually for physical or non-electronic records and logs.

All anomalous events are analyzed to determine the cause and to ensure that the system is operating correctly. All anomalous events are maintained by Auditors in an anomaly tracker.

A record of the review, all significant events, and any actions taken as a result of these reviews are explained in an audit log summary completed by Auditors at each monthly audit. This review summary is retained as part of the long-term archive.

5.4.1 Types of Events Recorded

Security auditing capabilities of the FPKI Repository, the FPKI Trust Infrastructure CA operating system, and FPKI Trust Infrastructure CA applications have been enabled for logging the types of events specified in Table 5.4-1. The table indicates whether the auditable event is logged automatically by the application/operating system, is logged manually in a logbook as prescribed by applicable procedures, or both. Requests for certificate issuance or revocation by any FPKI Trust Infrastructure CA is documented and retained by way of LOAs, Certificate Activity Forms, or emails for retention in the archive. At a minimum, each audit record includes the following (either recorded automatically or manually for each auditable event):

- The type of event;
- The date and time the event occurred;

- Where the event occurred (e.g., on what systems or in what physical locations);
- Source of the event;
- A success or failure indicator when executing the FPKI Trust Infrastructure CA signing process;
- A success or failure indicator when performing certificate revocation; and
- The identity of the entity and/or operator (of the FPKI Trust Infrastructure CA) that caused the event.

The FPKIMA staff has verified that the equipment and application software supports capturing audit logs for the events specified in the table below. Firewall logs are also used to audit who is accessing or attempting to access the system. System logs and firewall operating system access logs are audited. Manual audit artifacts such as sign-in logs and key signing ceremony documents are audited and retained.

Table 5.4-1. Auditable Events

Auditable Event	FPKI System			CA		
	Manual	**Automatic**	**Location**	**Manual**	**Automatic**	**Location**
SECURITY AUDIT						
Any changes to the Audit parameters, e.g., audit frequency, type of event audited	✓	✓	CM Package OS and Event Logs	✓	✓	CM Package OS and CA Logs
Any attempt to delete or modify the Audit logs		✓ After a modification following any archive operation	OS and Event Logs SIEM		✓	OS Logs CA Audit Log
IDENTIFICATION AND AUTHENTICATION						
Platform or CA application level authentication attempts		✓	OS and Event Logs		✓	OS and CA Logs
Change in the value of maximum authentication attempts	✓	✓	CM Package OS and Event Logs	✓	✓	CM Package OS Logs
Maximum number of unsuccessful authentication attempts during user login		✓	OS and Event Logs		✓	OS Logs
An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts		✓	OS and Event Logs		✓	OS Logs
An Administrator changes the type of authenticator, e.g., smart card login to password	✓		CM Package	✓		CM Package
DATA ENTRY AND OUTPUT						
Any additional event that is relevant to the security of the		✓	OS and Event Logs		✓	OS Logs

CA (such as remote or local data entry or data export); must be documented					
KEY GENERATION					
Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys)				✓	✓	Key Signing Ceremony CA Audit Log
PRIVATE KEY LOAD AND STORAGE					
The loading of CA, RA, CSS, CMS, or other keys used by the CA in the lifecycle management of certificates					✓	HSM logs(backup and restore from backup device)
All access to certificate subject private keys retained within the CA for key recovery purposes					✓	HSM logs(backup and restore from backup device)
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE					
Any changes to public keys used by components of the CA to authenticate other components or authorize certificate lifecycle requests (e.g., RA or CMS trust stores)				✓	✓	Key Signing Ceremony Decommission Documents CA Audit Log
PRIVATE AND SECRET KEY EXPORT					
The export of private-keys (keys used for a single session or message are excluded)				✓	✓	HSM logs(backing up partition to backup device)
CERTIFICATE REGISTRATION					
All records related to certificate request authorization, approval and signature, whether generated directly on the CA or generated by a related external system or process				✓	✓	CA Audit Log CRFs, LOAs & Certificate Activity Approval forms
CERTIFICATE REVOCATION					
All records related to certificate revocation request authorization, approval and execution, whether generated directly on the CA or generated by a related external system or process				✓	✓	CA Audit Log LOAs & Certificate Activity Approval forms (when applicable)
CERTIFICATE STATUS CHANGE APPROVAL					

All records related to certificate status change request authorization, approval and execution, whether generated directly on the CA or generated by a related external system or process				✓		Letter of Authorization MOA
CA CONFIGURATION						
Any security-relevant changes to the configuration of the CA. The specific configuration items relevant to the environment in which the CA operates must be identified and documented.				✓	✓	CM Package OS Logs
ACCOUNT ADMINISTRATION						
Roles and users are added or deleted	✓	✓	OS and Event Logs Training records and access list	✓	✓	OS Logs Training records and access list
The access control privileges of a user account or a role are modified	✓	✓	OS and Event Logs Training records and access list	✓	✓	OS and CA Logs Training records and access list
CERTIFICATE PROFILE MANAGEMENT						
All changes to the certificate profile				✓	✓	PA Meeting Minute/Change Proposal CA Audit Log
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT						
All changes to the certificate revocation list profile				✓	✓	PA Meeting Minutes/Change Proposal CA Audit Log
MISCELLANEOUS						
Appointment of an individual to a designated trusted role	✓					
Installation of the Operating System	✓	✓	Install and Setup Log CM Package OS and Event Logs	✓	✓	Install and Setup Log CM Package OS Logs
Installation of the CA				✓	✓	CA Install Log Build Documents CM Package for new or changed baselines OS Logs
Installing hardware cryptographic modules				✓	✓	CM Package Build Documents HSM Logs

Removing hardware cryptographic modules				✓		CM Package
Destruction of cryptographic modules				✓		CM Package or Decommission Package
System Startup		✓	OS and Event Logs	✓	✓	OS Logs HSM Logs
Logon Attempts to CA Apps					✓	CA Audit Log OS Logs
Receipt of Hardware / Software	✓		Purchase or Receiving Documents	✓		Purchase or Receiving Documents
Attempts to set passwords	✓		OS and Event Logs		✓	OS Logs
Attempts to modify passwords	✓		OS and Event Logs		✓	OS Logs
Backing up CA internal database					✓	CA Database Logs Backup log when generated
Restoring CA internal database					✓	CA Database Logs Backup log when generated
Records of manipulation of critical files (e.g. creation, renaming, moving), critical files will vary between installation, and must be identified in the relevant documentation	✓	✓	CM Package OS and Event Logs	✓	✓	CM Package OS Logs
Posting of any material to a repository	✓	✓	Community Notifications & Reports			
The date and time any CA artifact is posted to a public repository	✓	✓				Emails from FPKIPA for documents posted to idmanagement.gov
Access to CA internal database					✓	OS Logs CA Audit Log CA Database Logs
All certificate compromise notification requests				✓		Certificate Revocation Form
Loading tokens with certificates				✓	✓	CM Package Cryptographic module Syslog
Shipment and receipt of tokens containing key material, or tokens that allow access to key material (e.g., HSM operator cards)				✓		Purchasing and Receiving Document(s)
Zeroizing tokens					✓	Cryptographic module

						Syslog
Rekey of the CA				✓	✓	Key Signing Ceremony CA Audit Log
Configuration changes to the CA server involving:						
Hardware				✓	✓	CM Package OS Logs
Software				✓	✓ (Application Specific)	CM Package CA Audit Log
Operating System				✓	✓	CM Package OS Logs
Patches				✓	✓	CM Package OS Logs Patch Log
Security Profiles				✓	✓	CM Package OS Logs
PHYSICAL ACCESS / SITE SECURITY						
Personnel Access to room housing CA				✓	✓	Electronic building access log (both maintained by Colocation provider) Personnel/Visitor Sign In sheets
Access to the CA server				✓	✓	Facility Sign In Log and Electronic building access log (both maintained by Colocation provider) Personnel/Visitor Sign In sheets CA Security Container log sheets
Known or suspected violations of physical security	✓	✓	SIR Electronic building access log (maintained by Colocation provider)	✓	✓	SIR Electronic building access log (maintained by Colocation provider)
ANOMALIES						
Software Error conditions		✓	OS and Event Logs		✓	OS Logs
Software check integrity failures		✓	OS and Event Logs AV Logs		✓	OS Logs HSM Logs CA Logs
Equipment failure	✓	✓	SIR OS and Event Logs	✓	✓	SIR OS Logs

53

Electrical power outages	✓		Notification from Data Center provider	✓		Notification from Data Center provider
Uninterruptible power supply (UPS) failure	✓		Notification from Data Center provider	✓		Notification from Data Center provider
Network service or access failures that could affect certificate trust	✓	✓	SIR OS and Event Logs	*X*	X	*Not applicable. The CA is maintained offline, and not connected to any network.*
Violations of Certificate Policy	✓	Some violations are recorded in various electronic logs, as documented in other areas of this table	SIR	✓	Some violations are recorded in various electronic logs, as documented in other areas of this table	SIR
Violations of Certification Practice Statement	✓	Some violations are recorded in various electronic logs, as documented in other areas of this table	SIR	✓	Some violations are recorded in various electronic logs, as documented in other areas of this table	SIR
Resetting Operating System clock		✓	OS and Event Logs		✓	OS Logs HSM Logs

If the following events occur, they are manually logged:
- Obtaining a third-party timestamp
- All security-relevant data that is entered in the system
- All security-relevant messages that are received by the system
- All successful and unsuccessful requests for confidential and security-relevant information
- The manual entry of secret keys used for authentication
- Appointment of an individual to a Trusted Role
- Designation of personnel for multiparty control

5.4.2 **Frequency of Processing Log**

Audit logs from the non-CA zones are collected and processed, in an automated continuous process, checking for anomalies. The automatic logger creates alarms if anomalies are encountered. Reports of potential anomalies are reviewed at least once a month.

Logs from systems in the CA zone are collected, and are included in the potential anomalies report. CA zone logs are collected for archive at least once a month. The Auditor reviews CAs' application audit logs, CA zone audit logs and cryptographic module audit logs at least once per month.

The Auditor examines all of the collected electronic logs and reports generated at each operational site. Completed manual logs are transferred between operational sites by a Trusted

Role with unescorted cage access at least once per year and included in the following Auditor review. The Auditor examines the security audit data, paying particular attention to anomalies and suspicious entries. All security alerts and irregularities are explained in an audit log summary. The Auditor reviews include verifying that the log has not been tampered with, and then briefly inspecting log entries with a more thorough investigation of any alerts or irregularities in the logs. Actions taken as a result of these reviews are documented.

The Auditor collects and prepares audit logs for archival.

The manual logs include:
- Personnel Sign-in log
- Visitor Sign-in Log
- Secure container log
- CA IPS Security Container log
- Activity Security Checklists

The electronic logs include logs from the FPKI Trust Infrastructure CA zone servers, the CA database logs, and the cryptographic module syslog.

5.4.3 Retention Period for Audit Log

Audit logs are stored onsite on servers until the next periodic audit, and then the logs are pulled off for Auditor analysis and stored inside the Auditor security container in the FPKIMA office space. An entire year's worth of collected audit logs on disc are stored for an extra year. Multi-party control between Trusted Roles is enforced when removing audit logs from the Trust Infrastructure and given to the Auditor. Audit logs written to optical disk are labeled with the name of the program (FPKI), a description (e.g. Audit), CUI and today's date or a range of dates, if applicable.

5.4.4 Protection of Audit Log

The Auditor performs a routine review of security audit logs. The policies for protecting security audit data are as follows:

1. Security audit logs are automatically timestamped upon creation.
2. Only designated Trusted Roles and others designated by the FPKIMA Program Manager to perform security audit processing have read access to the logs.
3. Only the Auditor is authorized to archive audit logs.
4. Audit logs are deleted only under procedural multi-person control, one participating individual must be an Auditor.
5. Audit logs are protected under multi-person control, and cannot be modified without detection. One participating individual must be an Auditor.
6. Audit records written to optical disk are stored in a secure container accessible only by the Auditors. Disks may be destroyed after the designated disposal date.

Daily audit logs are generated on timestamped digital media, and are protected from deletion and modification until reviewed. System logs are automatically timestamped. Audit logs on disk are maintained until after the annual audit.

The FPKIMA maintains two internal Network Time Protocol (NTP) servers to synchronize system time for all servers, appliances, and applications within the FPKI Trust Infrastructure. The two internal servers will be synchronized to NIST.

5.4.5 Audit Log Backup Procedures

Manual audit logs are collected on at least a monthly basis and, along with an audit summary, are stored in a security container by the Auditor. Paper logs are scanned to PDF and stored on both the NAS and disk. The paper log is then shredded. Audit logs written to removable media as part of an audit are stored in a security container.

Non-CA zone logs sent to the automatic logging device are time stamped automatically and on a continual basis. Full backups of the database that stores these logs run nightly, and one week of backups are kept on network storage. The automatic logging device automatically rotates the logs to an archive, which is also maintained on network storage. The archive contains at least six months of logs from the non-CA zones. Copies of the reports of potential anomalies generated by the automatic logging device and manual paper logs are scanned and placed electronically on the monthly audit optical disks stored in a secure container.

5.4.6 Audit Collection System (Internal vs. External)

The audit log collection system is internal to the FPKI Trust Infrastructure components (see Section 5.4). Audit processes are invoked at system startup and cease only at system shutdown. Should it become apparent that an automated audit system has failed (as determined during the auditing process and documented in the auditing/trouble handling forms), and the integrity of the system or confidentiality of the information protected by the system is at risk (as determined by the ISSO in conjunction with the ISSM and Program Manager), the FPKIMA will suspend the FPKI Trust Infrastructure CA operation until the problem is remedied. Section 5.4 describes the collection procedures (manual or automatic) for the auditable events. Section 5.5 describes the protection procedures for backing up audited data that has been collected.

5.4.7 Notification to Event-Causing Subject

No notice that an event was audited is provided to the individual, organization, device, or application that caused the event.

5.4.8 Vulnerability Assessments

The FPKIMA performs self-assessments of the security controls at the time of initial installation and configuration of the FPKI Trust Infrastructure components. Periodic vulnerability assessments are performed on a routine basis as well as following a system configuration change with the potential for affecting system security (i.e., hardware, software, or network changes or upgrades). Periodic vulnerability assessments, as well as assessments of potential configuration changes are performed in a development environment.

The FPKIMA provides a report of the analysis of the results of both internal and external vulnerability assessments to the Program Manager and ISSM, specifically indicating security vulnerabilities identified and mitigation procedures of those vulnerabilities.

5.5 RECORDS ARCHIVAL

Archive procedures comply with government policy related to archival of PKI records. Prior to 2022, the FPKIMA archived records at NARA on an annual basis. NARA receipts for archived material are filed at the TOC Site. Starting with the 2022 archives, the FPKIMA stores archive records on the NAS with backup DVDs of the records stored in the Auditor safe at the TOC. Archive records on the NAS are separated by which CA they are associated with, as the retention period requirements are now associated with the lifetime of the CA.

5.5.1 **Types of Events Archived**

CA archive records must be sufficiently detailed to determine the proper operation of the CA and the validity of any certificate (including those revoked or expired) issued by the CA. At initialization, FPKI Trust Infrastructure system equipment configuration files were archived, as well as the CPS and any contractual agreements to which the FPKIMA is bound. During FPKI Trust Infrastructure operation, the following data are recorded for archive:

Table 5.5-1. Types of Events Archived

CP Archive Requirements	CPS Artifact to be Archived
FPKI Trust Infrastructure Certification and accreditation	FPKIMA ATO Letter, Report, and Documentation
Certificate Policy	FBCA and FCPCA Certificate Policy
Certification Practice Statement	FPKI Certification Practice Statement
Contractual obligations	MOAs
Other agreements concerning operations of the FPKI Trust Infrastructure CAs	Entity Records
FPKI Trust Infrastructure System and Equipment Configuration Documentation	Build Documentation / Change Requests / Maintenance Logs
Modifications and updates to system or configuration	Change Requests / Maintenance Logs
All records related to certificate request authorization, approval and signature, whether generated directly on the CA or generated as part of a related external system or process	LOA / P10 File / Certificate Issuance Form / MA Activity Approval Form
All records related to certificate revocation, whether generated directly on the CA or generated as part of a related external system or process	Certificate Revocation Form / MA Activity Approval Form (as applicable)
Subscriber agreement and identity authentication data as per Section 3.2	LOA (ID Authentication) /Application / Subscriber Agreement / MOA (as applicable)
Documentation of receipt and acceptance of certificates	Email or other out-of-band notification from Entity (if applicable)
Documentation of receipt of tokens	N/A (Do not issue tokens)
All certificates issued or published	Issued Certificates
Record of FPKI Trust Infrastructure CA Re-key	Key Generation or Rollover Package
Other data or applications to verify archive contents	Prior to 2022: SF-135 – NARA Records Transmittal and Receipt 2022 and later: Annual Archive Package List File Listing (for each CA)t
Audit summary reports generated by internal review	Monthly Audit Items Package List & Audit Summary
Documentation generated during third party audits	FPKIMA Annual PKI Compliance Reports
Any changes to the Audit parameters, e.g., audit frequency, type of event audited	Audit SOP / Change Requests / Change Management Log
Any attempt to delete or modify the Audit logs	Security Incident Report (if applicable)
Whenever the FPKI Trust Infrastructure CA generates a key. (Not mandatory for single session or one-time use symmetric keys)	Key Generation or Rollover Package / CA Audit Log

All access to certificate subject private keys retained within the FPKI Trust Infrastructure CA for key recovery purposes	N/A (The FPKI Trust Infrastructure CAs do not have access to affiliate/subject private keys)
Changes to trusted public keys used or published by the CA including certificates used for trust between the CA and other components such as CMS, RA, etc.s	Issuance Form / Key Generation Documentation
The export of private and secret keys (keys used for a single session or message are excluded)	Cryptographic Module Log
The approval or rejection of a certificate status change request	Email
Appointment of an individual to a Trusted Role	Digitally Signed Document or Email Describing Role Changes and/or Document Authorization
Destruction of cryptographic modules	Receipt / Certificate of Destruction and Recycling / Decommission Documentation
All certificate compromise notifications	Authenticated Revocation Request
Remedial action taken as a result of violations of physical security	System Incident Report (SIR)
Violations of Certificate Policy	System Incident Report (SIR)
Violations of Certification Practice Statement	System Incident Report (SIR)

See Sections 5.4.6 and 5.5.6 for a description of the audit and archive collection procedures.

5.5.2 Retention Period for Archive

Items that are required to be archived are stored on the FPKIMA controlled NAS and retained for the required period of 3 years past expiration or decommission of the FPKI Trust Infrastructure CA. Other items, such as signed certificates and CRLs, are backed up and stored on the servers themselves. This ensures that there is always a copy available.

5.5.3 Protection of Archive

Archive data is stored on the FPKIMA controlled NAS. Only an Auditor has read-write access to archive files. Other Trusted Roles have read-only access. Archive data is clearly labeled to identify the program name and appropriate dates of the artifact.

The archive data stored on removable media is stored in an auditor controlled security container at the TOC facility, which is separate from the location of the CAs, temperature-controlled and behind locked doors.

The contents of the archive will not be released except as determined by the FPKIPA or as required by law. Any request for archived information must be made to the FPKIMA Program Manager, who in consultation with the ISSM will determine if the requested information may be provided. If release of such information is authorized, the ISSM and Program Manager inform the ISSO, who will provide the information.

5.5.4 Archive Backup Procedures

The FPKIMA maintains a backup of the archive data on optical disks stored in the auditor controlled security container at the TOC facility,

5.5.5 Requirements for Time-Stamping of Records

Records are clearly labeled with date/time period information of the data contained in the record. System clocks are kept synchronized via NTP and system logs are automatically timestamped. Time for offline systems are synchronized manually.

5.5.6 Archive Collection System (Internal or External)

The archive information is collected by the Auditor, who (using a checklist) is responsible for assuring that all records required for the archive are correctly filed.

5.5.7 Procedures to Obtain and Verify Archive Information

The FPKIMA Auditor maintains logging information (and receipts) from archived data stored at NARA prior to the 2022 archive.

If archive material prior to 2022 records need to be retrieved from NARA, the FPKIMA Auditor makes the request of NARA via GSA Records Officers. Once received, the FPKIMA Auditor verifies the received data against the logging information and receipts. Contents of FPKIMA archives are only released upon request of the FPKIPA. Individual records pertaining to a specific Entity can be released to the authorized POC for that Entity upon Entity POC request.

5.6 KEY CHANGEOVER

The FPKI Trust Infrastructure CA key changeover procedures may be done in one of two methods:

Either:

1. The FPKI Trust Infrastructure CA will generate a self-issued certificate signed by the old private key whose *subjectPublicKeyInfo* field contains the new public key.
2. The FPKI Trust Infrastructure CA will generate a self-issued certificate signed by the new private key whose *subjectPublicKeyInfo* field contains the old public key.
3. The FPKI Trust Infrastructure CA will generate a self-signed certificate signed by the new private key whose *subjectPublicKeyInfo* field contains the new public key.
4. The FPKI Trust Infrastructure CAs and all Entity CAs will process new cross-certificates as described in this CPS.

Or:

1. The FPKIMA will establish a new FPKI Trust Infrastructure CA appending either a generational number or a year to the end of the commonName attribute of the subjectDN.
2. All required cross-certificates between the new and other FPKI Trust Infrastructure CAs will be issued. (For example between the FCPCA and a new FBCA).

For both alternatives:

- All certificates generated as part of the key changeover process will be posted to the FPKI Repository.
- The old FPKI Trust Infrastructure CA private key is used to sign CRLs that contain certificates signed with that key as long as required. The old key is retained and protected.

The FBCA signing key has a validity period of six years, and its corresponding certificate has a validity period of ten years.

The FBCA will support Entity CA key changeovers by issuing and posting new certificates as required.

The FCPCA signing key has a validity period of ten years, and its corresponding certificate has a validity period of twenty years.

The FCPCA will support Entity CA key changeovers by issuing and posting new certificates as required.

The old private key is used to sign CRLs that contain certificates signed with that key as long as required. The old key is retained and protected.

After a key changeover, the FPKIMA may transition all Entity CAs to the new key by issuing new CA certificates from the new key with the same expiration of the current certificate, and when appropriate requesting a new cross-certificate from the Entity CA for the new key. After an Entity CA has certificates with the new key, those associated with the old key can be revoked. Once all Entity CAs have been transitioned to the new key, the old key or CA may be terminated. See Section 5.8.

5.7   COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

The FPKIMA responds to all incidents and suspected compromise events. Detailed procedures are explained below.

In the event of a disaster, the following steps will be executed to regain system functionality:

1. Coordinate activities with individual facility owners. These individuals along with the FPKIMA will assess the outage and determine whether all or part of the Recovery team needs to be assembled.
2. Activation of the Damage Assessment and Disaster Recovery team.
3. Based on the severity of the event, activate the recovery procedures for that severity type.
4. Interface with the FPKIMA Management Team.
5. The FPKI Repository services are served by an externally-operated CDN service with service level agreement requirements that exceed FPKI availability requirements.
6.
7. Manage the recovery process of the affected facility.
8. Submit post recovery logs to FPKIPA.

The FPKIPA will be notified if any of the following is experienced by the FPKI Trust infrastructure:

● Suspected or detected compromise of FPKI Trust Infrastructure systems;

● Physical or electronic penetration of FPKI Trust Infrastructure systems;

● Successful denial of service attacks on a FPKI Trust Infrastructure component;

● Any incident preventing the FPKI Trust Infrastructure from issuing a CRL within 48 hours of the issuance of the previous CRL.

[FPKIMA IMP] will be followed to investigate and diagnose the suspected incident. The FPKIPA and other appropriate government and non-government organizations will be notified as soon as possible as described in the [FPKIMA IMP]. The FPKIMA will submit a preliminary remediation analysis to the FPKIPA within 24 hours of incident discovery. Within 10 business days after the incident resolution, the FPKIMA will publicly post a notice on idmanagement.gov or other FPKIPA designation public website. The public notice will include:

1) Which CA component(s) were affected
2) FPKIMA interpretation of the incident
3) Who was impacted by the incident
4) When the incident occurred
5) A complete list of erroneously issued or non-compliant certificates as a result of the incident.
6) A statement the incident is fully remediated with the measures taken to remediate the incident.

Incident response policies and procedures have been developed and documented, and are reviewed and updated periodically.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

In the event FPKI Trust Infrastructure CA equipment is damaged or rendered inoperative, but the FPKI Trust Infrastructure CA signature keys are not destroyed, FPKI Trust Infrastructure CA operation is reestablished as quickly as possible, giving priority to the ability to generate certificate status information.

In order to provide a 6-hour window for FPKI Trust Infrastructure CA service re-activation, the FPKIMA maintains full capabilities at all operational sites.

During system restoration, the FPKIMA needs to ensure the CRLs of FPKI Trust Infrastructure CAs are current with the latest Entity CA certificates revoked. Additionally, cross-certificates need to be validated, and new public keys/cross-certificates issued in the event anomalies exist.

The following reports are generated:

● Activity log – this log is maintained throughout the disaster recovery process;
● Test plan results;
● Equipment list – Update configuration management; and
● Restoration Expense report.

The FPKIMA will publicly post a remediation notice following Section 5.7.1.

5.7.3 Entity (CA) Private Key Compromise Procedures

If the FPKI Trust Infrastructure CA signature keys are compromised or lost (such that compromise is possible even though not certain) the following procedure is executed:

1. The FPKIPA and all member Entities will be securely notified (so that Entities may issue CARLs revoking any cross-certificates issued to the FPKI Trust Infrastructure CAs) via telephone to the designated POCs.
2. If possible, the self-signed certificate of the compromised key will be revoked. A compromised key can be used to sign the new CRL.
3. The Entity CAs that have issued certificates to the FPKI Trust Infrastructure CAs will publish a CARL revoking the cross-certificate issued to the FPKI Trust Infrastructure CAs as set forth above.
4. The FPKI Trust Infrastructure CA will generate a new CA key pair and self-signed certificate in accordance with procedures set forth in Section 6.1.
5. New CA certificates[4] will be issued to all Entity CAs in accordance with Section 4.3.
6. New FPKI Trust Infrastructure root certificates will be securely distributed along with the new Entity CA certificates.

The FPKIMA will also investigate and report to the FPKIPA what caused the compromise or loss, and what measures have been taken to preclude recurrence. The FPKIMA will publicly post a remediation notice following Section 5.7.1.

5.7.4 Business Continuity Capabilities After a Disaster

The FPKI Trust Infrastructure CA servers operate with back-up power and telecommunications and appropriate infrastructure system redundancies to minimize outages. However, if an outage appears likely to become, or becomes an extended outage, the disaster recovery plan will come into effect. An extended outage is currently defined as one in which the ability of the FPKI Trust Infrastructure CAs to revoke certificates cannot be re-established within 24 hours. However, the FPKI Trust Infrastructure has the ability to respond to an extended outage at one site. FPKI Trust Infrastructure operations are redundant across both sites and will tolerate a complete outage at either site.

In the case of a disaster whereby operational sites are physically damaged, the FPKIPA and all of its member entities will be securely notified, and the procedures described in Section 5.7.3 will be followed. FPKI Trust Infrastructure CA installation will then be completely rebuilt by reestablishing the FPKI Trust Infrastructure CA equipment, generating new private and public keys, being re-certified, and re-issuing all CA certificates.

5.8 CA OR RA TERMINATION

In the event operation of an FPKI Trust Infrastructure CA terminates, certificates signed by that FPKI Trust Infrastructure CA will be revoked, following the standard procedures for revoking CA certificates (see Section 4.9.3). The FPKIPA is notified via methods included in Section 2.2.2 or following the emergency revocation procedures in Section 5.7. The FPKIMA will advise all Entity CAs to which an FPKI Trust Infrastructure CA has issued certificates of its termination. All documentation and data will be archived using the archival procedures in Section 5.5.3. The FPKI Trust Infrastructure CA to be terminated will either continue issuing CRLs until the latest expiration date of any issued CA certificates, or will issue a long-term CRL valid until the expiration date of the root certificate. Once the last CRL has been issued, the private signing key(s) of the CA to be terminated will be destroyed. Retaining keys of terminated

---

[4] CA certificates include both subordinate cross-certificates and peer-to-peer cross-certificates.

CAs is not supported by the FPKIMA. If the FPKIMA ceases operations, any remaining FPKI Trust Infrastructure CA signing keys will be turned over to the FPKIPA.

The FPKIMA will coordinate scheduled termination with Entity CAs when authorized by the FPKIPA.

Entities will be given as much advance notice as circumstances permit, and attempts to provide alternative sources of interoperation will be sought in the event an FPKI Trust Infrastructure CA is terminated.

Entity CAs are registered on the FPKI Trust Infrastructure CA system which contains both the RA and CA components. Therefore, the RA cannot be terminated independently of an FPKI Trust Infrastructure CA termination.

6 TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

The FPKI Trust Infrastructure CAs do not issue Subscriber, CSS or PIV or PIV-I content Signing certificates and therefore do not generate key pairs for such certificates.

6.1.1.1 CA Key Pair Generation

The key pair for each FPKI Trust Infrastructure CA was generated on a FIPS 140-2 Level 3 cryptographic module. The key pair generation is RSA for digital signature in compliance with PKCS-10 (FIPS 140-2, level 3). The private key is never exposed outside the module in unencrypted form. After the key pair generation process, the cryptographic module partition was backed up onto a secure token and restored to the cryptographic module at one of the mirrored operational sites. Backup copies of the cryptographic module private keys were also created and stored in secure containers at both sites.

Private keys of FPKI Trust Infrastructure CAs are generated using the FPKI Trust Infrastructure CAs Key Signing Ceremony procedures. These procedures document the role separation and provide an auditable trail. The Key Signing Ceremony procedures are completed with a witness present. Each step is verified and the document is signed off on at the end of the procedure.

6.1.2 Private Key Delivery to Subscriber

The Entity CA generates its own key pair, and therefore does not need private key delivery.

6.1.3 Public Key Delivery to Certificate Issuer

Public keys are electronically delivered to the certificate issuer via PKCS#10 messages to the FPKIMA by secure means (e.g., CD delivered by registered mail or courier, digitally-signed email, SFTP, or out-of-band). Identity checking and proof of possession of the private key is accomplished as described in Section 4.3.1.

6.1.4 CA Public Key Delivery to Relying Parties

The FPKIMA posts all CA certificates it issues to the FPKI Repository. The FPKIMA also posts all cross-certificates issued by Entity CAs to the FPKI Trust Infrastructure CAs. FPKI Trust Infrastructure CA and Entity CA public keys are transported in a secure, out-of-band mechanism using PKCS#10 messages via digitally-signed e-mail, SFTP, or CD delivered by registered mail or courier.

FPKI Trust Infrastructure CA root certificates are securely distributed to Entity CAs along with CA certificates issued to Entity CAs using PKCS#7 files via digitally-signed e-mail, SFTP, or CD delivered by registered mail or courier.

The FCPCA root certificate may also be distributed via commercial product trust stores when the FPKIMA has an agreement with the vendor.

6.1.5 Key Sizes

The FBCA certificates are issued by a CA that signs certificates and CRLs using either SHA-256 or SHA-384, its CA key is a 2048-bit RSA key. The current FCPCA key is a 4096-bit RSA key and it signs certificates and CRLs using SHA-384.

The FBCA will not issue a cross-certificate to any Entity CA that does not adhere to the [FBCA CP] requirements regarding key size on the certificates they issue. Determination of Entity CA adherence to [FBCA CP] is determined by the FPKIPA and documented in the MOA between the FPKIPA and the Entity.

The FCPCA will not issue a certificate to any Entity CA that does not adhere to [FCPCA CP] requirements regarding key size on the certificates they issue. Determination of Entity CA adherence to [FCPCA CP] is determined by the FPKIPA.

6.1.6 Public Key Parameters Generation and Quality Checking

There are no public key parameters for RSA, and the FPKI Trust Infrastructure CAs use RSA signatures.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

Four key usage bits may be set in CA certificates issued by FPKI Trust Infrastructure CAs. cRLSign, CertSign are always set. Digital Signature and Non-Repudiation may be set if specified in the LOA. The *dataEncipherment*, *encipherOnly*, and *decipherOnly* bits shall not be asserted in certificates issued by the FPKI Trust Infrastructure CAs.

The use of a specific key is determined by the key usage extension in the X.509 certificate. Section 7 contains further details on key usage.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards and Controls

FPKI Trust Infrastructure CA private keys are protected using a FIPS 140-2 Level 3 validated cryptographic module.

All cryptographic modules are operated such that the private asymmetric cryptographic keys are never output in plaintext.

Activation of the cryptographic module requires activation material under multi-party control. Physical access to the cryptographic module requires two-party control (see Section 5.1.2). The FPKI Trust Infrastructure does not issue PIV or PIV-I cards.

6.2.1.1 Custodial Subscriber Key Stores

FPKI Trust Infrastructure CAs do not issue Subscriber certificates and do not maintain any custodial subscriber key stores.

6.2.2 Private Key Multi-Person Control

FPKI Trust Infrastructure CA private keys are under two-person control, using a split authentication method. The Trusted Roles present whenever the CA IPS secure container is accessed sign the CA IPS Secure Container Log, which is checked by the Auditor during the monthly audits and retained as part of the logs available during the annual PKI Compliance audit.

6.2.3 **Private Key Escrow**

6.2.3.1 Escrow of Trust Infrastructure CA and Entity CA Private Signature Key
FPKI Trust Infrastructure CA signature keys are not escrowed.

6.2.3.2 Escrow of CA Encryption Keys
FPKI Trust Infrastructure CA encryption keys are not escrowed.

6.2.4 **Private Key Backup**

6.2.4.1 Backup of Trust Infrastructure CA and Entity CA Private Signature Key
FPKI Trust Infrastructure CA private keys are stored in the cryptographic module at both sites. In addition, the private key is backed up on cryptographic module backup devices. A backup device is stored in a secure container at both sites. The backups of the private keys are made following procedures described in the HSM operations manuals and the FPKIMA SOP.

The FPKIMA is never in possession of Entity CA private signature keys.

6.2.4.2 Backup of Subscriber Private Signature Key
The FPKIMA does not issue any Subscriber certificates.

6.2.4.3 Backup of Subscriber Key Management Private Keys
The FPKIMA does not issue any Subscriber key management certificates.

6.2.4.4 Backup of CSS Private Key
The FPKIMA does not support a CSS.

6.2.4.5 Backup of Common PIV and PIV-I Content Signing Key
The FPKIMA does not issue any Common PIV or PIV-I Content Signing certificates.

6.2.5 **Private Key Archival**
No private keys of FPKI Trust Infrastructure CAs are archived or escrowed (see Section 6.2.3).

6.2.6 **Private Key Transfer Into or From a Cryptographic Module**
FPKI Trust Infrastructure CAs private keys are generated by and remain in a cryptographic module. The cryptographic module product uses proprietary secure means for transferring keys from one cryptographic module to another to back up the CA keys.

6.2.7 **Private Key Storage on Cryptographic Module**
FPKI Trust Infrastructure CA private keys are only stored in the cryptographic module, FIPS-140 Level-3 evaluated cryptographic module and on cryptographic module backup devices.

6.2.8 **Method of Activating Private Key**
The FIPS-140 Level-3 validated cryptographic module requires multi-party control through several split digital credentials and a combination of PINs and passphrases in order to activate cryptographic module partitions. PINs and passphrases require a minimum of six characters. Entry of PINs and passphrases is not displayed while being entered.

6.2.9 Methods of Deactivating Private Key

The cryptographic module is powered on and the partition is activated only as needed then deactivated when activity is completed. The cryptographic module and keying material are protected from unauthorized use by physical access mechanisms.

The cryptographic module is protected from unauthorized logical access by being offline or only accessible from the CA.

6.2.10 Method of Destroying Subscriber Private Signature Key

When a Trusted Role leaves, the CA authentication that uniquely identifies that individual Trusted Role is revoked.

When a CA private signature key is no longer needed, the key will be deleted from the cryptographic module partition and from all backup devices containing a partition backup that contains the key. If the FPKI Trust Infrastructure CA is being decommissioned, the corresponding partition on the cryptographic module and backup device will be deleted.

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 OTHER ASPECTS OF KEY MANAGEMENT

6.3.1 Public Key Archival

All certificates issued by FPKI Trust Infrastructure CAs, and their associated public keys, are included in the archival of the CA database backups.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The FBCA uses the following certificate operational and key pair usage periods:

1. Online operated FBCA - The key pair and self-signed certificate are issued for 6 years. The private signing key is used to sign certificates for 3 years. Rekeying will be performed on or before 3 years.
2. Offline operated FBCA - The key pair and self-signed certificate are issued for 10 years. The private signing key is used for a maximum of seven years for certificate signing. Rekeying will be performed on or before 7 years.

FCPCA - The key pair and self-signed certificate are issued for 20 years. The private signing key is used to sign certificates for a maximum of 10 years. Rekeying will be performed on or before 10 years.

The private keys are used for signing CRLs for the lifetime of the certificate or until the CA has issued its last long term CRL before being decommissioned.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

Activation data for the cryptographic module partition is generated during partition creation. Activation data is used to enable use of the FPKI Trust Infrastructure CA private signing keys. This activation data is stored in split digital credentials and satisfies the multi-part policy required by the CP and enforced by the cryptographic module. Once the use of the CA private

signing keys is enabled, actual use of the private signing keys continues under multi-party control of the CA software.

Activation data is not transmitted during routine operations. If transmission of activation data is necessary for replication of newly-generated data to the other site, it's transmitted by the Trusted role it's assigned to using the associated security bag and a two-party control method (with another trusted role or ISSO).

FPKI Trust Infrastructure CAs are installed using a supported CA software product. Multi-party control of the CA is enforced through physical means. Logical authentication makes use of hardware tokens and certificates or split credentials to access the CA. Each piece of the split key is a file stored on a FIPS 140-2 Level 3 encrypted USB flash drive, which requires the Trusted Role to enter a password to access the flash drive and a password to unencrypt the file. New split keys are generated when an FPKI Trust Infrastructure CA establishes a new CA instance.

6.4.2 Activation Data Protection

Activation information for the CA is stored on FIPS 140-2 Level 3 Encrypted USB Flash Drives, which are stored in security containers when not in use. The activation data are stored in GSA-approved security containers under two-party control.

FPKI Trust Infrastructure CAs are configured to temporarily lock out access following three unsuccessful login attempts.

6.4.3 Other Aspects of Activation Data

No additional detail.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

The FPKI Trust Infrastructure CA server is dedicated to providing FPKI Trust Infrastructure CA services. Online CA servers publish all information to an internal FPKI Directory that connects through a firewall to the online FPKI Repository systems in order to post validation information. Offline CA servers require validation information to be manually moved to the repositories.

The FPKI Repository servers only run those services necessary to operate and maintain the FPKI Repository and to support online certificate validations by Entity CA Subscribers (e.g., LDAP, HTTP).

All FPKI Trust Infrastructure component systems are configured with appropriate security features turned on as recommended by the host operating system vendor, in accordance with any associated security validation rating.

The FPKI Trust Infrastructure CA servers have the following security features and functions:

- Requires authenticated logins;
- Provides Discretionary Access Control via permissions and policies defined in the CA software;
- Provides security audit capability via automatic logging of all FPKI Trust Infrastructure CA activity;

- Restricts access control to FPKI Trust Infrastructure CA services and PKI roles as described in Sections 5.1.2 and 5.2.2;
- Enforces separation of duties for PKI roles as described in Sections 5.1.2 and 5.2.2;
- Requires identification and authentication of PKI roles and associated identities as described in Sections 5.1.2 and 5.2.2;
- Specific Operating Systems prevent object reuse by initializing all objects, including files and memory, before they are allocated to a user or process.
- Requires use of cryptography for session communication and database security;
- Archives history and audit data from FPKI Trust Infrastructure CA through data collection and archive procedures described in Sections 5.4 and 5.5;
- Requires self-test security related FPKI Trust Infrastructure CA services. FPKI Trust Infrastructure CA security audit logs are signed objects and the software verifies those objects at startup and each time the logs are accessed. If the verification changes, the software provides a message through the user interface and logs the event;
- Uses FIPS 140-2 certified hardware to protect activation data required to access the FPKI Trust Infrastructure CA key for certificate issuance and revocation;
- Requires a recovery mechanism for keys and the FPKI Trust Infrastructure CAs through backup and protection procedures described in Section 5.5; and
- Enforces domain integrity boundaries for security critical processes through self-test procedures described in an earlier bullet.
- Hypervisors hosting CA servers maintain the following security functions
  - Authenticated logins are used to access the VM console
  - Discretionary access control is available but all users who have access to the hypervisor are Administrators
  - Hypervisor logs are sent to a log analysis server for automatic auditing as well as to the Auditor for periodic, additional analysis and archiving
  - Session communications to the hypervisor are cryptographically protected
  - The hypervisor enforces separation between virtual machines.

6.5.2 Computer Security Rating

The FPKI CA systems were Common Criteria evaluated for the Protection Profile for Certification Authorities. Patches may be applied in between Common Criteria versions in order to maintain required security posture.

6.6 LIFE-CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

The FPKI system development controls are as follows:

- FPKI Trust Infrastructure CA software has been developed under a vendor-controlled development process;
- Hardware procured to operate the FPKI Trust Infrastructure CAs has been purchased in a fashion whereby the provider does not know that it is intended for FPKI Trust Infrastructure CA operations. The FPKI Trust Infrastructure CA software has been installed under the direction and control of authorized FPKI operations personnel. Hardware and software updates will be purchased or developed in the same manner as the original equipment, and will be installed by trusted and trained personnel;

- All software and hardware installed in, or run on, the FPKI Trust Infrastructure CA server is purchased following a government procurement process. Hardware and non-CA software are purchased through standard procurement procedures provided by the FPKIMA. An accountable method of packaging and delivery is used to provide a continuous chain of accountability from the vendor to the facility (e.g., UPS, FedEx, USPS Express Mail). The FPKIMA established a relationship with the CA software vendor prior to acquisition that gives assurance that the software has not been tampered with. Installation is performed under multi-person control with only authorized FPKIMA personnel; and
- Proper care is taken to prevent malicious software from being loaded onto FPKI Trust Infrastructure equipment. From the time software is received, software remains under continuous control. All shrink-wrapped packaging is opened and installed inside the secure FPKI facility under multi-person control**.** Antivirus software is used to scan all applications and files for malicious code – initially, periodically, and any time a new file is introduced to the system. Vulnerability assessments are conducted periodically, and any time a system configuration change occurs (e.g., adding a new CA to the FPKI).
- For Offline systems, vulnerability testing and scanning is performed in a test environment, prior to being applied to the production systems.
- Continuous monitoring of all FPKI systems is performed through Intrusion Detection Systems, vulnerability testing and scanning, external penetrations tests, log analysis, and procedural monitoring as required in operating procedures.
- FPKI Trust Infrastructure CA software and hardware, including hypervisors, are dedicated to performing FPKI Trust Infrastructure CA functions only.

6.6.2 Security Management Controls

The initial configuration of the FPKI software (i.e., CA software, Repository software) as well as any modifications and upgrades is documented and controlled in accordance with the *Configuration Management (CM) Plan for the FPKI Trust Infrastructure*. System- and application-level logging is enabled and reviewed monthly for offline systems, to maintain ongoing integrity of the software and configuration. The source for the software is described in Section 6.6.1. Audit procedures are used to ensure software integrity. These procedures are performed on a monthly basis for offline systems.

The offline CA systems do an automatic integrity check by the operating system when powered on. The CA software also does an integrity check when started.

6.6.3 Life Cycle Security Ratings

The FPKI Trust Infrastructure operates under standard maintenance. US-CERT Technical Alerts (TA) and Security Bulletins (SB), upgrades, and patches to the software and hardware are applied as necessary under FPKI configuration management procedures.

6.7 NETWORK SECURITY CONTROLS

The FPKI Trust Infrastructure CAs are operated as offline CAs. They are only powered up when required to perform a CA operation such as certificate, issuance or revocation or CRL generation. Artifacts that need to be published are manually moved from the offline CA to the FPKI Online Repositories for publication via secure USB keys.

FPKI Trust Infrastructure contains a private management network. The CRLs, certificates, and cross-certificates will be published first to a Master Directory in the private management network before being pushed out to the public Repositories residing in a non-CA zone. The servers in the CA private network can only be accessed from within the CA private network.

The cryptographic module is protected in the CA IPS security container under multi-party control.

The FPKI Online Repositories are protected by a firewall that is configured to only allow access to necessary services on the FPKI Repository systems (LDAP and HTTP) and specific machines. All activity is logged.

The FPKIMA manages monitoring of the content of the FPKI Trust Infrastructure Repository. All unused network ports and services are turned off.

All operational sites are connected through a secure connection. This enables Trusted Roles to perform tasks at any operational site while not physically at the site. Using the secure connection to access the alternate site requires the same authentication to the destination server as would happen if the Trusted Role were physically located with the server.

6.8   TIME-STAMPING

System time is maintained using Network Time Protocol (NTP) and a local timeserver synchronized with a time server synchronized with NIST. Clock adjustments are auditable events (see Section 5.4.1).

System time will be accurate to within three minutes by being automatically synchronized using NTP. Offline systems will have time manually synchronized at systems start.

7 CERTIFICATE, CRL, AND OCSP PROFILES

The FPKIPA has defined the Certificate and CRL profiles used by the FPKI. For ease of reference, this CPS includes a selective description in the following Sections.

7.1 CERTIFICATE PROFILE

The FBCA issues cross-certificates in accordance with the FBCA certificate profile contained in the *Federal Bridge Certification Authority (FBCA) X.509 Certificate and CRL Extensions Profile* [FBCA-Prof].

Certificates issued by the FCPCA conform to the *Common Policy X.509 Certificate and Certificate Revocation List (CRL) Profiles* [SSP-Prof].

7.1.1 Version Number(s)

FPKI Trust Infrastructure CAs issue X.509 v3 certificates (populate version field with integer "2").

7.1.2 Certificate Extensions

Certificates issued by the FBCA shall comply with [FBCA-Prof] using standard certificate extensions that comply with [RFC 5280].

Certificates issued by the FCPCA shall comply with [SSP-Prof] using standard certificate extensions that comply with [RFC 5280].

The only private extensions included in cross-certificates issued by FPKI Trust Infrastructure CAs are obtained from the PKCS#10 received from the Entity CA. The FPKIMA will verify that no private extension in the cross-certificate is marked critical.

7.1.3 Algorithm Object Identifiers

In compliance with [FBCA-Prof], cross-certificates issued by the FBCA use the signature OIDs listed in Table 7.1 -1:

Table 7.1-1. FBCA Signature Algorithm OIDs

Algorithm	OID
sha256WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }
sha384WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12 }

In compliance with [FBCA-Prof], cross-certificates issued by the FBCA use the OIDs listed in Table 7.1-2 for identifying the algorithm for which the subject key was generated:

Table 7.1-2. FBCA Subject Key Algorithm OIDs

Algorithm	OID
id-dsa	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1}
RsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
Dhpublicnumber	{iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1}
id-ecPublicKey	{iso(1) member-body(2) us(840) ansi-X9-62(10045) id-publicKeyType(2) 1}

Private extensions are not used.

Certificates issued by the FCPCA will use the OIDs listed in Table 7.1-3 for signatures:

Table 7.1-3. FCPCA Signature Algorithm OIDs

Algorithm	OID
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12}

Certificates issued by the FCPCA will use the OID listed in Table 7.1-4 to identify the algorithm associated with the subject key:

Table 7.1-4. FCPCA Subject Key Algorithm OIDs

Algorithm	OID
RsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
id-ecPublicKey	{iso(1) member-body(2) us(840) ansi-X9-62(10045) id-publicKeyType(2) 1}

For EC, public key must be encoded in uncompressed form. ECParameters is one of the following curves: Curve P-256 (1.2.840.10045.3.1.7) Curve P-384 (1.3.132.0.34)

7.1.4 Name Forms

The subject and issuer fields of the cross-certificate are populated with an X.500 DN, with the attribute type as further constrained by [RFC 5280].

7.1.5 Name Constraints

FPKI Trust Infrastructure CAs assert name constraints in certificates issued to Entity CAs appropriate for the PKI being certified, as specified in the LOA issued by the FPKIPA.

7.1.6 Certificate Policy Object Identifier

All certificates issued by FPKI Trust Infrastructure CAs include a non-critical certificate policies extension.

A certificate issued by the FBCA will assert (as directed in the applicable LOA) in the certificate policies extension one or more of the OIDs listed in Table 7.1-5.

Table 7.1-5. FBCA Policy OIDs

FBCA Policy	OID
id-fpki-certpcy-rudimentaryAssurance	::= { 2.16.840.1.101.3.2.1.3.1 }
id-fpki-certpcy-basicAssurance	::= { 2.16.840.1.101.3.2.1.3.2 }
id-fpki-certpcy-mediumAssurance	::= { 2.16.840.1.101.3.2.1.3.3 }
id-fpki-certpcy-mediumHardware	::= { 2.16.840.1.101.3.2.1.3.12 }
id-fpki-certpcy-medium-CBP	::={ 2.16.840.1.101.3.2.1.3.14 }
id-fpki-certpcy-mediumHW-CBP	::={ 2.16.840.1.101.3.2.1.3.15 }
id-fpki-certpcy-mediumDevice	::= { 2.16.840.1.101.3.2.1.3.37}
id-fpki-certpcy-mediumDeviceHardware	::= { 2.16.840.1.101.3.2.1.3.38}
id-fpki-certpcy-highAssurance	::= { 2.16.840.1.101.3.2.1.3.4 }
id-fpki-certpcy-pivi-hardware	::={ 2.16.840.1.101.3.2.1.3.18 }

| id-fpki-certpcy-pivi-cardAuth | ::={ 2.16.840.1.101.3.2.1.3.19 } |
| id-fpki-certpcy-pivi-contentSigning | ::= { 2.16.840.1.101.3.2.1.3.20 } |

A certificate issued by the FCPCA will assert (as directed by the applicable LOA) in the non-critical certificate policies extension one or more of the OIDs listed in Table 7.1-6. OIDs listed in Table 7.1-5 may also be asserted, if specified in the LOA.

Table 7.1-6. FCPCA Policy OIDs

FCPCA	OID
id-fpki-common-policy	::= {2.16.840.1.101.3.2.1.3.6}
id-fpki-common-hardware	::= {2.16.840.1.101.3.2.1.3.7}
id-fpki-common-devices	::= {2.16.840.1.101.3.2.1.3.8}
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}
id-fpki-common-cardAuth	::= {2.16.840.1.101.3.2.1.3.17}
id-fpki-common-devicesHardware	::= {2.16.840.1.101.3.2.1.3.36}
id-fpki-common-piv-contentSigning	::= {2.16.840.1.101.3.2.1.3.39}
id-fpki-common-pivAuth-derived	::= {2.16.840.1.101.3.2.1.3.40}
id-fpki-common-pivAuth-derived-hardware	::= {2.16.840.1.101.3.2.1.3.41}

The FPKIMA will verify that the certificate policies extension asserts the OID(s) as specified in the LOA.

7.1.7 Usage of Policy Constraints Extension

Policy constraints appear in certificates as specified in the LOA.

7.1.8 Policy Qualifiers Syntax and Semantics

The certificates issued by FPKI Trust Infrastructure CAs do not contain policy qualifiers.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Certificates issued by FPKI Trust Infrastructure CAs always contain a non-critical certificate policy extension.

7.1.10 Inhibit Any Policy Extension

Certificates issued by FPKI Trust Infrastructure CAs assert the InhibitAnyPolicyextension with Skip Certs set to 0.

7.2   CRL PROFILE

FPKI Trust Infrastructure CAs issue CRLs in accordance with [FBCA-Prof] and [SSP-Prof], as applicable.

7.2.1 Version Number(s)

FPKI Trust Infrastructure CAs issue X.509 version two (2) CRLs.

7.2.2 **CRL and CRL Entry Extensions**

Online FPKI Trust Infrastructure CAs generate CRLs in conformance with [FBCA-Prof] or [SSP-Prof] at least every 12 hours with an 18-hour nextUpdate time. If operated offline, FPKI Trust Infrastructure CAs issue CRLs upon every revocation update and at least every 31 days even if there are no changes to be made.

7.3   OCSP PROFILE

The FPKIMA does not support the Online Certificate Status Protocol (OCSP) checking capability for its issued certificates.

8 COMPLIANCE AUDIT AND OTHER AUDIT ASSESSMENTS

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

The FPKIMA will arrange, initially and annually, for independent inspections and compliance audits to validate that the FPKI Trust Infrastructure CAs are operating in accordance with the security practices and procedures described in this CPS. Results of the compliance audit will be provided to the FPKIPA in the form of an Auditor Letter of Compliance that follows the FPKIPA Annual Review Requirements [FPKI AUDIT].

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

The FPKI compliance audits will be provided by an independent Auditor as agreed between the FPKIPA and FPKIMA. The Auditor selected will be a Certified Information System Auditor (CISA), IT security specialist, and a PKI subject matter specialist who can offer input regarding acceptable risks, mitigation strategies, and industry best practices. The Auditor must perform such compliance audits as a regular ongoing business activity. The Auditor selected will have a demonstrated proven track record in one or more of the following areas:

- Specialization in Electronic Data Processing (EDP) security audit;
- Knowledge and experience with Compliance Audits and PKI;
- Independence from the organization being audited; or
- Understanding of the Federal assessment and authorization process required by OMB A-130 and the Federal Information Security Management Act (FISMA) of 2002 (Public Law 107-347).

The selected Auditor will verify and validate, through document reviews and demonstrations, that the FPKIMA complies with [FBCA CP] and [FCPCA CP].

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The selected FPKI Compliance Auditor is a contractor that is independent from the FPKIMA, FPKIPA, and ICAMSC. This contractor provides an unbiased, independent evaluation and is one whose primary responsibility is the performance of EDP Compliance Audits.

To ensure independence and objectivity, the FPKI Compliance Auditor may not have served the FPKIMA in developing or maintaining the FPKI's facility or CPS.

8.4 TOPICS COVERED BY ASSESSMENT

The compliance audit will address all aspects of FPKI Trust Infrastructure operation in accordance with the [FPKI AUDIT]. The compliance audit will verify that FPKI Trust Infrastructure CAs are operated in compliance with all the requirements of the current versions of the applicable CPs and this CPS. The audit shall also verify that the FPKIMA is implementing the relevant provisions of the MOAs between the FPKI Policy Authority and each Entity PKI.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

Based on the findings of the FPKI Compliance Auditor, an audit action plan will document what steps must be taken. Possible steps include:

- Correction of deficiencies prior to implementing full operation of the FPKI Trust Infrastructure or within another time period as determined by the FPKIPA and FPKIMA;
- Suspension of full operation of one or more of the FPKI Trust Infrastructure CAs (this alternative will execute the emergency procedure described in Section 4.9.1 for revocation of certificates);
- The FPKIMA shall determine what further notifications or actions are necessary to meet the requirements of [FBCA CP], [FCPCA CP], and the MOAs, and then proceed to make such notifications and take such actions without delay;
- Execute other corrective actions through procedures developed and published by the FPKIPA; and
- Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the FPKIPA may direct the FPKIMA to take additional actions as appropriate, including temporarily halting operation of one or more of the FPKI Trust Infrastructure CAs.

If the FPKIPA receives a report of audit deficiency from an Entity, the FPKIPA may direct the FPKIMA to take additional actions to protect the FPKI Trust Infrastructure's level of trust by revoking cross-certificates issued to that Entity (this alternative will execute the revocation procedure described in Section 4.9.1), or take other actions it deems appropriate.

8.6   COMMUNICATION OF RESULTS

The Compliance Auditor will submit a compliance audit written report (via signed e-mail and/or in writing) to the FPKIMA 24 hours after audit conclusion. The report will contain a summary table of topics covered, areas in which one or more of the FPKI Trust Infrastructure CAs were found to be non-compliant, a brief description of the problem(s) for each area of non-compliance, and possible remedies for each area. A more comprehensive report may be provided later.

Within 30 days of receipt of the written audit report, the FPKIMA will provide the audit results and corrective actions to the FPKIPA.

9   OTHER BUSINESS AND LEGAL MATTERS

9.1   FEES
The FPKIPA reserves the right to charge a fee to each Entity in order to support operations of the FPKI Trust Infrastructure.

9.1.1   Certificate Issuance or Renewal Fees
At this time, the FPKIMA does not charge a fee for certificate issuance or renewal.

9.1.2   Certificate Access Fees
The FPKIMA does not charge a fee for certificate access.

9.1.3   Revocation or Status Information Access Fees
Tthe FPKIMA does not charge a fee for access to certificate revocation or status information.

9.1.4   Fees for Other Services
At this time, the FPKIMA does not charge a fee for any other services.

9.1.5   Refund Policy
At this time, since there are no fees associated with FPKIMA services, there is no refund policy in place.

9.2   FINANCIAL RESPONSIBILITY
This CPS contains no limits on the use of any certificates issued by the FPKI Trust Infrastructure CAs or by Entity CAs. Rather, entities acting as Relying Parties shall determine what financial limits, if any, they wish to impose for certificates used to complete a transaction.

9.2.1   Insurance Coverage
The FPKIMA does not provide any insurance or warranty coverage for the use of any certificates issued either by the FPKI Trust Infrastructure CAs or any cross-certified Entity CA.

9.3   CONFIDENTIALITY OF BUSINESS INFORMATION
FPKI Trust Infrastructure information not requiring protection is publicly available in either the FPKI Repositories, the FPKIPA web site, or the FPKIMA web site. FPKIPA access to Entity information is addressed in the MOA with that Entity. Public access to Entity information is determined by the respective Entity.

9.3.1   Scope of Confidential Information
The FPKIMA does not maintain any confidential information about Entity CAs.

9.3.2   Information Not Within the Scope of Confidential Information
[FBCA CP] does not stipulate requirements for this Section.

9.3.3 Responsibility to Protect Confidential Information

Any information about Entity CAs that is not publicly available will be treated as confidential by FPKIMA personnel.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

The initial FPKIMA Privacy Impact Assessment determined there was no requirement for a Privacy Plan as no personal data/information is collected on the general public or government employees.

9.4.2 Information Treated as Private

All archive records will be treated as Controlled Unclassified Information (CUI) and will only be released as requested by the FPKIPA or as required by law. This includes any identity authentication and registration information collected from the Entity CAs.

The certificate issuance paper files are stored in the server room, leveraging the physical security requirements detailed in Section 5.1, until they are processed for audit review and archival by the Auditor. A copy of each certificate issuance paper file remains in binders secured inside the server room after the originals are processed for audit review and archival.

Information stored on FPKI Trust Infrastructure systems, including the FPKI Trust Infrastructure workstations, leverage the physical security requirements of the server room as detailed in Section 5.1. Access to the FPKI Trust Infrastructure systems is protected by password, limited to those in Trusted Roles, and security and access control settings are applied through group policies.

Collection of PII shall be limited to the minimum necessary to perform the certificate activity. PII collected for identity proofing purposes shall not be used for any other purpose.

9.4.3 Information Not Deemed Private

FPKI Trust Infrastructure certificates are public certificates. Information about entities cross-certified with the FPKI Trust Infrastructure is maintained on the FPKIPA web site. Therefore, information included in FPKI Trust Infrastructure certificates and about what PKIs are cross-certified is not subject to protections outlined in Section 9.4.1.

9.4.4 Responsibility to Protect Private Information

There is no privacy information collected. Any sensitive information, such as that identified in section 9.4.2, is stored securely and released only in accordance with the provisions of Section 9.4.

9.4.5 Notice and Consent to Use Private Information

The FPKIMA does not issue certificates to subscribers or Entity personnel, and is not required to provide any notice or obtain the consent of the Subscriber or Entity personnel in order to release private information in accordance with the stipulations of Section 9.4.6.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

The FPKIMA will disclose confidential information to any third party when required by this CPS, [FBCA CP], [FCPCA CP], law, government rule or regulation, or order of a court of

competent jurisdiction. Any request for release of information will be authenticated. The authentication will consist of validating the identity of the requester using two forms of photo identifications. The individual's authority to obtain the information will be validated using at least one of the following means:

- The individual has the duly-executed court order from a Federal court;
- The individual has duly-executed request from the respective Agency Office of Inspector General;
- The individual is the Subscriber itself; or
- The individual has a duly-signed request from the Subscriber requesting the release of the information from the Subscriber.

In compliance with 41 CFR 105-60.605, the FPKIMA Program Manager will be notified of any validated requests for disclosure of confidential information. The FPKIMA Program Manager will notify the Appropriate Authority.

9.4.7 Other Information Disclosure Circumstances

There are no other disclosure circumstances.

9.5 INTELLECTUAL PROPERTY RIGHTS

While executing the certificate management and operational practices of this CPS, the FPKIMA will not knowingly violate intellectual property rights held by others.

The U.S. Government retains exclusive rights to any products or information developed under or pursuant to this FPKI CPS.

9.6 REPRESENTATIONS AND WARRANTIES

The obligations described below pertain to the FPKI Trust Infrastructure CAs (and, by implication, the FPKIMA, and Entity CAs that either interoperate with the FPKI Trust Infrastructure CAs or are in a trust chain up to an Entity CA that interoperates with the FPKI Trust Infrastructure). The obligations applying to Entity CAs pertain to their activities as issuers of certificates. Further, the obligations focus on Entity CA obligations affecting interoperability with the FPKI Trust Infrastructure. Thus, where the obligations include, for example, a review (or audit) by the FPKIPA or some other body of an Entity's CA operation, the purpose of that review pertains to interoperability using the FPKI Trust Infrastructure CAs, and whether the Entity is complying with the MOA.

9.6.1 CA Representations and Warranties

FPKI Trust Infrastructure CA issued certificates are issued and revoked at the sole discretion of the FPKIPA. The FPKIMA warrants that FBCA and FCPCA operational procedures comply with this CPS, as well as [FBCA CP] and [FCPCA CP] respectively.

9.6.2 RA Representation and Warranties

The FPKIMA makes no representation or warranty that the information in a cross-certificate is accurate, other than it matches the information specified in the LOA authorizing the issuance of that certificate.

9.6.3 Subscriber Representations and Warranties

The FPKI Trust Infrastructure CAs do not issue subscriber certificates.

9.6.4 Relying Parties Representations and Warranties

The FPKIMA makes no representation or warranty about the use of certificates issued by Entity PKIs for Relying Parties.

9.6.5 Representations and Warranties of Other Participants

The FPKIMA makes no representation or warranty for other participants.

9.7 DISCLAIMERS OF WARRANTIES

The FPKIMA does not disclaim any responsibilities described in [FBCA CP] and [FCPCA CP].

9.8 LIMITATIONS OF LIABILITY

Certificates are issued and revoked at the sole discretion of the FPKIPA. When the FBCA issues a cross-certificate to a non-Federal Entity, it does so for the convenience of the Federal Government. Any review by the FPKIPA of a non-Federal Entity's certificate policy is for the use of the FPKIPA in determining whether or not interoperability is possible, and if possible, to what extent the non-federal Entity's certificate policy maps to [FBCA CP]. A non-Federal Entity must determine whether that Entity's certificate policy meets its legal and policy requirements. Review of a non-Federal Entity's certificate policy by the FPKIPA is not a substitute for due care and mapping of certificate policies by the non-Federal Entity.

Entities acting as Relying Parties are responsible for determining what financial limits, if any, they wish to impose for certificates used to consummate a transaction. This is entirely at the discretion of the Entity as Relying Party and is likely to depend upon several factors in addition to the certificate assurance level (e.g., likelihood of fraud, other procedural controls, Entity-specific policy or statutorily imposed constraints).

As an example, one Entity may be willing to accept a FBCA Basic assurance level certificate for transactions of a specific financial value for which another Entity would require a FBCA High assurance level certificate.

Neither the FPKIPA nor the FPKIMA is financially responsible for any losses incurred from using its services.

9.9 INDEMNITIES

This FPKI CPS does not include any claims of indemnity.

9.10 TERM AND TERMINATION

9.10.1 Term

This CPS becomes effective when approved by the FPKIPA. This CPS has no specified term.

9.10.2 Termination

Termination of this CPS is at the discretion of the FPKIPA.

9.10.3 Effect of Termination and Survival

The requirements of [FBCA CP] and [FCPCA CP] remain in effect through the end of the archive period for the last certificate issued.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

The FPKIMA uses the POC information provided by the FPKIPA in LOAs and MOAs, and as updated by Entity-authorized officials, when communicating with Entities. The FPKIPA listservs may also be used for communications to Entities. Any planned certificate issuance or revocation is authorized by the FPKIPA who is notified of the potential and result of the change via methods included in Section 2.2.2. In addition, the FPKI community is notified via the same mechanism of all new FPKI Trust Infrastructure certificate issuance activity.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

The FPKIMA shall review the FPKI CPS at least once every year, or when a change is made to [FBCA CP] or [FCPCA CP]. If the FPKIMA determines modifications to this CPS are required, the change, a change justification, and contact information for the person requesting the change will be presented to the FPKIPA for review and acceptance.

9.12.2 Notification Mechanism and Period

[FBCA CP] and [FCPCA CP], and any subsequent changes shall be made publicly available.

9.12.3 Circumstances under which OID must be Changed

If the FPKIPA determines that there is a requirement to change the OIDs defined in [FBCA CP], the FPKIPA will vote to amend [FBCA CP].

If the FPKIPA determines that there is a requirement to change the OIDs defined in [FCPCA CP], the FPKIPA will vote to amend [FCPCA CP].

9.13 DISPUTE RESOLUTION PROVISIONS

The FPKIPA will resolve any disputes associated with the use of the FPKI Trust Infrastructure or certificates issued by the FPKI Trust Infrastructure CAs.

9.14 GOVERNING LAW

The construction, validity, performance and effect of certificates issued under this FPKI CPS for all purposes are governed by United States Federal law (statute, case law or regulation).

Where an inter-governmental dispute occurs, resolution will be according to the terms of the MOA.

9.15 COMPLIANCE WITH APPLICABLE LAW

The FPKIMA will comply with applicable law.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire Agreement

There are no additional miscellaneous provisions on this CPS.

9.16.2 Assignment

This FPKI CPS does not assign rights or responsibilities other than what is specified in this CPS, [FBCA CP], [FCPCA CP], and MOAs with cross-certified Entities.

9.16.3 Severability

Should it be determined that one Section of this CPS is incorrect or invalid, the other Sections of this CPS shall remain in effect until the CPS is updated. The process for updating this CPS is described in Section 9.12.1.

9.16.4 Enforcement (Attorney's Fees or Waiver of Rights)

Failure by any person to enforce a provision of this CPS will not be deemed a waiver of future enforcement of that or any other provision.

9.17 OTHER PROVISIONS

This CPS does not stipulate any additional provisions.

APPENDIX A: REFERENCES

The documents and websites below were used in part to develop this CPS. The external FPKI documents can be found by going to https://www.idmanagement.gov/governance/fpkiaudit/ and using the search feature to find the specific document.

ABADSG	Digital Signature Guidelines, 1996-08-01.
BCCP	FPKI Business Continuity and Contingency Plan, October 2015
Bridge Process	Federal Public Key Infrastructure Bridge Application Process Overview https://www.idmanagement.gov/docs/fpki-bridge-app-process.pdf
CITE	Community Interoperability Test Environment (CITE) https://playbooks.idmanagement.gov/fpki/tools/citeguide/
FBCA CP	X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA) https://www.idmanagement.gov/governance/fpkiaudit/#fpki-policies-and-profiles
FCPCA CP	X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework https://www.idmanagement.gov/governance/fpkiaudit/#fpki-policies-and-profiles
FIPS 140-2	Security Requirements for Cryptographic Modules December 3, 2002. http://csrc.nist.gov/publications/
FIPS 186-3	Digital Signature Standard, July 2014. http://csrc.nist.gov/publications/
FISMA	Federal Information Security Modernization Act of 2014 (44 U.S.C. § 3541) https://www.gpo.gov/fdsys/search/pagedetails.action?collectionCode=PLAW&browsePath=113%2FPUBLIC%2F[200+-+299]&granuleId=&packageId=PLAW-113publ283
FOIACT	5 U.S.C. 552, Freedom of Information Act. http://www.justice.gov/oip/foia_updates/Vol_XVII_4/page2.htm
FPKI Audit	FPKI Annual Review Requirements, May 6, 2022, Version 1.2 https://www.idmanagement.gov/docs/fpki-annual-review-requirements.pdf
FPKI CPS	X.509 Certificate Practice Statement for the Federal PKI Trust Infrastructure https://www.idmanagement.gov/docs/fpki-fpkima-cps.pdf
FPKI HTTP Site Map	FPKI HTTP Site Map https://www.idmanagement.gov/docs/fpki-fpkima-sitemap.pdf
FPKI Guides	https://playbooks.idmanagement.gov/fpki/
FPKI Participating CAs and SSPs	https://www.idmanagement.gov/buy/trust-services/
FPKI-Prof	Federal Bridge Certification Authority (FBCA) X.509 Certificate and CRL Extensions Profiles https://www.idmanagement.gov/governance/fpkiaudit/

FPKI Security Profile	FPKI Security Controls Profile of NIST Special Publication 800-53, Security Controls for PKI Systems https://www.idmanagement.gov/docs/fpki-overlay-sp-800-53.pdf
FPKI IMP	FPKI Incident Management Plan https://www.idmanagement.gov/docs/fpki-imp.pdf
FPKIMA Website	Federal PKI Management Authority Website https://www.idmanagement.gov/governance/ficam/#federal-public-key-infrastructure-management-authority
FPKIPA Website	Federal PKI Policy Authority Website https://www.idmanagement.gov/governance/ficam/#federal-public-key-infrastructure-policy-authority
ISO9594-8	Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate Framework, 2008 https://www.iso.org/standard/53372.html
NAG69C	Information System Security Policy and Certification Practice Statement for Certification Authorities, rev C, November 1999.
NIST SP 800-53 Rev 4	Recommended Security Controls for Federal Information Systems and Organizations http://csrc.nist.gov/publications/
NSD42	National Policy for the Security of National Security Telecom and Information Systems, 5 Jul 1990. http://www.fas.org/irp/offdocs/nsd/nsd_42.htm
PIV-I-Prof	Combined into: Federal Bridge Certification Authority (FBCA) X.509 Certificate and CRL Extensions Profiles https://www.idmanagement.gov/governance/fpkiaudit/
PKCS#7	Cryptographic Message Syntax Standard https://tools.ietf.org/html/rfc2315
PKCS#10	Certification Request Syntax Standard https://tools.ietf.org/html/rfc2986
RFC 3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, November 2003 http://www.ietf.org/rfc/rfc3647.txt
RFC 4122	A Universally Unique IDentifier (UUID) URN Namespace http://www.ietf.org/rfc/rfc4122.txt
RFC 4210	Internet X.509 Public Key Infrastructure Certificate Management Protocol, Adams, Farrell, Kause, and Mononen, September 2005 http://www.ietf.org/rfc/rfc4210.txt
RFC 5280	Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile, Housley et al., April 2008. http://www.ietf.org/rfc/rfc5280.txt
SCEPACS	Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems https://www.idmanagement.gov/docs/pacs-tig-scepacs.pdf
SSP-Prof	Common Policy X.509 Certificate and Certificate Revocation List (CRL) Profiles https://www.idmanagement.gov/governance/fpkiaudit/