ISO/IEC JTC 1/WG 7
Working Group on Sensor Networks

Document Number:	N052
Date:	2010-07-05
Replace:	
Document Type:	Liaison Organization Contribution
Document Title:	Liaison Statement from JTC 1/SC 27/WG 5 to JTC 1/WG 7 on the ISO/IEC 1st CD 29115
Document Source:	JTC 1/SC 27/WG 5
Document Status:	For consideration at the 2nd WG 7 meeting in US.
Action ID:	FYI
Due Date:	
No. of Pages:	41

ISO/IEC JTC 1/WG 7 Convenor:

Dr. Yongjin Kim, Modacom Co., Ltd (Email: cap@modacom.co.kr)

ISO/IEC JTC 1/WG 7 Secretariat:

Ms. Jooran Lee, Korean Standards Association (Email: jooran@kisi.or.kr)

Committee Draft **ISO/IEC 1st CD 29115**	Reference number: ISO/IEC JTC 1/SC 27 **N8810**
Date: **2010-06-10**	Supersedes document SC 27 N8166

THIS DOCUMENT IS STILL UNDER STUDY AND SUBJECT TO CHANGE. IT SHOULD NOT BE USED FOR REFERENCE PURPOSES.

ISO/IEC JTC 1/SC27 Information technology - Security techniques Secretariat: Germany (DIN)	Circulated to P- and O-members, and to technical committees and organizations in liaison for voting (P-members only) by: **2010-09-10** Please submit your votes and comments via the online balloting application by the due date indicated.

ISO/IEC 1st CD 29115

Title: Information technology -- Security techniques – Entity authentication framework

Project: 1.27.57 (29115 I X.eaa)

Explanatory Report

Status	**SC 27 Decision**	**Reference documents**	
		Input	**Output**
NWIP (N5534)	Resolution 8 of 1st WG 5 meeting (N5513), Nov. 2006 & Recommendation 1 of SC 27 Head of Delegation meeting (N5561rev1)	US contr. (N5334)	NWIP (N5534)
1st WD 29115	2nd WG 5 meeting, May 2007, Resolution 7 (N5873) & Resolution 2 of 19th SC 27 Plenary (N5939), May 2007.	SoV (N5637)	Text f. 1st WD (N5875)

2nd WD 29115	3rd WG 5 meeting, Oct. 2007, resolutions 1, 3, 9, 10 (N6251)	SoCom. (N6053);
		AU com. (N6106);
		USA com. (N6059).
			DoC (N6271);
			Liaison to ITU-T SG 17;
			Text f. 2nd WD N6272rev2);
			Change of title (N6440);
			Liaison to ITU-T SG17 on collab. project (N6270); JTC 1 endors. (N6467).

3rd WD 29115	5th WG 5 meeting, April 2008, resolutions 1, 4, 8, (N6726) & 20th SC 27 Plenary, April 2008, resolution 2 (N6799).	SoCom. (N6524);
		AU com. (N6606);
		Liaison ITU-T SG 17 (N6633).
			Change of scope (N6270); 1st DoC (N6727); 2nd DoC (N6767); Text f. 3rd WD (N6728); Liaison to ITU-T SG17 (N6744).

4th WD 29115	6th WG 5 meeting, October 2008, resolutions 1, 8 (N7079).	SoCom (N7008); FIDIS (N7060).	Liaison to FIDIS (N7xxx); DoC (N7115); Text f. 4th WD (N7235).
5th WD 29115	7th WG 5 meeting, May 2009, resolutions 1, 5, P2, P10, P13 (N7724).	SoCom (N7548rev1); FIDIS (N7541).	DoC (N7754); Text f. 5th WD (N7755); Liaison to ITU-T SG17 (N7727); Call f. contr. (N7778); Call f. Editor (N7715).

6th WD 29115	8th WG 5 meeting, Nov. 2009, resolutions 1, 3, 6, 7, 11, 18, 21, P1 (N8138).	ITU-T SG17 liaisons (N7874rev1, N8075);
		SC 37 com (N8045);
		SoCom (N8051);
		US contr (N8053rev1);
		AU contr (N8110).
			Prop. f. Collab. Team (N8156);
			Liaison to ITU-T SG17 (N8146);
			Liaison to SC 37 (N8141);
			DoC (N8165); LB on Title+Scope change (N8278);
			Text f. 6th WD (N8166).

1st CD 29115	9th WG 5 meeting, April 2010, resolutions 3, P3 (N8828rev) & SC 27 resolution 1 (N8916).	TAS[3] (N8563); CA Com. (N8691); Endorsement limit dates extension (N8609); SoV on N8278 (N8403); SoCom (N8590).	Liaisons to ITU-T (N8846), TAS[3] (N8841); DoC (N8809); Text f. 1st CD (N8810).

1st CD Registration and Consideration

In accordance with resolution P3 (in SC 27 N8828rev) of the 9th SC 27/WG 5 meeting held in Melaka (Malaysia), 19th – 23rd April 2010, the attached document SC 27 N8810 has been registered with the ISO Central Secretariat (ITTF) as a 1st Committee Draft (CD) and is hereby circulated for a 3-month 1st CD LB closing by **2010-09-10.**

ITU
International
Telecommunication Union

ISO
International Organization
for Standardization

IEC
International
Electrotechnical
Commission

ITU-T Recommendation X.eaa | International Standard ISO/IEC 1st CD 29115 *

Information technology — Security techniques — Entity authentication assurance framework

** subject to JTC 1 endorsement on the project title change*

CONTENTS

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 29115 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*. The identical text is published as ITU-T Recommendation X.eaa.

Introduction

Many electronic transactions with or between ICT systems have security requirements which depend upon an understood or specified level of confidence in the identities of the entities involved. Such requirements may include the protection of assets and resources against unauthorized access, for which an access control mechanism might be used, and/or the enforcement of accountability by the maintenance of audit logs of relevant events, as well as for accounting and charging purposes.

The process of corroborating an identity or attribute with a specified or understood level of assurance is called authentication. This Recommendation | International Standard provides a framework for entity authentication assurance. Assurance within this Recommendation | International Standard refers to the confidence placed in all of the processes, management activities, and technologies used to establish and manage the identity of an entity for use in authentication transactions.

Using four specified Levels of Authentication (LoAs), this Recommendation | International Standard provides guidance concerning control technologies, processes, and management activities, as well as assurance criteria, that should be used to mitigate authentication threats in order to implement the four LoAs. It also provides guidance for the mapping of other authentication assurance schemes to the specified four levels, as well as guidance for exchanging the results of authentication. Finally, this Recommendation | International Standard provides informative guidance concerning the protection of personally identifiable information (PII) associated with the authentication process.

<Editor’s note: Editor will provide a proposal for splitting the standard into three parts, including a scope and title for each part. Editor will add the following text to the introduction. The editor requests contributions for the proposed part 3.>

[This Recommendation | International Standard is comprised of three parts. The first part covers authentication assurance generally. The second part covers authentication assurance for human entities. The third part covers authentication assurance for non-human entities.]

INTERNATIONAL STANDARD <29115>
ITU-T RECOMMENDATION <X.eaa>

Information technology — Security techniques — Entity authentication assurance framework[*]

1 Scope[**]

This Recommendation | International Standard provides a framework for managing entity authentication assurance in a given context. In particular, it:

- specifies four levels of entity authentication assurance;
- specifies criteria and guidelines for each of the four levels of entity authentication assurance;
- provides guidance concerning controls that should be used to mitigate authentication threats;
- provides guidance for mapping the four levels of assurance to other authentication assurance schemes;
- provides guidance for exchanging the results of authentication that are based on the four levels of assurance.

<Editor's note: There is no content for the last bullet. Please send contributions, or consider possible scope revisions when split into multi-part standard.>

2 Normative references

The following Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent edition of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations.

2.1 Identical Recommendations | International Standards

None.

2.2 Paired Recommendations | International Standards

None.

2.3 Additional references

- ITU-T Recommendation Y.2702 (2010), *Next generation network authentication and authorization requirements.*
- ITU-T Recommendation Y.2720 (2010), *Next generation network identity management framework.*
- ISO/IEC 9798:2010, *Information technology – Security techniques – Entity authentication.*
- ISO/IEC 19790:2006, *Information technology – Security techniques – Security requirements for cryptographic modules.*
- ISO/IEC 19792:2009, *Information technology – Security techniques – Security evaluation of biometrics.*

[*] Pending approval of title change by JTC1.

[**] Pending approval of scope change by JTC1.

- ISO/IEC 24760:2010, *Information technology – Security techniques – A framework for identity management.*
- ISO/IEC 29100:2010, *Information technology – Security techniques – Privacy framework.*
- ISO/IEC 29101:2010, *Information technology – Security techniques – Privacy reference architecture.*
- ISO/IEC 29146:2010, *Information technology – Security techniques – A framework for access management.*

3 Definitions

For the purposes of this Recommendation | International Standard, the following definitions apply:

3.1 **Authentication:** Process of corroborating an identity or attribute with a specified or understood level of assurance.

3.2 **Authentication Protocol:** Defined sequence of messages between a claimant and a verifier that enables the verifier to corroborate the claimant's identity.

3.3 **Claimant:** Entity which is or represents a principal for the purposes of authentication.

NOTE: A claimant includes the functions necessary for engaging in authentication exchanges on behalf of a principal.

3.4 **Credential:** Representation of information elements which can be used to corroborate an identity.

NOTE - This definition refers to both electronic and paper credentials.

3.5 **Credential Service Provider:** A trusted entity that issues and manages credentials. The Credential Service Provider (CSP) may encompass Registration Authorities (RAs) and verifiers that it operates. A CSP may be an independent third party, or it may issue credentials for its own use.

3.6 **Distinguishing Identifier:** Information which unambiguously distinguishes an entity in the context of an authentication exchange.

3.7 **Entity Authentication Assurance:** Confidence that the entity asserting a particular identity is in fact the entity to which the identity has been assigned.

3.8 **Hardware Cryptographic Credential:** A credential that is comprised of a hardware device that contains a protected cryptographic key.

NOTE - It is also referred to as a hard credential or hard cryptographic credential.

3.9 **Man-in-the-middle Attack:** Attack in which an attacker is able to read, insert, and modify messages between two parties without their knowledge.

3.10 **Masquerade:** Pretence by an entity to be a different entity.

3.11 **Mutual Authentication:** Entity authentication which provides both entities with assurance of each other's identity.

3.12 **Non-repudiation:** Security objective aimed at preventing the denial of previous commitments or actions.

3.13 **Pharming:** Attack aimed at redirecting a website's traffic to another, bogus website.

3.14 **Physical Credential:** A credential comprised of a tangible object (e.g, a smart card).

3.15 **Principal:** An entity whose identity can be authenticated.

3.16 **Registration Authority:** A trusted entity that establishes and vouches for the identity of a claimant to a CSP. The RA may be an integral part of a CSP, or it may be independent of a CSP, but it has a relationship with the CSP.

3.17 **Relying Party:** Entity that relies on an identity representation or claim by a claimant within some request context in order to authenticate or grant access to other entities based on identity information from a CSP.

3.18 **Replay Attack:** Masquerade which involves use of previously transmitted messages.

3.19 **Repudiation:** Denial of previous commitments or actions.

3.20 **Salt:** A non-secret, often random, value that is used in a hashing process, usually to ensure that the results of computations for one instance cannot be reused by an attacker.

NOTE - It is also referred to as sand.

3.21 **Secret Credential:** Credential based on the “something you know” factor (e.g., password).

3.22 **Shared Secret:** A secret used in authentication that is known to the claimant and the verifier.

3.23 **Software Cryptographic Credential:** A credential that is comprised of software that contains a protected cryptographic key.

NOTE - It is also referred to as a soft credential, soft cryptographic credential, or soft credential.

3.24 **Time Stamp:** Time variant parameter which denotes a point in time with respect to a common reference.

3.25 **Transaction:** Discrete event between an entity and service provider that supports a business or programmatic purpose.

3.26 **Trust Framework:** A set of technical, operational, and legal requirements, and enforcement mechanisms for parties exchanging identity information.

3.27 **Trusted Third Party:** Security authority or its agent, trusted by other entities with respect to security related activities.

NOTE - A trusted third party is trusted by a claimant and/or a verifier for the purposes of authentication.

3.28 **Validity Period:** Time period during which an identity or credential may be used in a transaction for authenticating an entity’s authorization, identity, or attribute information within a given context.

3.29 **Verification:** Process of checking identity proofing information and credentials against issuers, data sources, or other internal or external resources with respect to authenticity, validity, correctness, and binding to the entity.

3.30 **Verify:** Process of establishing the veracity of an assertion to a specified or understood level of assurance.

4 Abbreviations

For the purposes of this International Standard | Recommendation, the following abbreviations apply:

CSP	Credential Service Provider
EAAF	Entity Authentication Assurance Framework
IdM	Identity Management
ICT	Information and Communications Technology
IP	Internet Protocol
LoA	Level of Assurance
LoAs	Levels of Assurance
MAC	Media Access Control
PII	Personally Identifiable Information
PIN	Personal Identification Number
RA	Registration Authority
SAC	Service Assurance Criteria
SSL	Secure Sockets Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
TTP	Trusted Third Party

URL	Uniform Resource Locator

5 Conventions

This Recommendation | International Standard follows the ISO Directive, Part 2, Annex H regarding verbal forms for the expression of provisions.

a) “Shall” indicates a requirement;

b) “Should” indicates a recommendation;

c) “May” indicates a permission;

d) “Can” indicates a possibility and capability.

6 Levels of assurance

The cornerstone of the Entity Authentication Assurance Framework (EAAF) is the four Levels of Assurance (LoAs). Each LoA describes the degree of confidence that the entity asserting a particular identity (i.e., the claimant) is in fact the entity to which that identity was assigned.

This framework outlines four LoAs, with LoA1 being the lowest level of assurance and LoA4 being the highest level of assurance. Determining which LoA is appropriate in a given situation depends on a variety of factors. It is mainly based on the consequences of an authentication error and/or misuse of credentials, the resultant harm and impact, and their likelihood of occurrence. The higher the perceived risk, the higher the LoA should be. Lower authentication requests require low assurance, whereas higher risk authentication requests require more stringent assurance.

This framework articulates requirements and implementation guidance for each of the four LoAs. In particular, this Framework provides guidance for the implementation of the following processes and services:

e) Enrolment (application and initiation, proofing, verification, and registration)

f) Credential management (binding, issuance, and revocation)

g) Usage (authentication)

h) Record-keeping

It also provides requirements for management and organizational considerations (e.g., legal compliance, information security management) that affect authentication assurance.

The levels are defined as shown in Table 6-1.

Table 6-1 – Levels of assurance

Level	Description
1 – Low	Little or no confidence in the asserted identity
2 – Medium	Some confidence in the asserted identity
3 – High	High confidence in the asserted identity
4 – Very high	Very high confidence in the asserted identity

6.1 Level of assurance 1 (LoA1)

At LoA1, there shall be minimal confidence in the asserted identity. This LoA shall be used when no negative consequences result from erroneous authentication, and the authentication mechanism used provides some assurance. A wide range of available technologies and any of the types of credentials associated with higher LoAs, including username and PIN combinations, can satisfy the authentication requirement. This level shall not require use of cryptographic methods.

The electronic submission of forms by individuals can be LoA1 transactions when all information flows to the organization from the individual, there is no release of information in return, and the criteria for higher LoAs are not triggered.

For example, LoA1 may be applicable for transactions in which a claimant presents a self-registered username or password to a merchant's web page to create a customized page, or transactions involving web sites that require registration for access to materials and documentation, such as news or product documentation.

6.2 Level of assurance 2 (LoA2)

At LoA2, there shall be some confidence that the asserted identity is accurate. Moderate risk is associated with erroneous authentication. Single-factor authentication shall be acceptable. Successful authentication shall be dependent upon the claimant proving, through a secure authentication protocol, that he has control of the credential. Eavesdropper, replay, and online guessing attacks are prevented.

For example, a transaction in which a beneficiary changes an address of record through an insurance provider's web site may be a LoA2 transaction. The site needs some authentication assurance to ensure that the address is being changed by the claimant entitled to change it. However, this transaction involves a relatively low (moderate) risk of inconvenience. Since official notices regarding payment amounts, account status, and records of changes are sent to the principal’s address of record, the transaction additionally entails moderate risk of unauthorized release of PII.

6.3 Level of assurance 3 (LoA3)

LoA3 shall be used for transactions requiring high confidence in an asserted identity. This LoA shall be used where substantial risk is associated with erroneous authentication. This level shall employ multi-factor authentication. Identity proofing procedures shall be dependent upon verifiable identifying materials and information. Authentication shall be based on proof-of-possession of a key or password through a cryptographic protocol. Credentials may be “soft” or “hard” credentials.

For example, a transaction in which a patent attorney electronically submits confidential patent information to the Patent and Trademark Office can be a Level 3 transaction. Improper disclosure would give competitors an economic advantage. Other LoA3 transaction examples include online access to a brokerage account that allows the claimant to trade stock, approval by an executive of a transfer of funds out of an organization's bank accounts (up to a defined limit), or use by a third party contractor of a remote system to access potentially sensitive client personal information.

6.4 Level of assurance 4 (LoA4)

LoA4 shall be used for transactions requiring very high confidence in an asserted identity. This level provides the highest level of authentication assurance, based on proof-of-possession of a key through a cryptographic protocol. LoA4 is similar to LoA3, except that only hard credentials shall be used. High levels of cryptographic assurance shall be required for all elements of credential management. All PII and other sensitive data transfers shall be cryptographically authenticated using keys bound to the authentication process.

For example, access by a law enforcement official to a law enforcement database containing criminal records requires LoA4 protection. Unauthorized access could compromise investigations. Dispensation by a pharmacist of a controlled medication also requires LoA4 protection. The pharmacist needs full assurance that a qualified doctor prescribed the drug, and the pharmacist is likely to be criminally liable for any failure to verify the prescription and dispense the correct medication in the prescribed amount. Finally, approval by an executive of a transfer of funds in excess of prescribed limits from an organization's bank accounts would be a LoA4 transaction.

6.5 Selecting the appropriate level of assurance

Selection of the appropriate level of assurance for a transaction should be determined by a risk assessment. By mapping impact levels to LoAs, parties to an authentication transaction can determine what LoA they require and can procure services and place reliance on assured identities accordingly. Further information on assessing impact levels is provided in Table 6-2.

Table 6-2 – Potential impact at each level of assurance

Potential impact of authentication errors	Level of assurance*			
	1	2	3	4
Inconvenience, distress or damage to standing or reputation	Min	Mod	Sub	High
Financial loss or agency liability	Min	Mod	Sub	High
Harm to the entity, its programs, or public interests	N/A	Min	Mod	High
Unauthorized release of sensitive information	N/A	Mod	Sub	High
Personal safety	N/A	N/A	Min	Sub High
Civil or criminal violations	N/A	Min	Sub	High
* Min=Minimum; Mod=Moderate; Sub=Substantial; High=High				

Provision of services at each LoA shall be determined by the strength and rigor of the identity proofing process, the credential's strength, and the management processes the CSP applies to provision of its service. The EAAF establishes a need for operational service assurance criteria (SAC) at each LoA for CSPs. These criteria requirements are described at a high level in clause 11.

The risk assessment of the transaction should be conducted as a part of the individual's or the organization's overall information security risk assessment (e.g., as required by ISO/IEC 27001, where organizations are concerned), but should focus on the specific need for security in the transactions being contemplated. The risk assessment should address risk related to assurances of identity and to the environmental factors relating to the circumstances and conditions under which these transactions will take place (e.g., public kiosks are an inherently higher-risk environment than home computers or those installed in premises which have some kind of physical security). On the basis of the outcome of the risk assessment, a comparison should be made with the four LoAs and that which meets or exceeds the outcome of the risk assessment should determine the requisite LoA(s). Where multiple classes of transactions are envisaged there may be good reason to determine that a different LoA applies to each or to groups of them (i.e., multiple LoAs may be accepted by a single person or institution, according to the specific transaction in which they are engaged).

The individuals and organizations concerned should then take steps to:

a) Communicate to their counter-parties their expectations of acceptable assurances and therefore the credential LoA which counter-parties must possess;

b) Implement operational policies and technical controls to ensure that those LoAs are upheld within systems which execute the identified transactions (publication of policies, in part or whole, may effectively accomplish item a) above);

c) Have themselves (including all forms of entities within their domain) issued with credentials at the requisite LoA(s) in order to take their part in the identified transactions;

d) In the case of organizations, possibly put in place the means to issue credentials to their user communities, so as to facilitate their requirements in item a) above.

Providers of identity management and credentialing services shall undertake a risk assessment in order to ensure that their services are able to uphold the LoA at which they claim their services operate.

6.6 LoA mapping and interoperability

Different organizations may have their own LoAs, and these LoAs may not result in a 1-to-1 mapping to the four LoAs described in this Framework. For example, one organization may adopt the 4-level model, and another organization may adopt a 5-level model. Until Credential Service Providers (CSPs) are able to support the use of different authentication models, the various criteria for the different authentication models must be separately defined and widely communicated.

In order to achieve interoperability between different LoA models, each organization shall explain how its mapping scheme relates to the LoAs defined in this standard by:

a) Developing a well defined entity authentication assurance methodology, including well defined categories of LoAs;

b) Widely publishing this methodology so that others wishing to enter into federation-type agreements with them can clearly understand each others processes and terminology.

It is further recommended that the LoA methodology take into account and clearly define LoAs in terms of a risk assessment:

a) Expected threats;

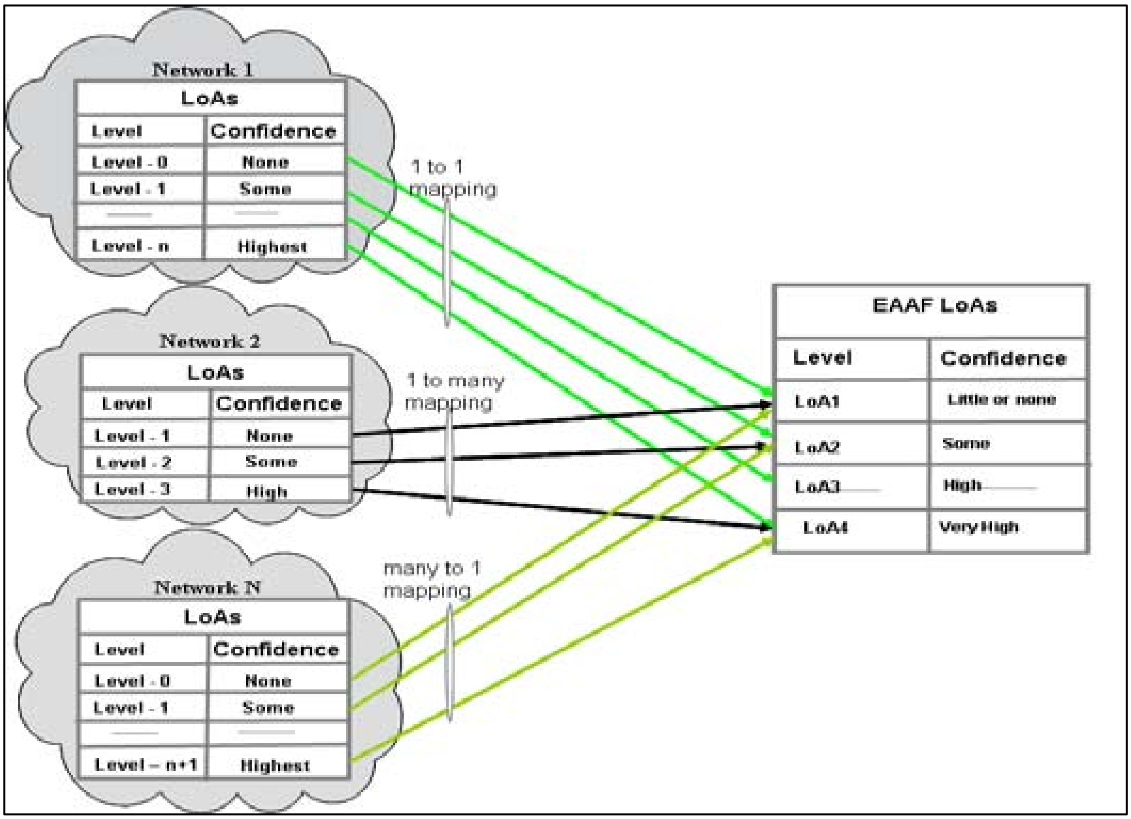
b) Levels of impact, (i.e., low, moderate), should threat become reality;

c) Identification of threats that must be controlled at each LoA;

d) Recommended security technologies and processes for use in implementing controls at each LoA.

One approach to address the issue of mapping/bridging between different LoA models would be to use the four-level model defined in this document and map other n-level models against it. That would allow identity federations using different models for authentication assurance to map against the four-level model. Mappings would need to define how un-mapped LoAs should be handled, which may be to simply ignore them or to effectively map them to the next lowest Level (since there could be no basis for assuming a higher LoA if it had not been specifically determined).

Figure 6-1 illustrates 1-to-1, 1-to-many, and many-to-1 mapping between the different variants.



Network 1

LoAs	
Level	Confidence
Level - 0	None
Level - 1	Some
—	—
Level - n	Highest

Network 2

LoAs	
Level	Confidence
Level - 1	None
Level - 2	Some
Level - 3	High

Network N

LoAs	
Level	Confidence
Level - 0	None
Level - 1	Some
—	—
Level – n+1	Highest

EAAF LoAs	
Level	Confidence
LoA1	Little or none
LoA2	Some
LoA3	High
LoA4	Very High

Figure 6-1 – Mapping LoAs

The remainder of this Framework addresses the structure within which processes and requirements for such services are established and covers threats and impacts relating to entity authentication before concluding with an overview of criteria against which services shall be assessed to ensure that they employ practices which support the achievement of credentialing services at each of the LoAs which the service supports.

7 Entity authentication assurance framework components

This clause is normative in that it describes the functional components of the Entity Authentication Assurance Framework (EAAF). Although the precise form of a conformant structure may differ from this Framework, its functional capacities shall meet the requirements set forth in this Framework. This Framework is technology agnostic.

The functional components of the EAAF are depicted in Figure 7-1.

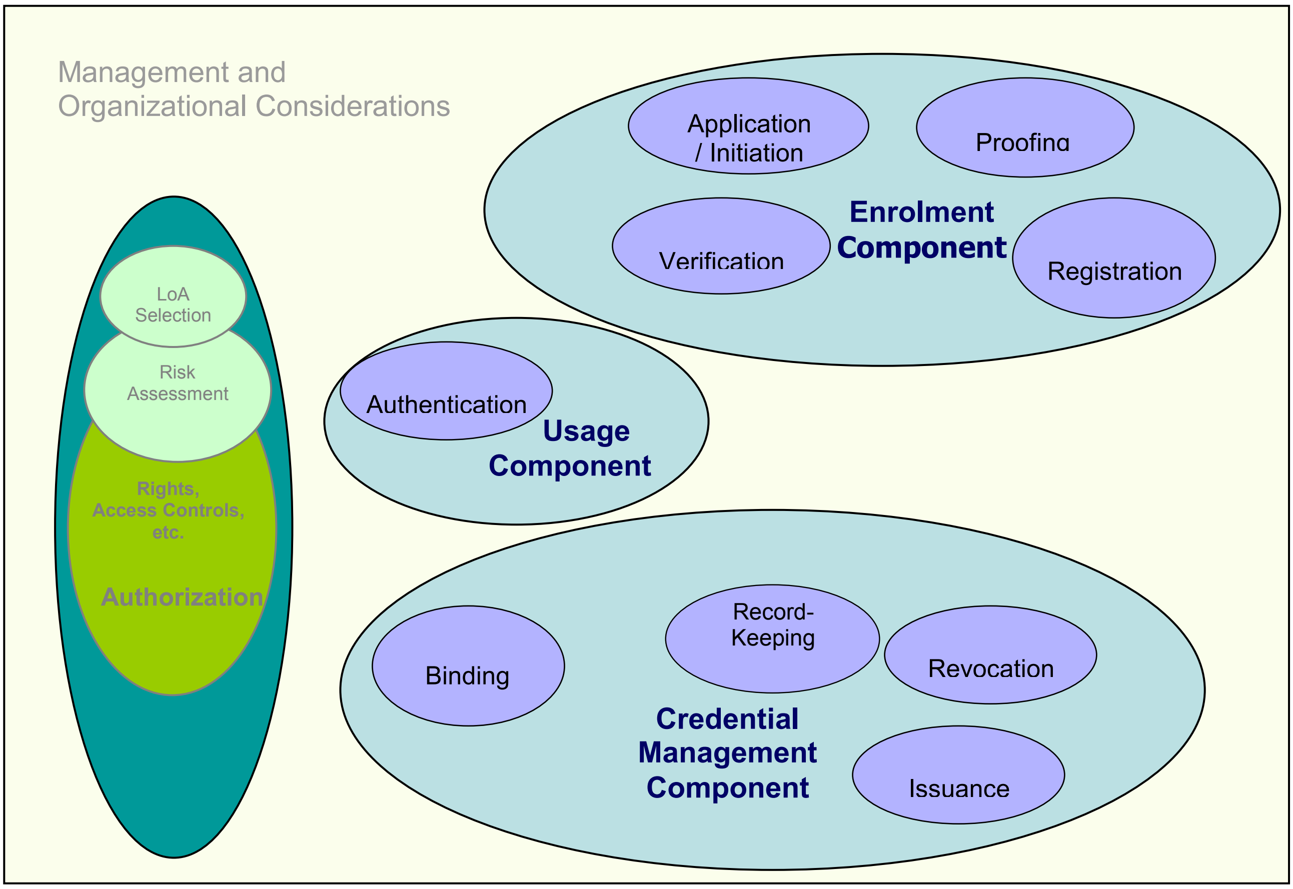


Figure 7-1 – EAAF components and functions

<Editor's note: Editor requests assistance in modifying this figure. The discussion from Melaka did not provide clear instructions. Please submit actual figure rather than comments on the figure.>

Organizations adopting this Framework shall establish policies and procedures that provide the necessary supporting functions and fulfil requirements set out in this Framework. These will vary according to the role chosen by a particular organization and, for instance, the Level or Levels of Assurance at which an organization provides credentials and authentication. For example, an organization may encounter the following:

a) Requirements for particular actions on behalf of the organization or its representatives related to particular LoA;

b) Requirements for external or third party assessment of an organization's operational capability within the EAAF;

c) Policies, actions, and capabilities necessary to facilitate the trustworthiness of the processes, services, and capabilities provided by organizations adopting the Framework.

The components are discussed below in the order in which they typically arise in entity authentication assurance processes.

7.1 Enrolment

The enrolment component is comprised of the processes leading up to and including registration of a principal. It consists of four processes: application and initiation; proofing; verification; and registration. These processes may be conducted entirely by a single organization, or they may consist of a variety of relationships and capabilities provided by a number of organizations including shared or interacting components, systems and services.

The required processes will differ according to the rigour required by the applicable LoA. In the case of a person enrolling under LoA1, these processes will be very minimal (e.g., an individual may click a "new user" button on a webpage and create a username and password). In other cases, enrolment processes could be extensive. For example, enrolment at LoA4 requires an in-person meeting between the future claimant and the RA, as well as verification of the proofing information provided by the future claimant.

7.1.1 Application and initiation

Prior to using the services of a CSP, the entities to which credentials will be issued should be introduced to the service. Although the requirements for identity proofing have already been discussed, the CSP should set forth the terms under which the service is provided, under which it may be used, any liabilities and legal agreements which must be accepted by and on behalf of principals/claimants and the mutual obligations of parties to the service.

These provisions will vary according to the LoA under which services are being provided and consumed. For example, at LoA1, a simple click-through agreement of basic terms may be sufficient for the purposes of the service and intended use. In contrast, at LoA3 or LoA4, where the service is supporting specific high-value transactions with high potential impacts should failures or breaches occur (e.g., large financial transactions, health and safety implications such as medical systems, air traffic control) then a more complex description of the terms of use and the consequences and obligations assumed by accepting the terms of use could be appropriate, possibly requiring witnessed signatures (electronic or ink).

7.1.2 Proofing

Proofing is the process of collecting information attesting to the identity of an entity. Different documents (e.g., identity cards, driver's licenses) may fulfil proofing requirements. The higher the required level of assurance, the more stringent proofing requirements shall be.

Just as four authentication factors (see clause 7.3.1) are used to determine a level of assurance, in human identity proofing, three categories containing five proofing objectives are used to establish an entity's identity to a specified level of assurance. Figure 7-2 shows the three categories containing five proofing objectives that information attesting to the identity of an entity needs to satisfy.

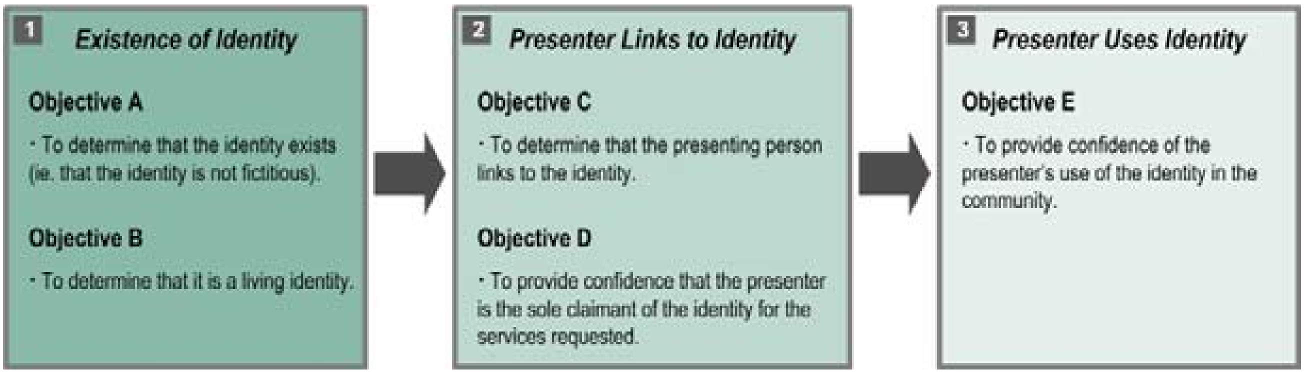

1
Existence of Identity
Objective A
• To determine that the identity exists (ie. that the identity is not fictitious).
Objective B
• To determine that it is a living identity.
2
Presenter Links to Identity
Objective C
• To determine that the presenting person links to the identity.
Objective D
• To provide confidence that the presenter is the sole claimant of the identity for the services requested.
3
Presenter Uses Identity
Objective E
• To provide confidence of the presenter's use of the identity in the community.

Figure 7-2 – Identity proofing objectives

Not all of the objectives in Figure 7-2 will necessarily need to be satisfied to establish an entity's identity. Proofing requirements will depend on the level of assurance in the identity that is required for the particular service. While high risk services will need identity proofing that satisfies each of the above objectives, meeting objectives A, D and E may provide enough assurance in an identity for a low risk service. Objective C, the individual links to the identity, is a vital aspect of the process, typically requiring the individual to produce a biometric identity document, such as one bearing a photograph.

Table 7-1 provides an overview of how the objectives apply to the LoAs. See clause 10.1.2 for the application of the identity proofing objectives to documentation requirements at given LoAs.

Table 7-1 – Applying Proofing Objectives to the LoAs

Level of Assurance	Objective A	Objective B	Objective C	Objective D	Objective E	Comment
1						Publish identity proofing policy.
2	√			√	√	Information accepted at 'face value' without third party verification unless discrepancies found in information proffered with the following two provisions: 1. A check of organisation records reveals no other person has claimed the same identity; and 2. Two information sources used - at least one of which is a primary form of identification (either the document itself or verification against records at an authoritative source); and a. At least one of which is a photograph; and b. At least one of which demonstrates that the identity is used by the principal in the community.
3	√	√	√	√	√	
4	√	√	√	√	√	As above, but provided by the principal 'in person,' or is verified with a third party to confirm its authenticity, plus any additional documentation the organisation's identity proofing policy requires.

7.1.3 Verification

This is the process of checking the proofing information against issuers, data sources, or other internal or external resources. Both the proofing and the verification process are performed in order to achieve a certain level of confidence in the identity of an entity before registering it as a particular claimant. Verification differs from proofing in the sense that it involves additional corroboration of proofing information with additional (either internal or external) sources (e.g., issuers of the proofing documents presented during enrolment). Although this process is sometimes referred to as "authentication," in this Framework that term has a very specific usage. See clause 7.3.1.

7.1.4 Registration

This is the process of concluding the enrolment of an entity. A record is created of the enrolment transaction. This record may include the information and documentation that was collected (and may be retained), the information about the verification process, the results of these steps, and other pertinent data. A decision is then rendered and recorded to accept, deny, or refer the enrolment for further examination or other follow up.

7.2 Credential management

The credential management component is comprised of the processes that enable an entity to join, participate within, and terminate participation in a particular context. This component consists of issuance, binding, revocation, record-keeping.

7.2.1 Issuance

Credential issuance is the process of providing an entity with a particular credential. The complexity of this process varies with the LoA required. For higher LoAs, this process may for example involve the secure delivery of a hard credential (e.g., a smart card) whereby the principal must collect the credential in person from the issuer (or his agent), after having received a registered letter requesting him to do so. In case of lower LoAs the issuance process might be a simple as sending a password or PIN to the claimant's [principal's] known address.

Where the credential issued to the claimant is a physical credential (e.g., smart card with cryptographic capabilities), the credential issuance process may involve the issuance of additional credentials which shall help to corroborate possession and control of the credentials during later authentication protocols. These additional credentials (e.g., PIN, password) are typically issued to mitigate risks associated with physical credential theft (see clauses 10.3.9 and 10.3.10).

7.2.2 Binding

Before a principal may be issued a credential for later authentication purposes, the issuer must ensure that the credentials it issues shall be clearly bound to that particular principal. Binding can be described as the process of establishing a durable association between a credential and a particular principal. The binding process must result in a record detailing which credential has been issued to which entity.

7.2.3 Revocation

This is the process for cancelling and ending the use of a credential. Credentials may be compromised, lost, stolen, expired, or removed from a claimant that is deemed no longer acceptable. It is important that revocation be conducted efficiently and quickly to prevent illegitimate use of a credential and thus to prevent access to or compromise of assets protected by authentication processes under the EAAF. While revocation is listed here, a range of related processes are also necessary under the EAAF and may include, among others, suspension, renewal, re-issuance, replacement, and termination.

7.2.4 Record-keeping

Throughout the life of a credential, including before and after its creation and activation, records shall be maintained, for a variety of service provision, technical operational and legal purposes. Distinct data may be required for specific purposes or may be applied by more than one aspect of the overall service provision and operation. At any time, the requirements for the collection, usage, protection, preservation and release of data (as specific instances of confidentiality, integrity, and availability paradigms) shall be observed according to the most stringent demands over the life of the data's retention and final destruction.

In general, higher LoAs may necessitate greater collation of data, even if some is retained for a relatively short time. It is inevitable that such data becomes increasingly sensitive in terms of its value per se and the potential for inferences being drawn when multiple data are accessed together. Management of these records is necessary, taking into account the nature of the data, the LoA, and the parties to whom and the terms under which that information may potentially released. See appendix A.

7.3 Credential usage

Credential usage is the point at which the CSP facilitates third-party reliance upon a claim of identity made by the claimant. This service is known as "authentication" and is concerned solely with the establishment (or not) of confidence in the claim, but has no bearing on or relationship with the actions the relying party may choose to take based upon an authenticated claim.

7.3.1 Authentication process

The authentication process is the use of a protocol to demonstrate possession and/or control of the credential in order to establish confidence in a claim of identity. Authentication protocol requirements vary based on the applicable LoA. For example, for a lower LoA, authentication could involve providing a password. At a higher LoA, authentication could involve a cryptographic based challenge-response protocol.

Authentication protocols involve the use of one or more authentication factors, which are the basis on which a RP develops confidence that another entity's identity is as claimed. Authentication factors are often divided into four categories:

a) Something the entity has (e.g., device signature, hard credential, private key)

b) Something the entity knows (e.g., password, PIN)

c) Something the entity is (e.g., biometric characteristic)

d) Something the entity typically does (e.g., typical behaviour patterns, such location of activities and times of activities)

Not all authentication factors provide the same strength, and different or combined factors are preferred for different LoAs. Moreover, different factors protect against different threats. For example, static passwords are considered weaker than one-time passwords, and a hard credential with a PIN is generally stronger than software credential. Factors can be combined for use in multi-factor authentication protocols to protect against certain threats. See clause 10.

8 Actors

The actors involved in the authentication process include principals, claimants, CSPs, RAs, RPs, verifiers, and trusted third parties.

8.1 Principals and claimants

A principal is an entity whose identity can be authenticated. The ability to authenticate a principal depends on a number of factors. In the context of this Framework, the ability to authenticate an entity implies that the principal has been registered and issued the appropriate credentials by a CSP and that an authentication protocol has been specified. During an authentication protocol, the principal may assert its own identity, but it is also possible that there is a separate entity representing the principal for the purposes of authentication. A claimant is an entity which is or represents a principal for the purposes of authentication.

8.2 Credential service provider

A credential service provider (CSP) is an entity that manages and issues credentials. Such credentials may include paper-based documents, usernames and passwords, smart cards, digital credentials. The types of credentials that are issued and the safeguards that are implemented by the CSP are key factors in determining which LoA will be reached during a particular authentication protocol (see also clause 10.3).

As indicated in the previous section, every entity will need to be issued one or more credentials to enable later authentication. Credentials are typically only issued after successful completion of an enrolment process, at the end of which the claimant is registered. Often the CSP operates its own registration service, but it is equally possible that registration is performed by a separate entity, called the Registration Authority (RA).

8.3 Registration authority

A Registration Authority (RA) is an entity that establishes and vouches for the identity of a principal to a CSP. The RA may be an integral part of a CSP, or it may be independent of a CSP, but it will in any event have a relationship to the CSP. The RA is trusted by the CSP to perform the registration service (i.e., the service of identifying entities) and registering them in a way that allows later assignment of credentials by the CSP.

Each RA will perform some form of proofing and verification according to a specified procedure. This is typically done through the evaluation of paper credentials (e.g., a national identity card, a driver's license), verification of records in databases or the sending of a request to a Trusted Third Party. In order to differentiate the claimant from other entities, it is typically assigned one or more distinguishing identifiers, which will allow the claimant to later be recognized in the domain of applicability.

8.4 Relying party

A relying party is an entity which needs to have a claimant authenticated and for this purpose places confidence in a specific authentication protocol. The relying party may require this authenticated identity for a variety of purposes, such as account management, access control, authorization decisions, non-repudiation, etc.

The relying party may itself perform the operations necessary to authenticate the principal, or it may entrust these operations to a verifier. In other words, the verifier and the relying party may the same entity, or they may be separate entities.

8.5 Verifier

A verifier is an entity which is or represents the entity requiring an authenticated identity. It is the entity which executes the specified authentication protocol by validating the claimant's credentials. The claimant may authenticate its identity to the verifier in a variety of manners. The authentication strength of the protocol used to do so will be a key factor in determining which LoA will be reached during a particular authentication protocol (see also clause 10.3)

The verifier may be a relying party, or a separate entity, which acts as a trusted party towards the verifier. If the latter is the case, then the verifier will typically, upon successful completion of the authentication protocol, provide the claimant or the relying party with an assertion that contains the result of the authentication.

The verifier may also be the CSP that initially issued the credential to the claimant.

8.6 Trusted third party

A trusted third party (TTP) is a security authority or its agent, trusted by other entities with respect to security related activities. In the context of this Framework, a TTP is trusted by a claimant and/or a verifier for the purposes of authentication. Examples of TTPs in the context of entity authentication include Certification Authorities (CAs) and Time-Stamping Authorities (TSAs).

8.7 Interactions among actors

Figure 8-1 describes the interactions among the actors. <Editor's note – please provide text to accompany figure.>

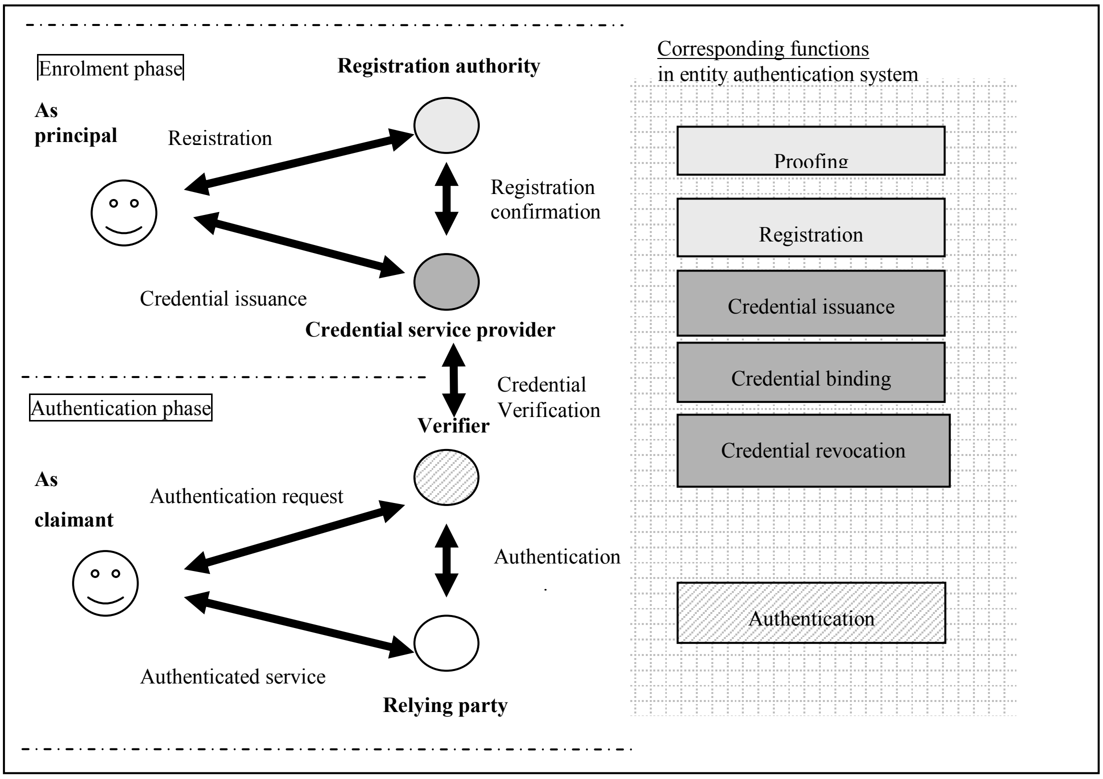


Figure 8-1 – Interactions among actors

9 Management and organizational considerations

Assurance in authentication comes not from technical factors alone, but also from consideration of how the service provision is managed and organized. A technically rigorous solution without competent management and operation can fall very much short of its potential for providing security in the provision of entity authentication assurance.

This clause discusses management and organizational factors that influence assurance and establishes requirements for these elements of a service. How they might vary with LoA is addressed. These factors are further considered in clause 11.

9.1 Established service

Establishment addresses both the legal status of the service provider and the status of the functional service provision. In the first case, knowing that the provider of identity management and authentication services is a registered legal entity gives confidence that the CSP is a bona fide enterprise in the jurisdiction within which it operates. This becomes more significant when service components are operated by different legal entities (e.g., registration as a separate function). In terms of the functional service provision, it shall be established that the service is fully operational, rather than being a sub-set of the required total functionality (e.g., a fully-developed proofing and credentialing capability with no actual means to authenticate issued credentials when presented in the context of a transaction has no assurance of its overall provision).

Although the basic requirements are the same for all LoAs, greater assurance requirements shall have greater dependency on the service provision being complete and reliable. For instance, at LoA3 and above, greater assurance about the CSP shall also be taken from knowledge of its corporate ties and understanding of the level of independence it is permitted in its operations.

9.2 Legal and contractual compliance

All EAAF actors shall understand and comply with any legal requirements incumbent on them in connection with operation and delivery of the service. This has implications including, but not limited to the types of information that may be sought, how verification is conducted, and what information may be retained. Although PII considerations apply for human entities (see appendix A), there may be similar concerns with other entities, at least insofar as their "sponsors" are concerned (i.e., the legal entity owning or taking responsibility for any machine entity). Account shall also need to be taken of all jurisdictions within which the CSP operates. At LoA2 and higher, specific policy and contractual requirements shall also be identified.

9.3 Data retention and disposal

As a specific case of legal compliance, at LoA2 and above the service provision shall be shown to be compliant with requirements incumbent upon it concerning the retention and disposal of private and identifiable information (e.g., PII, business information). Disposal options may include archiving, anonymization, or destruction of information.

9.4 Financial provisions

Where long-term availability of services is a consideration in both a claimant's and relying parties' expectations, financial stability shall be shown, sufficient to ensure the continued operation of the service and to underwrite the degree of liability exposure being carried. For LoA1 services and reliance, such provisions are unlikely to be a consideration, whereas services supporting more significant transactions at LoA2 and higher shall address such needs.

9.5 Notices and user information

The nature and extent of services, to both claimants and relying parties, shall be clearly set out in appropriate publications and media, as shall be the terms and conditions of use. As the level of assurance being supported increases so shall the extent and level of detail provided. This could require more explicit types of documentation (e.g., limitations on usage, liability), required agreements, policies applied, etc. Records of agreements shall also be retained, even at the lowest levels of assurance.

9.6 Information security management

How a CSP manages the security of its business in general, the specified service, and information it holds relating to its user community will each contribute to the dependence, hence assurance, placed upon its authentication services. At LoA1, no such consideration need be applied. However, at LoA2 and higher, organizations shall have in place defined information security management practices, policies, approaches to risk management and other recognised controls, so as to provide assurance that effective practices are in place which ensure that the service is being operated as defined. From LoA3 onwards, a formal management system such as defined in ISO/IEC 27001 and supported by other standards in the 27000-family will be a sound basis for the delivery of this assurance.

9.7 Security audit and records

Allied closely to the information security management effected by an organization is the assurance that can be provided by having frequent reviews of its operations and adherence to its policies and procedures. At LoA2 and higher, this assurance can be supported by security audits, both internal and external, and the secure retention of records of significant events, including those audits. The rigour applied shall be in keeping with the rigour imposed by the selected information security management approach.

9.8 Operational infrastructure

A well-defined operational environment with appropriate infrastructure elements is a further means of ensuring that the service provision is competently managed, in turn providing assurance that the authentication can be relied upon. Establishing an effective infrastructure shall include having security controls which suit the service and the risks facing it, ensuring that proper roles are defined and that there are adequate personnel trained to fulfil them and that access to systems and services is adequately controlled. These measures are typically not necessary for LoA1, but at LoA2 and above will have increasing significance.

9.9 External service components

When an organization is dependent upon third parties for elements of its service, how it directs the actions of these parties and oversees them will contribute to assurance about the overall service provision. Arrangements with third parties shall be proportional to the LoA and to the information security management being applied. At LoA1, such assurance shall have a minimal effect, but that from LoA2 and up, these measures contribute to the overall assurance being given.

10 Threats and controls

This clause describes threats to each component of the EAFF and provides required controls for each LoA.

10.1 Threats to the enrolment component

The following subclauses describe threats and provide controls to the enrolment component.

10.1.1 Registration and proofing threats

The primary threats to the registration and proofing processes are impersonation and compromise of the infrastructure. Some examples of impersonation are when a claimant illegitimately asserts another claimant's identity by using a forged driver's license or when a device registers with a network using a spoofed Media Access Control (MAC) address. An example of compromise of the infrastructure is poor information security controls leading to the modification to the registration data.

10.1.2 Controls against registration and proofing threats

<Editor's note: Please provide suggestions for making registration and proofing controls less government-centric and more universally applicable. See WD6 DoC – [TAS[3]] 26 and [JP] 27.>

At LOA1, there is little or no confidence in the asserted identity. Controls should include the following:

a) The RA should have in place a policy which ensures that credentials issued by it can be distinguished from those issued by other organizations. The policy should also ensure that an identity for which a credential is issued for each claimant is unique within its universe of identities;

b) Allow self assertion of identity and trust that the evidence provided is not fraudulent;

c) If remote registration is used, the claimant should provide contact information such as an email address or phone number. Verification should be done by calling the number or successfully sending a confirmation email and receiving acknowledgement.

At LOA2, there shall be some confidence in the asserted identity. Controls should include the following:

a) Publish the identity proofing policy;

b) Perform all identity proofing in accordance with its published identity proofing policy;

c) For in-person identity proofing, ensure that the claimant is in possession of a primary government picture identification document that bears a photographic image of the holder that matches the appearance of the claimant and states an address at which the claimant can be contacted;

d) For in-person identity proofing, ensure that the presented document appears to be a genuine document properly issued by the claimed CSP and valid at the time of application;

e) For remote identity proofing, ensure that the claimant submits the references of and attests to current possession of at least one primary government picture identification document, and either a second government identification document or an employee or student identification number; a financial account number (e.g., checking account, savings account); or a utility service account number (e.g., electricity, gas, water) for an address matching that in the primary document;

f) Ensure that the claimant provides additional verifiable personal information that at a minimum must include a name that matches the referenced picture identification document;

g) Verify the existence of such records with matching name and reference numbers. Corroborate date of birth, current address of record, and other personal information sufficient to ensure a unique identity. Confirm address of record by at least one of the following means:

   1) RA sends notice to an address of record confirmed in the records check and receives a mailed or telephonic reply from claimant;

   2) CSP issues credentials in a manner that confirms the address of record supplied by the claimant, for example by requiring claimant to enter on-line some information from a notice sent to the claimant; or

   3) CSP issues credentials in a manner that confirms ability of the claimant to receive telephone communications at telephone number or email at email address associated with the claimant in records. Any secret sent over an unprotected channel shall be reset upon first use.

At LoA3, there shall be high confidence in the asserted identity. Controls should include the following:

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

   1) The existence of such records with matching name and reference numbers;

   2) Corroboration of date of birth, current address of record or personal telephone number, and other personal information sufficient to ensure a unique identity;

   3) Dynamic verification of personal information previously provided by or likely to be known only by the claimant.

b) Confirm address of record by at least one of the following means:

   1) RA sends notice to an address of record confirmed in the records check and receives a mailed or telephonic reply from claimant;

   2) CSP issues credentials in a manner that confirms the address of record supplied by the claimant, for example by requiring claimant to enter on-line some information from a notice sent to the claimant; or

3) CSP issues credentials in a manner that confirms ability of the claimant to receive telephone communications at telephone number or e mail at e mail address associated with the claimant in records. Any secret sent over an unprotected channel shall be reset upon first use.

At LoA4, there shall be very high confidence in the asserted identity. Controls should include the following:

a) The physical presence of the claimant in front of the RA. Remote verification is not permitted at this level. The claimant must have with him/her a picture identification document or other readily verifiable identity information, as well as the following added requirements

   1) A primary government picture identification document and either:

      i) Second government picture identification document;

      ii) An account number issued by a financial institution; or

      iii) Two items confirming name and address or telephone number (e.g., utility bill, professional license, membership).

b) Assurance that the presented picture identification document:

   1) Appears to be a genuine document properly issued by the claimed issuing authority and valid at the time of application;

   2) Contains a photographic image of the holder which matches the appearance of the claimant;

   3) States an address at which the claimant can be contacted;

   4) Is electronically verified by a record check with the specified CSP or through similar databases that establishes the existence of such records with matching name and reference numbers and corroborates date of birth, current address of record, and other personal information sufficient to ensure a unique identity.

c) For device identity proofing, required identity information may include common name, description, serial number, MAC address, owner, location, and manufacturer.

10.2 Threats to the credential management component

The following subclauses describe threats and provide controls to the credential management component.

10.2.1 Issuance threats

Threats to the issuance process involve either an impersonation attack or a threat to the mechanism for the credential issuance. Table 10-1 describes issuance threats and provides examples of each type of threat.

Table 10-1 – Issuance Threats

Threat/attack	Example
Disclosure	A password created by the CSP for a claimant is copied by an attacker as it is transported from the CSP to the claimant during credential establishment.
Tampering	A new password created by the claimant is modified by an attacker as it is being submitted to the CSP during credential establishment phase.
Masquerading	A person claiming to be the claimant, but in reality is not the claimant, is issued credentials for that claimant.

10.2.2 Controls against issuance threats

At LOA1, there is little or no confidence in the asserted identity. Controls shall include the following:

a) Credentials should only be generated after authentication of source of the request for the credentials (i.e., RA);

b) Take steps to ensure that the identity to which a credential refers is unique within its context;

c) Claimant can choose his own credential (e.g., username and password), but only after the system has performed a check that it is unique within the context.

At LOA2, there shall be some confidence in the asserted identity. Controls shall include the following:

a) Review and modification procedures should be in place to allow the updating of data relating to the claimant after registration (e.g., pursuant to a modification request of the claimant provided the claimant (or the request) has been successfully authenticated and subject to applicable policy);

b) Design passwords and one-time passwords to take into account state-of-the-art attack methods, the life span of a password's use, and an estimation of number of attacks (guesses) it will have to withstand;

c) Ensure that software cryptographic keys stored on general-purpose devices are protected by a key and cryptographic protocols that are evaluated against ISO/IEC 19790, or equivalent, as established by a recognized national technical authority; hard credentials used to store cryptographic keys should employ cryptographic modules that are like-wise evaluated against ISO/IEC 19790, or equivalent;

d) Keep records for each credential, listing name of user, entities acting on behalf of user in a manner that can unequivocally associate the credential and the identity that it asserts;

e) Send an issuance notice to the claimant to which the credential is issued using the claimant's contact information address of record confirmed during identity proofing. If electronic notification is used, send the notice and/or credential in a way that confirms the email address of record supplied by the claimant during the identity proofing process.

At LoA3, there shall be high confidence in the asserted identity. Controls shall include the following:

a) If passwords are issued, only allow one-time password systems; no repeatable password systems should be used;

b) One-time passwords should use cryptography as the basis for their generation, and the key should be stored on a device evaluated against ISO/IEC 19790 and require password or biometric activation by the claimant;

c) If the specified service generates the claimant's keys, use an approved algorithm, as established by a recognized technical authority, that is recognized as being fit for the purposes of the transaction service;

d) Only create keys of a key length and for use with a approved public key algorithm, as established by a recognized technical authority, recognized as being fit for the purposes of the transaction service;

e) Generate and store the keys securely until delivery to and acceptance by the claimant;

f) If public key cryptography is used, deliver the claimant's private key in a manner that ensures that the confidentiality of the key is not compromised and only the claimant has access to the private key.

At LoA4, there shall be very high confidence in the asserted identity. Controls shall include the following:

a) Do not issue passwords, one- time passwords, or software cryptographic credentials;

b) Only issue hard credentials (e.g., smart card). Ensure that they use a cryptographic module that is evaluated against ISO/IEC 19790 level 2 or higher as determined by a recognized technical authority. Also, ensure that physical security of the module is evaluated at level 3 of ISO/IEC 19790 or higher;

c) Require password or biometric activation of the credential by the claimant;

d) If the issuing organization generates the claimant's private key and its related public key, ensure that the key generation process securely and uniquely binds that process to the certificate generation and maintains at all times the confidentiality of the private key until it is accepted by the claimant;

e) Maintain records of all attributes provided by the claimant during the enrolment process in a manner that can be unequivocally associated with the credential and the identity that it asserts;

f) For credential delivery, the issuing service must notify the claimant of the credential issuance and, if necessary, confirm claimant's contact information;

g) Before activating the credential, the issuing organization must receive acknowledgement of receipt of the credential from the claimant.

10.2.3 Credential management threats

Credentials are only as strong as the strength of the management mechanisms used to secure them. These threats represent the potential to breach the confidentiality, integrity, and availability of credentials. Table 9-2 provides a non-exhaustive listing of credential management threat categories, as well as examples for each of these threat categories.

Table 10-2 – Credential management threats

Credential management activity	Threat/attack	Example
Credential storage	Disclosure	Usernames and passwords stored in a system file are revealed.
	Tampering	The file that maps usernames to passwords within the CSP is hacked so that the mappings are modified, and existing passwords are substituted with passwords known to the attacker.
Credential verification services	Disclosure	An attacker is able to view requests and responses between the CSP and the verifier.
	Tampering	An attacker is able to masquerade as the verifier and provide bogus responses to the verifier's password verification requests.
	Unavailability	The password file or the verifier is unavailable to provide password and username mappings.
		Public key certificates for entities are unavailable to the verifier because the directory systems are down (for example for maintenance or as a result of a denial of service attack).
Credential renewal/re-issuance	Disclosure	Password renewed by the CSP for a claimant is copied by an attacker as it is transported.
	Tampering	New password created by the claimant is modified by an attacker as it is being submitted to the CSP to replace an expired password.
	Unauthorized renewal/re-issuance	Attacker fools the CSP into issuing a new credential for a current claimant, and the new credential binds the current claimant's identity with a credential provided by the attacker. For non-human entities, an example can be re-labelling (re-issuing) a system component (e.g., RAM) as new after it has been used.
		Attacker is able to take advantage of a weak credential renewal protocol to extend the credential validity period for a current claimant.

Credential management activity	Threat/attack	Example
Credential revocation/destruction	Delayed revocation/destruction of credentials	Stale certificate revocation lists allow accounts (that should have been locked as a result of credential revocation) to be used by an attacker.
		User accounts are not deleted when employees leave a company leading to a possible use of the old accounts by unauthorized persons.
	Credential use after decommissioning	A hard credential is used after its cryptographic keys have been revoked.

10.2.4 Credential management controls

At LoA1, the following controls shall be required.

a) Credential storage – files of shared secrets used by CSPs at LoA1 shall be protected by access controls that limit access to administrators and only to those applications that require access. Such shared secret files shall not contain the plaintext passwords; typically, they contain a one-way hash or "inversion" of the password. In addition, any method allowed for the protection of long-term shared secrets at LoAs 2, 3 or 4 may be used at LoA1;

b) Credential verification services – secret credentials should not be shared with other parties unless absolutely necessary;

c) Credential renewal and re-issuance – no requirements;

d) Credential revocation and destruction – no requirements;

e) Records retention – no requirements.

At LoA2, the following controls shall be required.

a) Credential storage – files of shared secrets used by CSPs at LoA2 shall be protected by discretionary access controls that limit access to administrators and only to those applications that require access. Such shared secret files shall not contain the plaintext passwords or secrets; an alternative method may be used to protect the shared secret;

   1) Passwords may be concatenated to a salt (variable across a group of passwords that are stored together) and then hashed with an algorithm so that the computations used to conduct a dictionary or exhaustion attack on a stolen password file are not useful to attack other similar password files. The hashed passwords are then stored in the password file. The salt may be composed using a global salt (common to a group of passwords) and the username (unique per password) or some other technique to ensure uniqueness of the salt within the group of passwords.

   2) Shared secrets should be stored in encrypted form, and the needed secret decrypted only when immediately required for authentication. In addition, any method allowed to protect shared secrets at LoAs 3 or 4 may be used at LoA2;

b) Credential verification services – shared secrets, if used, shall never be revealed to any party except the Claimant and CSP (including verifiers operated as a part of the CSP); however, session (temporary) shared secrets may be provided by the CSP to independent verifiers;

c) Cryptographic protections are required for all messages between the CSP and verifier which contain private credentials or assert the authority of weakly bound or potentially revoked credentials. Private credentials shall only be sent through a protected channel to an authenticated party to ensure confidentiality and tamper protection;

d) The CSP may send the verifier a message, which either asserts that a weakly bound credential is valid, or that a strongly bound credential has not been subsequently revoked. In this case, the message shall be logically bound to the credential, and the message, the logical binding, and the credential shall all be transmitted within a single integrity protected session between the verifier and the authenticated CSP. If revocation is an issue, the integrity protected messages shall either be time stamped, or the session keys shall expire with an expiration time no longer than that of the revocation list. Alternatively, the time stamped message, binding, and credential may all be signed by the CSP, although, in this case, the three in combination would comprise a strongly bound credential with no need for revocation;

e) Credential renewal and re-issuance – the CSP shall establish suitable policies for renewal and re-issuance of credentials. Proof-of-possession of the unexpired current credential shall be demonstrated by the Claimant prior to the CSP allowing renewal and re-issuance. Passwords shall not be renewed; they shall be re-issued. After expiry of the current credential, renewal and re-issuance shall not be allowed. All interactions shall occur over a protected channel such as SSL/TLS.;

f) Credential revocation and destruction – CSPs shall revoke or destroy credentials within 72 hours after being notified that a credential is no longer valid or has been compromised to ensure that a claimant using the credential will no longer be able to successfully authenticate himself. If the CSP issues credentials that expire automatically within 72 hours (e.g., issues fresh certificates with a 24 hour validity period each day) then the CSP is not required to provide an explicit mechanism to revoke the credentials. CSPs that register passwords shall ensure that the revocation or de-registration of the password can be accomplished in no more than 72 hours;

g) Records retention – A record of the registration, history, and status of each credential (including revocation) shall be maintained by the CSP or its representative. All entities shall comply with applicable legislation concerning records and data retention.

At LoA3, the following controls shall be required.

a) Credential storage – files of long-term shared secrets used by CSPs or verifiers at LoA3 shall be protected by discretionary access controls that limit access to administrators and only to those applications that require access. Such shared secret files shall be encrypted with the encryption key for the shared secret file being encrypted under a key held in a cryptographic module (hardware or software) and decrypted only as immediately required for an authentication operation;

b) Shared secrets shall be protected with a key within the cryptographic module and are not exported in plaintext from the module;

c) Strongly bound credentials support tamper detection mechanisms such as digital signatures, but weakly bound credentials shall be protected against tampering using access control mechanisms as described above;

d) Credential verification services – CSPs shall provide a secure mechanism to allow verifiers or RPs to ensure that the credentials are valid. Such mechanisms may include on-line verification servers or the involvement of CSP servers that have access to status records in authentication transactions;

e) Temporary session authentication keys may be generated from long-term shared secret keys by CSPs and distributed to third party verifiers, as a part of the verification services offered by the CSP, but long-term shared secrets shall not be shared with any third parties, including third party verifiers. This type of third-party (or delegated) verification is used in the realm of GSM (Global System for Mobile Communications) roaming; the locally available network authenticates the “roaming” claimant using a temporary session authentication key received from the Base Station. Such temporary session authentication keys are typically created by cryptographically combining the shared secret with a nonce challenge. The challenge and session key are securely transmitted to the verifier. The verifier in turn sends only the challenge to the claimant, and the claimant applies the challenge to the long-term shared secret to generate the session key. Both claimant and verifier now share a session key, which can be used for authentication. Such verification schemes are permitted at this level provided that approved cryptographic algorithms are used for all operations;

f) Credential renewal and re-issuance – Renewal and re-issuance shall only occur prior to expiration of the current credential. Claimants shall authenticate to the CSP using the existing credential in order to renew or re-issue the credential. All interactions shall occur over a protected channel such as SSL/TLS;

g) Credential revocation and destruction – CSPs shall have a procedure to revoke credentials within 24 hours. Verifiers shall ensure that the credentials they rely upon are either freshly issued (within 24 hours) or still valid. Shared secret based authentication systems may simply remove revoked claimants from the verification database.

h) Records retention – all requirements from LoA2 apply.

At LoA4, the following controls shall be required.

a) Credential storage – all requirements from LoA3 apply;

b) Credential verification services – all requirements from LoA3 apply;

c) Credential renewal and re-issuance – sensitive data transfers shall be cryptographically authenticated using keys bound to the authentication process. All temporary or short-term keys derived during the original authentication operation shall expire and re-authentication shall be required after not more than 24 hours from the initial authentication;

d) Credential revocation and destruction – CSPs shall have a procedure to revoke credentials within 24 hours. Verifiers or RPs shall ensure that the credentials they rely upon are either freshly issued (within 24 hours) or still valid. It is generally good practice to destroy a credential within 48 hours of the end of its life or the end of the claimant's association with the CSP. Destroying includes either the physical destruction of the credential or cleansing it of all information related to the Claimant;

e) Records retention – all requirements from LoA2 apply.

10.2.5 Credential threats

Unmitigated threats can result in an attacker gaining control of a credential and masquerading as the claimant to whom the credential was actually issued. There are many threats to credentials, and table 9-3 lists some of those threats and provides specific examples.

Table 10-3 – Credential threats

Credential threats/attacks	Description	Examples
Theft	A credential with a physical manifestation is stolen by an attacker.	Hardware credential stolen. One-time password device stolen. Lookup credential stolen. Cell phone stolen.
Discovery	The responses to credential prompts are easily discovered through searching various data sources.	Asking the question "What is your phone number?" for authentication when the phone number can be found in the phone book.
Duplication	The claimant's credential has been copied with or without his or her knowledge.	Passwords written on paper disclosed. Passwords stored in electronic file copied. Software PKI credential (private key) copied.
Credential threats/attacks	**Description**	**Examples**
Eavesdropping	The secret credential (e.g., password) is revealed to the attacker as the claimant is submitting the credential to send over the network.	Shoulder surfing of passwords. Keystroke logging on keyboard. PIN captured from PIN pad device. Fingerprint data captured from reader.
Offline cracking	The credential is exposed using analytical methods outside the authentication mechanism.	Differential power analysis on stolen hardware cryptographic credential. Software PKI credential is subjected to dictionary attack to identify correct PIN, password, or passphrase to use the private key within credential.
Phishing or pharming	The secret credential is captured by fooling the claimant into thinking the	Password revealed by claimant to website impersonating as the verifier.

		Password revealed by claimant in response to an email inquiry from a phisher pretending to represent a bank.
		Password revealed by claimant at a bogus verifier website reached through DNS re-routing.
Social engineering	An attacker establishes a level of trust with a claimant in order to convince the claimant to reveal his or her credential or secret credential.	Credential revealed by claimant to officemate asking for password on behalf of supervisor.
		Credential revealed by claimant in telephone inquiry from masquerading system administrator.
Online guessing	An attacker connects to the verifier online and attempts to guess a valid secret credential in the context of that verifier.	Online dictionary attacks to guess passwords.
		Online guessing of a password registered to legitimate claimant.

10.2.6 Controls against credential threats

The following subclauses list credential requirements for single and multi-factor authentication.

Often, the use of a single factor will not protect against all types of attacks, and multiple factors should be used. To achieve LoA3 and above, one of the two credentials used in a multi-credential scheme shall be rated at LoA3, or, both credentials shall be rated at LoA2 and represent two different factors of authentication. For example, a secret credential (e.g., password) combined with a lookup credential (e.g., lookup card password) can be used to achieve LoA3, since the lookup credential is “something you have” and the secret credential is “something you know”. However, combining a multi-factor software cryptographic credential (which is rated at LoA3) and a secret credential (which is rated at LoA2) still achieves an overall LoA3, since the addition of the secret credential does not lower the assurance of the combination.

10.3 Threats to the usage component

Credentials are often subject to attack by a variety of methods during their use in the authentication process. Table 9-4 lists some broad categories of threats to the authentication process itself and provides examples to illustrate the threats.

Table 10-4 – Usage threats

Type of Attack	Description	Example
Online guessing	An attacker performs repeated logon trials by guessing possible values of the secret credential.	An attacker navigates to a web page and attempts to log in using a claimant’s username and commonly used passwords, such as “password” and “secret”.
Phishing	A claimant is lured to interact with a counterfeit verifier, and tricked into revealing his or her password or sensitive personal data that can be used to masquerade as the claimant.	A claimant is sent an email that redirects him or her to a fraudulent website and is asked to log in using his or her username and password.
Pharming	A claimant that is attempting to connect to a legitimate verifier is routed to an attacker’s website through manipulation of the domain name service (DNS) or routing tables.	A claimant is directed to a counterfeit website through DNS poisoning and reveals or uses his or her credential believing he or she is interacting with the legitimate verifier.

Eavesdropping	An attacker listens passively to the authentication protocol to capture information which can be used in a subsequent active attack to masquerade as the claimant.	An attacker captures the transmission of a password or password hash from a claimant to a verifier.
Replay	An attacker is able to replay previously captured messages (between a legitimate claimant and a verifier) to authenticate as that claimant to the verifier.	An attacker captures a claimant's password or password hash from an actual authentication session, and replays it to the verifier to gain access at a later time.
Session hijack	An attacker is able to insert himself or herself between a claimant and a verifier subsequent to a successful authentication exchange between the latter two parties. The attacker is able to pose as a claimant to the relying party or vice versa to control session data exchange.	An attacker is able to take over an already authenticated session by eavesdropping on or predicting the value of authentication cookies used to mark HTTP requests sent by the claimant.
Man-in-the-middle	The attacker positions himself or herself between the claimant and relying party so that he or she can intercept and alter the content of the authentication protocol messages. The attacker typically impersonates the relying party to the claimant and simultaneously impersonates the claimant to the verifier. Conducting an active exchange with both parties simultaneously may allow the attacker to use authentication messages sent by one legitimate party to successfully authenticate to the other.	An attacker breaks into a router that forwards messages between the verifier and a claimant. When forwarding messages, the attacker substitutes his or her own public key for that of the verifier. The claimant is tricked into encrypting his or her password so that the attacker can decrypt it.
		An attacker sets up a fraudulent website impersonating the relying party. When an unwary claimant tries to log in using his or her one time password device, the attacker's website simultaneously uses the claimant's one time password to log in to the real relying party's website.

For threats to the usage process, it is not appropriate to delineate controls in terms of LoA. Some controls may not be appropriate for all contexts. For example, controls for authentication of users accessing online magazine subscriptions are probably different from medical doctors accessing patient records. Therefore, it is recommended that as the risk and consequence of exploitation grows more severe, the system designer should consider security in depth: layering protective measures appropriate to the operational environment, the application and the LoA of assurance deemed necessary. This clause describes attacks and provides controls for each type of attack. It is up to the system designer, based on risk analysis, to make the decisions as to how and when and in what combination to use these controls.

10.3.1 Network eavesdropping

Eavesdroppers generally attempt to obtain secret credentials (e.g., password) to pose as claimants. Thus, if passwords are passed in plaintext from client to server, an attacker can capture traffic and obtain user names and passwords. Using rudimentary network monitoring software, an eavesdropper on a host on the same network can observe authentication protocol message exchanges and can use this information at a later time in a replay attack or for other purposes.

10.3.2 Controls against network eavesdropping

The following controls should be applied as determined necessary by a risk assessment:

a) Use of authentication mechanisms that do not transmit passwords over the network, such as the Kerberos protocol;

b) If authentication exchange over the network is necessary, encrypt that data and/or encrypt the communication channel (e.g., TLS in anonymous mode);

c) As authentication implementations may be subject to replay attacks, use a different authentication parameter for each authentication transaction.

10.3.3 Replay attacks

A replay attack is one in which a valid data transmission is maliciously or fraudulently repeated. This is carried out by an attacker who intercepts the data and retransmits it, possibly as part of a masquerade attack with the goal of data modification.

10.3.4 Controls against replay attacks

The following controls should be applied as determined necessary by a risk assessment:

a) Require a different authentication parameter for each authentication transaction (e.g., one-time password, session credential);

b) Timestamp each message with a non-forgeable timestamp.

10.3.5 Cookie replay attacks

In a cookie replay attack, the attacker captures the user's authentication cookie using monitoring software and replays it to the application to gain access under a false identity.

10.3.6 Controls against cookie replay attacks

The following controls should be applied as determined necessary by a risk assessment:

a) Use an encrypted communication channel whenever an authentication cookie is transmitted;

b) Use a cookie timeout value that forces authentication after a relatively short time interval. Although this does not prevent replay attacks, it reduces the time interval in which the attacker can replay a request without being forced to re-authenticate because the session has timed out;

c) In order to assure that the authentication information is not used in a new cookie, apply the general anti-replay controls specified in clause 10.3.4.

10.3.7 Threats to credentials

Threats to credentials can be categorized into attacks on the four types of authentication factors: "something the entity has," "something the entity knows," "something the entity is," and "something the entity typically does".

"Something the entity has" refers to a physical credential. When attacked, it may be stolen from the claimant or cloned by the attacker. For example, a hardware credential might be stolen or duplicated.

"Something the entity knows" refers to credentials such as passwords, pass-phrases, or other secret knowledge used to authenticate a claimant.

"Something the entity is" refers to authentication mechanisms using personal characteristics of the claimant, such as fingerprints, voice recognition, or gait. This type of authentication factor may be subject to a replication or spoofing attack. For example, an attacker could obtain a copy of a claimant's fingerprint and construct a replica.

"Something an entity typically does" refers to authentication mechanisms using the typical behaviours of the claimant, such as usual location based on IP address, usual login times, etc. For example, a credential has likely been compromised if a claimant tries to authenticate from two different countries in a span of three minutes.

<Editor's note: Please provide content for the last factor contributed by AU at Melaka.>

10.3.8 General controls against credential compromise

The following controls should be applied as determined necessary by a risk assessment:

a) Employ multi-factor authentication, whereby a combination of two or more credentials are used in combination;

b) Employ physical security, where appropriate. Physical security mechanisms can provide tamper evidence, detection, and response;

c) Use and enforce strong passwords;

d) Use system and network security controls to prevent an attacker from gaining access to a system or installing malicious software;

e) To counter the possibility of the browser cache allowing login access, create functionality that either allows the user to choose to not save credentials, or force this functionality as a default policy.

10.3.9 Theft of physical credentials

Physical credentials can be stolen or duplicated. For example, a smart card or a password lookup card can be stolen and used by an attacker.

10.3.10 Controls against theft of physical credentials

The following controls should be applied as determined necessary by a risk assessment:

a) Add an activation feature to the credential, such as entering a PIN or using a biometric;

b) Add a lock-out mechanism after a certain number of failed attempts for the activation feature;

c) Add anti-counterfeiting measures, such as holograms and microprint.

10.3.11 Password cracking

Password cracking refers to the techniques used by an attacker to obtain a victim's password. Password cracking often relies upon brute force methods, such as the use of dictionary attacks. Most password systems do not store plaintext passwords. Instead, they store the value of the hashes (or digests) of passwords. Brute force attacks rely on computational power to crack hashed passwords or other secrets secured with hashing and encryption. With dictionary attacks, an attacker uses a program to iterate through all of the words in a dictionary (or multiple dictionaries in different languages), computes the hash value for each word, and checks the resultant hash value against the database.

The use of rainbow tables is another password cracking method that is quicker than typical brute force methods. Rainbow tables are pre-computed tables of clear text/hash value pairs. Rainbow tables are quicker than brute-force attacks because they use reduction functions to decrease the search space. Once generated or obtained, rainbow tables can be used repeatedly by an attacker.

10.3.12 Controls against password cracking

The following controls should be applied as determined necessary by a risk assessment:

a) Deter brute force and rainbow table attacks by using hashed passwords with salt;

b) Adding a reverse Turing test[1] to on-line authentication protocols;

c) Use strong passwords that are complex, are not dictionary words, and contain a mixture of upper case, lower case, numeric, and special characters;

d) Enforce application of lockout policies to end-user accounts to limit the number of retry attempts that can be used to guess the password, or slow down the rate at which retries are possible after a limit is reached;

e) Disallow use of default account names and rename standard accounts, such as the administrator's account and the anonymous internet user account;

f) Maintain an audit trail of failed logins and analyze for patterns of password hacking attempts;

g) Use system and network security controls to prevent an attacker from gaining access to a system or installing malicious software.

[1] Before being allowed to perform some action on a website, the user is presented with alphanumerical characters in a distorted graphic image and asked to type them out. This is intended to prevent automated systems from abusing the site. The rationale is that software sufficiently sophisticated to read and reproduce the distorted image accurately does not exist (or is not available to the average user), so any system able to do so is likely to be a human.

10.3.13 Spoofing and masquerading

Spoofing and masquerading refer to situations in which an attacker impersonates another entity to obtain a particular result (typically geared towards gaining access to an otherwise inaccessible asset). This is done either by making use of the credential(s) of a claimant or otherwise posing as a claimant (e.g., by forging a credential).

A masquerade takes place when one claimant pretends to be a different claimant in order to successfully authenticate as the different claimant.

Examples of masquerading include:

a) Replay of authentication sequences after a valid authentication sequence by an attacker allowing him to impersonate the claimant;

b) An attacker posing as a claimant to the verifiers in order to test previously guessed credentials;

c) An attacker posing as a claimant spoofs a biometric template by creating a "gummy" finger that matches the pattern of the victim and results in a matching template;

d) An attacker posing as the CSPs to legitimate claimants in order to obtain credentials that can then be used to impersonate entities to legitimate relying parties;

e) An attacker posing as the relying party to a CSP or verifier (e.g., to obtain sensitive user information);

f) An attacker posing as a legitimate software publisher responsible for downloading on-line software applications and/or up-dates.

As indicated in the previous section, masquerading attacks are typically performed in order to allow the attacker to perform an action he would otherwise not be able to perform (e.g., gain access to a valuable resource).

Spoofing is a type of masquerading that refers to an attempt by an unauthorized entity to gain access to a system's or end-user's information by employing a fake identity thus hiding its true identity. There are many forms of spoofing, such as email and MAC address spoofing.

10.3.14 Controls against masquerading and spoofing

This particular type of threat is dynamic and variable, and the response may be different for different types of masquerading and spoofing attacks. Additionally, controls should be constantly monitored and adjusted based on the changing nature of the attacks. The following controls should be applied as determined necessary by a risk assessment:

a) To counter on-line masquerade-related threats, authentication must be used in conjunction with some form of integrity service, which binds the authenticated identity to the activity;

b) For spoofing, filter incoming packets that appear to come from an internal IP address at your perimeter;

c) For spoofing, filter outgoing packets that appear to originate from an invalid local IP address;

d) To counter the downloading of software that has been modified by unauthorized parties, add a digital signature to the code.

10.3.15 Phishing

Phishing is the fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular web sites (e.g., banking, social networking, or auction web sites) are commonly used to lure claimants. Phishing is typically carried out by e-mail, social networking, or instant messaging, and it often directs users to enter details at a fake website whose Uniform Resource Locator (URL) and "look and feel" are almost identical to the legitimate one.

10.3.16 Controls against phishing

The following controls should be applied as determined necessary by a risk assessment:

a) For both incoming and outbound messages implement Bayesian filters, IP blacklists, URL-based filters, heuristics and fingerprinting schemes specifically designed to detect phishing attacks;

b) Adopt practices such as hiding images, disabling hyperlinks from untrusted sources, and providing visual cues in email clients to identify messages from trusted sources;

c) Employ mutual authentication, also described as two-way authentication.

10.3.17 Session hijacking

Session hijacking deceives a server or a client into accepting the upstream host as the actual legitimate host. Instead, the upstream host is an attacker's host that is manipulating the network so the attacker's host appears to be the desired destination. It is a type of a man-in-the-middle attack whereby the attacker inserts himself between two communicating parties.

10.3.18 Controls against session hijacking

The following controls should be applied as determined necessary by a risk assessment:

a) Establish encrypted sessions in a way that prevents the man-in-the-middle attack;

b) Stay informed of, and implement as required, platform patches to fix TCP/IP vulnerabilities, such as predictable packet sequences;

c) Use a mutual handshake exchange based on cryptography (e.g., TLS).

11 Operational service assurance criteria

11.1 General

Specific criteria are required to provide a consistent and measurable basis for the delivery and assessment of the trusted services defined for the EAAF. Adherence to these criteria shall be the basis of assurance in entity identities which this framework supports. These service assurance criteria (SAC) shall take into account:

a) The LoAs defined in clause 6;

b) The trusted service (function) components defined in clause 7;

c) The actors involved in the authentication process as described in clause 8;

d) Management and organizational factors which uphold assurance as described in clause 9;

e) The authentication risks and threats described in clause 10.

f) The privacy protections described in appendix A.

These criteria shall set out the requirements for services, and their providers, by focusing on requirements for the following:

a) The general business and organizational conformity of services and their providers;

b) The functional conformity of identity proofing services;

c) The functional conformity of credential management services and their providers.

This clause describes criteria topics that shall be taken into consideration in the establishment of specific criteria for the delivery and assessment of the trusted services defined for the EAAF. The criteria topics are intended to cover all four defined LoAs, although in developing specific criteria the following should be taken into account:

a) The rigour required by specific criteria will likely vary according to the LoA that they are intended to support;

b) Certain criteria may be inapplicable at some LoAs, either because they are stronger than required (i.e., at a lower LoA) or are not strong enough (i.e., at a higher LoA, where they will probably be replaced by alternative criteria of greater strength having the same general intention and purpose);

c) The functional conformity of credential management services and their providers.

The application of specific criteria to the assessment of services which claim conformity to the EAAF, assessment shall require that the services comply with all applicable criteria within the SAC, at their nominated LoA (s). It is also necessary that SAC are set out such that conformity is assessed for each service, rather than only for the CSP, since assurance is derived from confidence in the functional conformity of each service.

Certain criteria will be relevant to the qualities of the CSP or to operational considerations which are commonly applied, irrespective of the specific trust service functionality being provided. It will be efficacious to define and assess these criteria only once. Other criteria will be service-type specific and therefore have a unique applicability. For this reason, criteria topics are considered under the following groupings:

a) Common organizational criteria, applicable to the organization and all trust services;

b) Identity proofing criteria;

c) Credential management criteria;

d) Credential verification criteria;

Trust framework operators which seek to comply with this Framework shall establish specific criteria fulfilling the requirements of this clause for each LoA that they intend to support and shall assess the CSPs that claim compliance with the Framework against those criteria. Likewise, CSPs shall determine the LoA at which their services comply with this framework by evaluating their overall business processes and technical mechanisms against specific criteria meeting the requirements of this clause.

11.2 Common organizational service assurance criteria

The SAC in this group establish the general business and organizational requirements for conformity of services and CSPs at all LoAs. These criteria apply to any service provision and hence shall only be used in combination with one or more other SAC groups that address the technical functionality of specific service offerings.

Criteria shall be established to address:

a) Enterprise and service maturity;

b) Legal compliance (e.g., applicable privacy and data protection laws);

c) Fiscal governance and solvency;

d) Notices and user information and agreements:

e) Information security management

f) Security-relevant event (audit) records;

g) Operational infrastructure within which the delivery of the specified service takes place;

h) External services and components to manage the relationships with and obligations upon contracted parties;

i) Secure communications.

11.3 Identity proofing service assurance criteria

The service assurance criteria in this group establish the requirements for the technical conformity of identity proofing services at all LoAs. These criteria apply to a particular kind of trust service recognized by this framework and to the related CSP — an identity proofing service for both individual identity and institutional identity credentials.

These criteria do not address the delivery of a credential to the claimant, which is dealt with by the credential management SAC described in clause 11.4.

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

a) In conjunction with the common organizational SAC described in clause 11.2, for a standalone identity proofing service;

b) In combination with one or more other SACs that shall include the common organizational SAC and where the identity proofing functions that these criteria address form part of a larger service offering.

Criteria shall be established to address:

a) Identity proofing policies:

b) Identity proofing processes, allowing for at least one of the following forms of proofing:

c) Keeping records of all the relevant facts of the verification process, whether successful or not, for the duration of the claimant's account and thereafter for whatever period of time is required by applicable legislation or contract;

d) Making available to RPs, such portions of records as permitted by applicable legislation and/or allowed for by the service definition;

11.4 Credential management service assurance criteria

The service assurance criteria in this group establish requirements for the functional conformity of credential management services and their providers at all LoAs. These criteria are generally referred to elsewhere within EAAF documentation as credential management SAC.

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

a) Credential operating environment;

b) Credential issuing;

c) Credential renewal and re-issuing;

d) Credential revocation;

e) Credential status management.

These criteria shall be used in conjunction with the common organizational SAC, and, in addition, shall either:

a) Explicitly include the criteria of the identity proofing SAC described in clause 11.3; or

b) Rely upon the criteria of the identity proofing SAC being fulfilled by the use of a previously-certified identity proofing service.

11.4.1 Credential operating environment

The criteria in this part deal with the overall operational environment in which the credential management is conducted. The credential management SAC shall be used in conjunction with the common organizational SAC described in clause11.2. In addition, they shall either explicitly include the identity proofing SAC described in clause 11.3 or rely upon those criteria being fulfilled by the use of a certified identity proofing service.

The common organizational criteria describe broad requirements. The criteria in this clause describe operational specifics. Implementation depends on the chosen LoA. The procedures and processes required to create a secure environment for management of credentials and the particular technologies that are considered strong enough to meet the assurance requirements differ considerably from LoA to LoA, thus:

a) At LoA1, these criteria apply to PINs and passwords, as well as SAML assertions;

b) At LoA2, these criteria apply to passwords, as well as acceptable SAML assertions;

c) At LoA3, these criteria apply to one-time password devices and soft crypto applications protected by passwords or biometric controls, as well as cryptographically-signed SAML assertions;

d) At LoA4, these criteria apply exclusively to cryptographic technology deployed through a Public Key Infrastructure. This technology requires hard credentials protected by password or biometric controls. No other forms of credential are permitted at LoA4.

Criteria shall be established to address:

a) Credential policy and procedures;

b) Security controls;

c) Privacy controls;

d) Storage of long-term secrets;

e) Maintaining a log of security-relevant events, capturing all key credential events;

f) Changeable PINs and passwords.

11.4.2 Credential issuing

These criteria shall deal with the verification of the identity of the claimant seeking a credential and with credential strength and credential delivery mechanisms. They shall address requirements levied by the use of various technologies to achieve the appropriate LoA.

Criteria shall be established to address:

a) Identity proofing functions;

b) Credential creation;

c) Claimant key-pair generation;

d) Credential delivery.

11.4.3 Credential renewal and re-issuing

These criteria shall apply to the renewal and re-issuing of credentials. The renewal and re-issuing processes shall comply in all practical senses with the applicable criteria set forth in sub-clause 11.4.2.

Criteria shall be established to address:

a) Permitting claimants to change their PINs/passwords;

b) Setting pre-defined validity periods and expiry dates;

c) Defining who can request a renewal/reissuance and under what circumstances;

d) Verifying the authority to request a renewal/reissuance.

11.4.4 Credential revocation

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

Criteria shall be established to address:

a) Revocation procedures;

b) Verification of the revocant's identity;

c) Requiring that a request for revocation made to the credential issuer service (function) is submitted using a secured network communication, where necessary;

d) Providing for re-keying credentials;

e) Ensuring that all revocation and re-key requests communicated between components of the service provision are communicated over a secured network.

11.4.5 Credential status management

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

Criteria shall be established to address the maintenance of the status of all credentials issued whether current or revoked/cancelled/expired.

11.5 Credential usage service assurance criteria

Criteria shall be established to address credential usage, such as:

a) Authenticating credentials, on the request of a verifier or RP, using a secure protocol;

b) Not providing bogus authentication results;

c) Only authenticating credentials which have not been revoked in response to a specific transaction time-stamp;

d) Issuing assertions with a lifetime limited to the applicable LoA, and which accounts for whether the RP shares a common domain or not.

Annex A
Privacy and protection of PII

(This annex forms an integral part of this Recommendation | International Standard)

The suitability of a particular authentication approach for a particular use will depend not only on an assessment of authentication effectiveness, but also on the risks and risk tolerance of the organizations involved. Misuse or lack of adequate protection of the PII of claimants entails significant risks for organizations, ranging from reputational damage to liability exposure. The use and protection of PII in an envisaged authentication approach, therefore, needs to be carefully weighed and considered. This section provides informative guidance relating to some of the privacy considerations organizations should take into account when deciding on the use and implementation of a particular authentication approach.

Where claimants are individuals, the majority of authentication approaches will involve processing of PII during one or more of the following processes described in this EAAF:

a) During the enrolment process when collecting, proofing, and verifying identity and other information relating to claimants;

b) During the creation, issuance, and management of credentials of claimants;

c) During the use of credentials by the claimant and their verification by relying parties and verifiers.

It is possible to have strong authentication and strong privacy. There exist many cryptographically strong authentication approaches which have limited negative impact on privacy (e.g., anonymous credentials, group signatures). Additionally, it should be noted that the increased strength of the assurance level (e.g., LoA4 versus LoA2) can, but does not necessarily need to, adversely affect the privacy of an individual. Much will depend on the chosen authentication approach and how it is implemented. In making these decisions, every organization should carefully consider the need to protect the PII of claimants, in addition to the needs of protecting their resources and holding entities accountable in case of unauthorized activities.

The majority of authentication approaches involve the use of distinguishing identifiers to unambiguously distinguish a claimant from possible claimants in the context of an authentication transaction. Use of distinguishing identifiers is often also necessary for a variety of other purposes, such as account management and the maintenance of an appropriate audit trail. The main privacy concerns relating to the use of distinguishing identifiers do not relate to the usage of a distinguishing identifier as such, but rather to the reuse of the same identifier in many different settings. For example, an account number assigned for a single purpose is generally considered to be less sensitive than a government administrative reference used for multiple purposes (e.g., taxation, healthcare, retirement). In certain jurisdictions, there may also be legislation restricting the use of certain identifiers.

In light of the previous considerations, organizations should implement effective safeguards to protect the PII of claimants in the components and processes described in this EAAF. In particular, the chosen authentication approach should be designed and implemented in a way that generally minimizes the disclosure and processing of PII. In addition, the use of distinguishing identifiers that are also used in other contexts or domains should be restricted to instances where it is necessary to use them and the laws of the relevant jurisdiction(s) allow it. Additional ISO/IEC guidance for the protection of PII can be found in two sources:

a) ISO/IEC 29100 defines privacy requirements in terms of three main factors: (1) legal and regulatory requirements for the safeguarding of the individual's privacy and the protection of his/her PII, (2) the particular business and use case requirements, and (3) individual privacy preferences of the PII principal. IS0/IEC 29100 provides basic privacy principles covering: Consent and Choice, Purpose Specification, Collection Limitation, Use, Retention and Disclosure Limitation, Data Minimization, Accuracy and Quality Openness, Transparency and Notice, Individual Participation and Access, Accountability, Security Controls, and Compliance. In addition to performing the risk assessment to analyze for threats, organizations should conduct a privacy impact assessment of their authentication approach to assess which elements of their systems will require specific attention in terms of privacy protection measures.

b) ISO/IEC 29101 provides best practice privacy reference architecture guidance for planning and building ICT system architectures to facilitate the proper handling of PII. Using this architecture can facilitate the incorporation of necessary privacy safeguarding controls into an ICT environment.

For detailed guidance on requirements, principles, and system design with regard to protection of PII, the reader is referred to the above standards.

Annex B

Bibliography

(This annex forms an integral part of this Recommendation | International Standard)

This bibliography provides a listing of non-normative references used in the development of the Framework.

[1] The National e-Authentication Framework http://www.finance.gov.au/e-government/security-and-authentication/authentication-framework.html

[2] Australian Government Gatekeeper Public key Infrastructure http://www.gatekeeper.gov.au/

[3] ITU-T Focus Group on Identity Management Report 5 Report on Requirements for Global Interoperable Identity Management http://www.itu.int/ITU-T/studygroups/com17/fgidm/

[4] ITU-T Focus Group: Report on Identity Management Report 6 Framework for Global Interoperability http://www.itu.int/ITU-T/studygroups/com17/fgidm/

[5] ITU-T Report on the Definition of the Term "Identity", April, 2008 http://www.itu.int/ITU-T/jca/idm/

[6] Liberty Alliance Identity Assurance Framework (IAF) Specification http://www.projectliberty.org/resource_center/specifications/liberty_alliance_identity_assurance_framework_iaf_1_1_specification_and_associated_read_me_first_1_0_white_paper

[7] New Zealand Standard: *Evidence of Identity (EOI)* June 2006 http://www.dia.govt.nz/diawebsite.nsf/wpg_URL/Resource-material-Evidence-of-Identity-Standard-Evidence-of-Identity-Standard-(html-version)?Open Document

[8] NIST Special Pub 800-36 Guide to Selecting Information Technology Security Products October 2003, http://csrc.nist.gov/publications/nistpubs/800-36/NIST-SP800-36.pdf

[9] NIST Special Pub 800-63 Electronic Authentication Guideline Version 1.0.2, April 2006 http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

[10] "OECD Recommendation for Electronic Authentication and OECD Guidelines for Electronic Authentication" http://www.oecd.org/dataoecd/32/45/38921342.pdf

[11] OMB M-04-04, *e-Authentication Guidance for Federal Organization* http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

[12] Principles for Electronic Authentication: A Canadian Framework, http://strategis.ic.gc.ca/epic/site/ecic-ceac.nsf/en/h_gv00240e.html

[13] B. VAN ALSENOY and D. DE COCK, 'Due processing of personal data in eGovernment? A Case Study of the Belgian electronic identity card', Datenschutz und Datensicherheit, March 2008, p. 180.

[14] A. Menezes, P. van Oorschot, S. Vanstone, 'Handbook of Applied Cryptography', 1997, p. 3-4. http://www.cacr.math.uwaterloo.ca/hac/.