International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1254

(09/2012)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cyberspace security – Identity management

Entity authentication assurance framework

Recommendation ITU-T X.1254

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	**X.1250–X.1279**
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1254

Entity authentication assurance framework

Summary

This Recommendation defines four levels of entity authentication assurance (i.e., LoA 1 – LoA 4), and the criteria and threats for each of the four levels of entity authentication assurance. Additionally, it:

- specifies a framework for managing the assurance levels;
- provides guidance concerning control technologies that are to be used to mitigate authentication threats, based on a risk assessment;
- provides guidance for mapping the four levels of assurance to other authentication assurance schemas; and
- provides guidance for exchanging the results of authentication that are based on the four levels of assurance.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.1254	2012-09-07	17

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

A similar text is published as ISO/IEC 29115. It differs from this text in four instances: 1) clause 3.1.6: the definition for credential is different and in this Recommendation references the definition in Recommendation ITU-T X.1252; 2) Table 10-1: ISO/IEC 29115 includes an example for impersonation that includes use of an identity for an entity that does not exist; 3) clause 10.2.2.1: ISO/IEC 29115 describes SSL as an example of a protected channel; 4) In this Recommendation, Annex A, *Characteristics of a credential*, is normative.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Page

Introduction

Many electronic transactions within 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.

Recommendation ITU-T X.1254 provides a framework for entity authentication assurance. Assurance within this Recommendation 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.

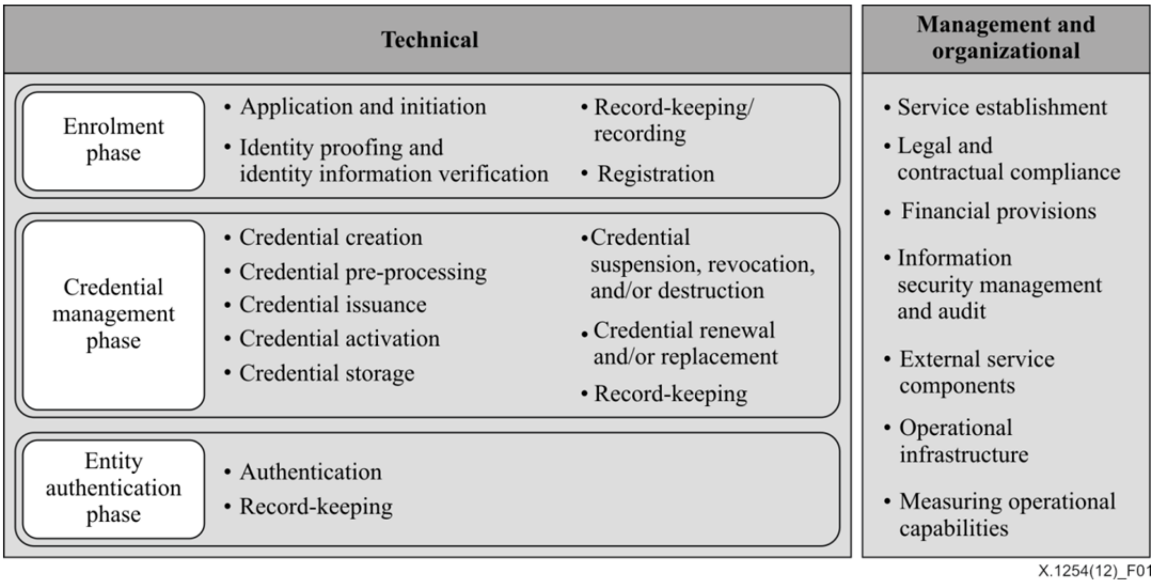
Technical
Management and organizational
Enrolment phase
• Application and initiation
• Identity proofing and identity information verification
• Record-keeping/ recording
• Registration
Credential management phase
• Credential creation
• Credential pre-processing
• Credential issuance
• Credential activation
• Credential storage
•Credential suspension, revocation, and/or destruction
• Credential renewal and/or replacement
• Record-keeping
Entity authentication phase
• Authentication
• Record-keeping
• Service establishment
• Legal and contractual compliance
• Financial provisions
• Information security management and audit
• External service components
• Operational infrastructure
• Measuring operational capabilities
X.1254(12)_F01

Figure 1 – Overview of the entity authentication assurance framework

Using four specified levels of assurance (LoAs), this Recommendation 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 an authentication transaction. Finally, this Recommendation provides guidance concerning the protection of personally identifiable information (PII) associated with the authentication process.

This Recommendation is intended to be used principally by credential service providers (CSPs) and by others having an interest in their services (e.g., relying parties, assessors and auditors of those services). This entity authentication assurance framework (EAAF) specifies the minimum technical, management and process requirements for four LoAs to ensure equivalence among the credentials issued by various CSPs. It also provides some additional management and organizational considerations that affect entity authentication assurance, but it does not set forth specific criteria for those considerations. Relying parties (RPs) and others may find this Recommendation helpful to gain an understanding of what each LoA provides. Additionally, it may be adopted for use within a trust framework to define technical requirements for LoAs. The EAAF is intended for, but not limited to, session-based and document-centric use cases using various authentication technologies. Both direct and brokered trust scenarios are possible, within either legal/bilateral arrangements or federations.

Recommendation ITU-T X.1254

Entity authentication assurance framework[1]

1 Scope

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

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 assertion [b-ITU-T X.1252]: A statement made by an entity without accompanying evidence of its validity.

NOTE – The meaning of the terms claim and assertion are generally agreed to be somewhat similar but with slightly different meanings. For the purposes of this Recommendation, an assertion is considered to be a stronger statement than a claim.

3.1.2 authentication [b-ISO/IEC 18014-2]: Provision of assurance in the identity of an entity.

3.1.3 authentication factor [b-ISO/IEC 19790]: Piece of information and/or process used to authenticate or verify the identity of an entity.

NOTE – Authentication factors are divided into four categories:

- something an entity has (e.g., device signature, passport, hardware device containing a credential, private key);
- something an entity knows (e.g., password, PIN);
- something an entity is (e.g., biometric characteristic);
- something an entity typically does (e.g., behaviour pattern).

[1] Korea (Republic of) has expressed a reservation and will not apply this Recommendation because this Recommendation is in conflict with regulations in Korea, with regard to the required four levels of entity authentication assurance and their criteria for achieving each of the four levels of entity authentication assurance.

3.1.4 claim [b-ITU-T X.1252]: To state as being the case, without being able to give proof.

NOTE – The meaning of the terms claim and assertion are generally agreed to be somewhat similar but with slightly different meanings. For the purposes of this Recommendation, an assertion is considered to be a stronger statement than a claim.

3.1.5 context [b-ITU-T X.1252]: An environment with defined boundary conditions in which entities exist and interact.

3.1.6 credential [b-ITU-T X.1252]: A set of data presented as evidence of a claimed identity and/or entitlements.

NOTE – See Appendix I for additional characteristics of a credential.

3.1.7 entity [b-ITU-T X.1252]: Something that has separate and distinct existence and that can be identified in a context.

NOTE – For the purposes of this Recommendation, entity is also used in the specific case for something that is claiming an identity.

3.1.8 identity [b-ISO/IEC 24760]: Set of attributes related to an entity.

NOTE – Within a particular context, an identity can have one or more identifiers to allow an entity to be uniquely recognized within that context.

3.1.9 multifactor authentication [b-ISO/IEC 19790]: Authentication with at least two independent authentication factors.

3.1.10 non-repudiation [b-ITU-T X.1252]: The ability to protect against denial by one of the entities involved in an action of having participated in all or part of the action.

3.1.11 repudiation [b-ITU-T X.1252]: Denial in having participated in all or part of an action by one of the entities involved.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 authentication protocol: A defined sequence of messages between an entity and a verifier that enables the verifier to perform authentication of an entity.

3.2.2 authoritative source: A repository which is recognized as being an accurate and up-to-date source of information.

3.2.3 credential service provider (CSP): A trusted actor that issues and/or manages credentials.

3.2.4 entity authentication assurance (EAA): A degree of confidence reached in the authentication process that the entity is what it is, or is expected to be (this definition is based on the 'authentication assurance' definition given in [b-ITU-T X.1252]).

NOTE – The confidence is based on the degree of confidence in the binding between the entity and the identity that is presented.

3.2.5 identifier: One or more attributes that uniquely characterize an entity in a specific context.

3.2.6 identity information verification: A process of checking identity information and credentials against issuers, data sources or other internal or external resources with respect to authenticity, validity, correctness and binding to the entity.

3.2.7 identity proofing: The process by which the registration authority (RA) captures and verifies sufficient information to identify an entity to a specified or understood level of assurance.

3.2.8 man-in-the-middle attack: An attack in which an attacker is able to read, insert and modify messages between two parties without their knowledge.

3.2.9 mutual authentication: The authentication of identities of entities which provides both entities with assurance of each other's identity.

3.2.10 phishing: A scam by which an email user is duped into revealing personal or confidential information which the scammer can then use illicitly.

3.2.11 registration authority (RA): A trusted actor that establishes and/or vouches for the identity of an entity to a credential service provider (CSP).

3.2.12 relying party (RP): Actor that relies on an identity assertion or claim.

3.2.13 salt: A non-secret, often random value that is used in a hashing process.

NOTE – It is also referred to as sand.

3.2.14 shared secret: A secret used in authentication that is known only to the entity and the verifier.

3.2.15 time stamp: This is a reliable time variant parameter which denotes a point in time with respect to a common reference.

3.2.16 transaction: A discrete event between an entity and service provider that supports a business or programmatic purpose.

3.2.17 trust framework: A set of requirements and enforcement mechanisms for parties exchanging identity information.

3.2.18 trusted third party (TTP): An authority or its agent, trusted by other actors with respect to specified activities (e.g., security-related activities).

NOTE – A trusted third party is trusted by an entity and/or a verifier for the purposes of authentication.

3.2.19 validity period: The time period during which an identity or credential may be used in one or more transactions.

3.2.20 verification: The process of checking information by comparing the provided information with previously corroborated information.

3.2.21 verifier: The actor that corroborates identity information.

NOTE – The verifier can participate in multiple phases of the EAAF and can perform credential verification and/or identity information verification.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CA	Certification Authority
CSP	Credential Service Provider
EAA	Entity Authentication Assurance
EAAF	Entity Authentication Assurance Framework
ICT	Information and Communication Technology
IdM	Identity Management
IP	Internet Protocol
LoA	Level of Assurance
LoAs	Levels of Assurance
MAC	Media Access Control
NPE	Non-Person Entity

PDA	Personal Digital Assistant
PII	Personally Identifiable Information
PIN	Personal Identification Number
RA	Registration Authority
RP	Relying Party
SAML	Security Assertion Markup Language
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
TPM	Trusted Platform Module
TTP	Trusted Third Party
URL	Uniform Resource Locator

5 Conventions

This Recommendation applies the following 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 a capability.

6 Levels of assurance

This entity authentication assurance framework (EAAF) defines four levels of assurance (LoA) for entity authentication. Each LoA describes the degree of confidence in the processes leading up to and including the authentication process itself, thus providing assurance that the entity that uses a particular identity is in fact the entity to which that identity was assigned. For the purposes of this Recommendation, an LoA is a function of the processes, management activities and technical controls that have been implemented by a credential service provider (CSP) for each of the EAAF phases based on the criteria set forth in clause 10. Entity authentication assurance (EAA) is affected by management and organizational considerations, but this Recommendation does not provide explicit normative criteria for these considerations. An entity can be a human or a non-person entity (NPE).

For example, a network's LoA could be a function of the LoAs of all components that make up the network and includes NPEs or endpoint devices (e.g., mobile phones, personal digital assistants (PDAs), set-top boxes, laptops). In some instances, endpoint devices may impersonate legitimate entities. Consequently, the ability to distinguish a trusted device, with some degree of confidence, from a rogue device is fundamental to EAA.

LoA1 is the lowest level of assurance, and LoA4 is the highest level of assurance specified in this Recommendation. Determining which LoA is appropriate in a given situation depends on a variety of factors. The determination of the required LoA is based mainly on risk: the consequences of an authentication error and/or misuse of credentials, the resultant harm and impact, and their likelihood of occurrence. Higher LoAs shall be used for higher perceived risk.

The EAAF provides requirements and implementation guidance for each of the four LoAs. In particular, it provides requirements for the implementation of processes for the following phases:

a) enrolment (e.g., identity proofing, identity information verification, registration)

b) credential management (e.g., credential issuance, credential activation)

c) authentication.

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

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

Table 6-1 – Levels of assurance[2]

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

This framework contains requirements to achieve a desired LoA for each entity authentication assurance framework phase. The overall LoA achieved by an implementation using this framework will be the level of the phase with the lowest LoA.

6.1 Level of assurance 1 (LoA1)

At LoA1, there is minimal confidence in the claimed or asserted identity of the entity, but some confidence that the entity is the same over consecutive authentication events. This LoA is used when minimum risk is associated with erroneous authentication. There is no specific requirement for the authentication mechanism used; only that it provides some minimal assurance. A wide range of available technologies, including the credentials associated with higher LoAs, can satisfy the entity authentication assurance requirements for this LoA. This level does not require use of cryptographic authentication methods (e.g., cryptographic-based challenge-response protocol).

For example, LoA1 may be applicable for authentication in which an entity presents a self-registered username or password to a service provider's website to create a customized page, or transactions involving websites that require registration for access to materials and documentation, such as news or product documentation.

For example, at LoA1, a media access control (MAC) address may satisfy a device authentication requirement. However, there is little confidence that another device will not be able to use the same MAC address.

6.2 Level of assurance 2 (LoA2)

At LoA2, there is some confidence in the claimed or asserted identity of the entity. This LoA is used when moderate risk is associated with erroneous authentication. Single-factor authentication is acceptable. Successful authentication shall be dependent upon the entity proving, through a secure authentication protocol, that the entity has control of the credential. Controls should be in place to reduce the effectiveness of eavesdroppers and online guessing attacks. Controls shall be in place to protect against attacks on stored credentials.

For example, a service provider might operate a website that enables its customers to change their address of record. The transaction in which a beneficiary changes an address of record may be considered an LoA2 authentication transaction, as the transaction may involve a moderate risk of inconvenience. Since official notices regarding payment amounts, account status, and records of

[2] LoA is a function of the processes, management activities, and technical controls that have been implemented by a CSP for each of the EAAF phases based on the criteria set forth in clause 10.

changes are usually sent to the beneficiary's address of record, the transaction additionally entails moderate risk of unauthorized release of PII. As a result, the service provider should obtain at least some authentication assurance before allowing this transaction to take place.

6.3 Level of assurance 3 (LoA3)

At LoA3, there is high confidence in the claimed or asserted identity of the entity. This LoA is used where substantial risk is associated with erroneous authentication. This LoA shall employ multifactor authentication. Any secret information exchanged in authentication protocols shall be cryptographically protected in transit and at rest (although LoA3 does not require the use of a cryptographic-based challenge-response protocol). There are no requirements concerning the generation or storage of credentials; they may be stored or generated in general purpose computers or in special purpose hardware.

For example, a transaction in which a company submits certain confidential information electronically to a government agency may require an LoA3 authentication transaction. Improper disclosure could result in a substantial risk for financial loss. Other LoA3 transaction examples include online access to accounts that allow the entity to perform certain financial transactions, 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)

At LoA4, there is very high confidence in the claimed or asserted identity of the entity. This LoA is used when high risk is associated with erroneous authentication. LoA4 provides the highest level of entity authentication assurance defined by this Recommendation. LoA4 is similar to LoA3, but it adds the requirements of in-person identity proofing for human entities and the use of tamper-resistant hardware devices for the storage of all secret or private cryptographic keys. Additionally, all PII and other sensitive data included in authentication protocols shall be cryptographically protected in transit and at rest.

For example, services where there is a potential high risk for harm or distress in the case of an authentication failure may require LoA4 protection. The responsible party needs full assurance that the correct entity provided certain critical information, and the responsible party may even be criminally liable for any failure to verify the information. Finally, approval of a transaction involving high risk of financial loss may be an LoA4 transaction.

At LoA4, digital certificates (e.g., ITU-T X.509, card-verifier (CV) certificates) may be used to authenticate NPEs, such as laptops, mobile phones, printers, fax machines and other devices connected to a network. For example, the smartphone enrolment process may require the deployment of digital certificates to the smartphone. Also, in order to prevent unauthorized access to the power grid, digital certificates may be used in the deployment of smart meter technologies.

6.5 Selecting the appropriate level of assurance

Selection of the appropriate LoA should be based on a risk assessment of the transactions or services for which the entities will be authenticated. 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. Table 6-2 indicates possible consequences and impacts of authentication failure at the various LoAs.

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

Possible consequences of authentication failure	Potential impact of authentication failure by LoA			
	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 organization, 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 Mod	Sub High
Civil or criminal violations	N/A	Min	Sub	High
* Min=Minimum; Mod=Moderate; Sub=Substantial; High=High.				

Determination of what constitutes minimum, moderate, substantial, and high risk depends on the risk criteria defined by the organization using this Recommendation for each of the possible consequences. Additionally, it is possible to have multiple impact scenarios (e.g., consequences could include harm to the organization, as well as, unauthorized release of sensitive information). In multiple impact scenarios, the highest LoA corresponding to the consequences should be used.

Each LoA shall be determined by the strength and rigour of the controls and processes for each phase of the EAAF that the CSP applies to the provision of its service. The EAAF establishes a need for operational service assurance criteria at each LoA for CSPs. Service assurance criteria are introduced in clause 11, but specific requirements are out of scope for this Recommendation.

There may be other business related factors to take into account, beyond the scope of security, when using the results of the risk assessment to determine the applicable LoA. Such business factors may include:

a) the organization's approach to managing residual risk;

b) the organization's appetite for accepting risk in terms of the impacts shown in Table 6-2;

c) the business objectives for the service (e.g., a service with the business objective of driving uptake may be better served by a lower LoA using a credential such as a password, if the organization has processes in place to mitigate fraud and is comfortable accepting the risk of fraud).

The risk assessment of a transaction may be conducted as a part of an organization's overall information security risk assessment (e.g., ISO/IEC 27001) and should focus on the specific need for security in the transactions being contemplated. The risk assessment shall address risk related to EAA. The results of the risk assessment shall be compared to the four LoAs. The LoA that best matches the results of the risk assessment shall be selected.

Where multiple classes of transactions are envisaged, it is possible that a different LoA applies to each transaction or to groups of transactions. In other words, multiple LoAs may be accepted by a single organization, according to the specific transaction in question.

6.6 LoA mapping and interoperability

Different domains may define LoAs differently. These LoAs will not necessarily support a one-to-one mapping to the four LoAs described in this framework. For example, one domain may adopt a four-level model, and another domain may adopt a five-level model. 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 domain shall explain how its mapping scheme relates to the LoAs defined in this Recommendation by:

a) developing a well-defined entity authentication assurance methodology, including well defined categories of LoAs; and

b) widely publishing this methodology so that organizations wishing to enter into federation-type agreements with them can clearly understand each other's processes and terminology.

The LoA methodology shall take into account and clearly define LoAs in terms of a risk assessment that specifies and quantifies:

a) expected threats;

b) impacts (i.e., min, mod) should threats 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, such as specifying a credential to be carried on a hardware device (e.g., smart card) or specifying requirements for the generation and storage of credentials;

e) criteria for determining the equivalence of different combinations of authentication factors taking into account both identity proofing and associated credentials.

One approach to address the issue of mapping/bridging between different LoA models may be to use the four-level model defined in this document and map other n-level models against it. This method would allow identity federations using different models for authentication assurance to map against the four-level model. Mappings shall define how un-mapped LoAs will 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 beforehand).

6.7 Exchanging authentication results based on the 4 LoAs

Actors participating in an authentication transaction (e.g., CSPs, RPs) may need to exchange information to complete the transaction or activity.

The range of actions includes, but is not limited to, the following:

a) allowing an RP to express its expectations for the LoA at which an entity should be authenticated;

b) allowing an entity or CSP to indicate the actual LoA in its responses;

c) allowing an entity or CSP to advertise those LoAs for which it has been certified capable of meeting the requirements associated with that LoA.

Actors participating in an authentication transaction shall agree on the protocol, semantics, format and structure of the information to be exchanged. The RP may need to specify if it will accept any authentication response other than that exactly requested.

While digital certificates are an established way to convey information concerning the assurance of related credentials, metadata is increasingly being used as a method to communicate what assurance requirements the exchanging parties have. A 'Context Class', such as a 'Security Assertion Markup Language (SAML) Authentication Context Class' in the form of a uniform resource locator (URL), is a well-known mechanism for parties to express those classes concerning authentication assurance in authentication requests and assertions. For example, a typical assertion from an identity provider might convey information such as "This user is John Doe; he has an email address of john.doe@example.com, and he was authenticated into this system using a password mechanism."

The remainder of this framework addresses the structure within which processes and requirements for services are established and the threats and impacts relating to entity authentication. It concludes with an overview of the need for service assurance criteria against which services may be assessed to ensure that the appropriate LoA is assigned to achieve adequate credential services.

7 Actors

The actors involved in the EAAF include entities, CSPs, RAs, RPs, verifiers and TTPs. These actors may belong to a single organization or separate organizations. There may be a variety of relationships and capabilities provided by a number of organizations including shared or interacting components, systems and services.

7.1 Entity

An entity can have its identity authenticated. The ability to authenticate an entity depends on a number of factors. In the context of this framework, the ability to authenticate an entity implies that the entity has been registered and issued the appropriate credentials by a CSP and that an authentication protocol has been specified. During authentication, the entity may attest to its own identity. It is also possible that there is a separate party representing the entity for the purposes of authentication.

7.2 Credential service provider

A credential service provider (CSP) issues and/or manages credentials or the hardware, software and associated data that can be used to produce credentials. Passwords and biometric data are examples of a credential that may be issued and managed by a CSP. Smart cards containing private keys are an example of hardware and associated data (that can be used to produce credentials) that may be issued and managed by a CSP. A CSP may also issue and manage data that can be used to authenticate credentials. If passwords are used as credentials, this data may be the values of one-way functions of the passwords. If credentials are based on digitally-signed information, CSPs may produce public key certificates that can be used by verifiers. The credentials that are issued and supported, as well as the safeguards that are implemented by the CSP, are key factors in determining which LoA will be reached during a particular authentication transaction (see also clause 10.3).

Every entity shall be issued one or more credentials, or the means to produce credentials, to enable later authentication. Credentials, or the means to produce credentials, are typically only issued after successful completion of an enrolment process, at the end of which the entity is registered.

7.3 Registration authority

A Registration Authority (RA) establishes and/or vouches for the identity of an entity to a CSP. The RA shall be trusted by the CSP to execute the processes related to the enrolment phase and register entities in a way that allows later assignment of credentials by the CSP.

Each RA shall perform some form of identity proofing and identity information verification according to a specified procedure. In order to differentiate the entity from other entities, an entity is typically assigned one or more identifiers, which will allow the entity to be recognized later in the applicable context.

7.4 Relying party

An RP is an actor that relies on an identity claim or assertion. The relying party may require an authenticated identity for a variety of purposes, such as account management, access control, authorization decisions, etc. The relying party may itself perform the operations necessary to authenticate the entity, or it may entrust these operations to a third party.

7.5 Verifier

The verifier is an actor that corroborates identity information. The verifier can participate in multiple phases of EAA and can perform credential verification and/or identity information verification.

7.6 Trusted third party

A TTP is an authority or its agent, trusted by other actors with respect to certain activities (e.g., security-related activities). For this framework, a TTP is trusted by an entity and/or a verifier for the purposes of authentication. Examples of TTPs for the purposes of entity authentication include certification authorities (CAs) and time-stamping authorities.

8 Entity authentication assurance framework phases

This clause provides a description of the phases and processes of EAA. Although some EAA models may differ from the structure of this model, conformance to this model requires that functional capabilities fully meet the requirements set out in this framework. This framework is technology neutral.

Organizations adopting this framework shall establish policies, procedures and capabilities that provide the necessary supporting processes and fulfil requirements set forth in this framework. These will vary according to the role chosen by a particular organization and, for instance, the LoAs at which an organization provides credentials. For example, an organization may be subject to:

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

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

c) policies, actions and capabilities necessary to establish the trustworthiness of the processes, services and capabilities provided by organizations adopting the framework.

8.1 Enrolment phase

The enrolment phase consists of four processes: application and initiation, identity proofing, identity verification, and record-keeping/recording. 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 differ according to the rigour required by the applicable LoA. In the case of an entity enrolling under LoA1, these processes are 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 may be extensive. For example, enrolment at LoA4 requires an in-person meeting between the entity and the RA, as well as extensive identity proofing.

8.1.1 Application and initiation

The enrolment phase is initiated in a variety of ways. For instance, it may be initiated pursuant to a request made by entities seeking to obtain a particular credential themselves (e.g., when a new user of a website wishes to obtain a username and password). It is equally possible that the enrolment process is initiated by a third party on behalf of the entity or by the CSP itself (e.g., government-issued identification card, employee badge). For example, at higher LoAs, applications may be accepted only where the entity has been sponsored by a third party.

In any event, the initiation process of the enrolment phase for humans may involve the completion of an application form. This form should record sufficient information to ensure the entity may be identified uniquely within a context (e.g., by recording the full name, date and place of birth). For NPEs, such as a mobile device, enrolment may require initialization through the deployment of credentials to the device, which enables the device to be identified uniquely and to receive tailored device settings via an encrypted configuration profile.

CSPs shall set forth the terms under which enrolment is provided and under which the services associated with that enrolment shall be used. The terms of services associated with the enrolment may be established pursuant to a trust framework. Where appropriate, liability disclaimers or other legal provisions shall be accepted by, or on behalf of, the entity prior to continuation of the enrolment processes.

8.1.2 Identity proofing and identity information verification

Identity proofing is the process of capturing and verifying sufficient information to identify an entity to a specified or understood level of assurance. Identity information verification is the process of checking identity information and credentials against issuers, data sources or other internal or external resources with respect to authenticity, validity, correctness and binding to the entity. Depending on the context, a variety of identity information (e.g., government identity cards, driver's licences, biometric information, machine-based attestation, birth certificates) issued or approved by authoritative sources may fulfil identity proofing requirements. The actual identity information presented to fulfil identity proofing requirements varies with the LoA.

Identity proofing may include the physical checking of presented identity documents to detect possible fraud, tampering or counterfeiting. Identity proofing may also include checking to ensure the identity is used in other contexts (i.e., verified from other RAs). The identity proofing requirements shall be more stringent the higher the LoA. Also, the identity proofing process shall be more stringent for entities asserting or claiming an identity remotely (e.g., via an online channel) than locally (e.g., in person with the RA).

The stringency of identity proofing requirements is based on the objectives that must be met for each LoA. At LoA1, the only objective is to ensure the identity is unique within the intended context. The identity should not be associated with two different entities. At LoA2, there are two objectives. First, the identity shall be unique in the context. Second, the entity to which the identity pertains shall exist objectively, which means the identity is not fictitious or intentionally fabricated for fraudulent purposes.[3] For example, human identity proofing at LoA2 may include checking birth and death registers to ensure some provenance (although it does not prove that the entity in possession of a birth certificate is the entity to which the birth certificate relates). Similarly, identity proofing at LoA2 for NPEs may include checking a serial number with the manufacturer.

LoA3 includes the objectives of LoA1 and LoA2, as well as the objective of verifying the identity information through one or more authoritative sources, such as an external database. Identity information verification shows that the identity is in use and links to the entity. However, there is no assurance that identity information is in the possession of the real or rightful owner of the identity. For humans, LoA4 adds one additional objective to LoA3 by requiring entities to be witnessed in person to help protect against impersonation.

Identity proofing processes at a higher LoA shall include the processes of the lower LoAs. For example, LoA3 identity proofing assumes that LoA1 and LoA2 identity proofing controls have been satisfied.

[3] This does not preclude the use of pseudonyms.

Table 8-1 – Applying identity proofing objectives to the LoAs

LoA	Description	Objective	Controls	Method of processing[4]
LoA1 – low	Little or no confidence in the claimed or asserted identity	Identity is unique within a context	Self-claimed or self-asserted	Local or remote
LoA2 – medium	Some confidence in the claimed or asserted identity	Identity is unique within context and the entity to which the identity pertains exists objectively	Proof of identity through use of identity information from an authoritative source	Local or remote
LoA3 – high	High confidence in the claimed or asserted identity	Identity is unique within context, entity to which the identity pertains exists objectively, identity is verified, and identity is used in other contexts	Proof of identity through use of identity information from an authoritative source + identity information verification	Local or remote
LoA4 – very high	Very high confidence in the claimed or asserted identity	Identity is unique within context, entity to which the identity pertains exists objectively, identity is verified, and identity is used in other contexts	Proof of identity through use of identity information from multiple authoritative sources + identity information verification + entity witnessed in person[5]	Local only

Required LOA controls to protect against threats to enrolment shall be determined by the use of controls listed in clause 10.1.2.

Any implementation of the EAAF relies on (a subset of) the identity information and sources that are available to prospective entities and/or to the RA.

The reliability and accuracy of these credentials, identity information and sources determine the actual assurance provided by the enrolment phase. Consequently, implementers of the EAAF shall carefully consider the assurance provided by the identity (management) infrastructures that are used by the different sources and issuers when deciding which credentials, identity information and/or sources to rely on for identity proofing and identity information verification purposes. Any implementation of the EAAF shall involve the publication of a document (e.g., identity proofing policy as described in clause 10.1.2.1) which provides an overview of the identity information, sources and/or issuers that are relied upon in support of the enrolment phase.

[4] Remote identity proofing is accomplished over a network and therefore involves not being able to physically see the entity whereas local identity proofing is accomplished in a manner that requires physically seeing the entity.

[5] The witnessed in-person control applies only to human entities.

8.1.3 Record-keeping/recording

This is the process of concluding the enrolment of an entity. It is the record-keeping process of the enrolment phase in which a record of the enrolment is created. This record shall include the information and documentation that was collected (and may be retained), information about the identity information 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.

8.1.4 Registration

Registration is a process in which an entity requests to use a service or resource. Although the registration process is generally considered as a part of an enrolment process, such that it is performed at the end of the enrolment phase, it may also be performed at a later time. Unlike other processes in enrolment that are likely to be necessary only once, registration may be necessary when an entity requests access to each service or resource for the first time.

8.2 Credential management phase

The credential management phase comprises all processes relevant to the lifecycle management of a credential, or the means to produce credentials, which enables the user to participate in an activity or context. The credential management phase may involve some or all of the following processes: creation of credentials, issuance of credentials or of the means to produce credentials, activation of credentials or the means to produce credentials, storage of credentials, revocation and/or destruction of credentials or of the means to produce credentials, renewal and/or replacement of credentials or the means to produce credentials, and record-keeping. Some of these processes depend on whether the credential is carried on a hardware device.

8.2.1 Credential creation

The credential creation process encompasses all necessary processes to create a credential, or the means to produce a credential, for the first time. These processes may include pre-processing, initialization, and binding.

8.2.1.1 Credential pre-processing

Some credentials, or the means to produce credentials, require pre-processing before issuance, such as personalization where a credential is customized to the entity's identity. Personalization can take many different forms depending on the credential. For instance, the personalization of a smart card that holds credentials may involve printing (on the outside of the card) or writing (to the card's chip) the name of the entity to which the card will be issued. There are also credentials that do not require personalization, such as passwords.

8.2.1.2 Credential initialization

Credential initialization encompasses all steps to ensure that a means to produce a credential will later be able to support the functionalities that it is expected to support. For instance, a smart card chip might be required to calculate the cryptographic key pairs necessary to later support the generation of digital signatures. Similarly, a smart card might be issued in a "locked" state that requires a PIN during the activation process.

8.2.1.3 Credential binding

Binding is the process of establishing an association between a credential, or the means to produce a credential, and the entity to which it will be issued. How binding is accomplished and the confidence in the binding association varies with the LoA. For instance, in an online scenario when binding an entity's persistent pseudonymous identifier to the entity's customer record, a first time "activation code" may be carried through the binding process in a session-only encrypted cookie over a secured channel. Alternatively, the activation code may be requested at the end of the process once the entity-to-persistent identifier binding step has been completed, in order to bind the persistent identifier to the customer record.

8.2.2 Credential issuance

Credential issuance is the process of providing or otherwise associating an entity with a particular credential, or the means to produce a credential. The complexity of this process varies with the LoA required. Higher LoAs, will require secure delivery of a hardware device (e.g., a smart card) that holds a credential and may require in-person delivery of the device. In the case of lower LoAs, the issuance process might be as simple as sending a password or PIN to the entity's physical or email address.

For NPEs, such as devices, issuance processes at higher LoAs typically begin when the device manufacturer orders digital certificates in bulk, by providing a CSP with a list of unique device identification numbers for each of the digital certificates. The CSP responds by providing certificates and private keys to the manufacturer in an encrypted format. During the manufacturing process, the manufacturer may embed a digital certificate into each device, which creates a unique device identifier.

8.2.3 Credential activation

Credential activation is the process whereby a credential, or the means to produce credentials, is made ready for use. The activation process may involve a variety of measures depending on the credential. For instance, a credential, or the means to produce credentials, may have been "locked" after its initialization until the moment of issuance to the entity to prevent interim misuse. In such cases, activation may involve the "unlocking" of the credential (e.g., use of a password). A credential, or the means to produce credentials, can also be re-activated after a suspension where its validity has been temporarily stopped.

8.2.4 Credential storage

Credential storage is the process whereby credentials, or the means to produce credentials, are securely stored in a way that protects against their unauthorized disclosure, use, modification or destruction. Credential storage involves the entity associated with a credential and actions required to prevent the unauthorized use of a credential.

Credential storage does not necessarily include protection of information used to check that a credential is legitimate, if that information is not part of the credential. The protection of information, such as tables of hashed passwords required for authentication, is required at higher LoAs.

8.2.5 Credential suspension, revocation and/or destruction

Revocation is the process whereby the validity of a credential is permanently ended. Suspension is a related process whereby the validity of a credential is temporarily stopped. Revocation may be appropriate in many different instances. Revocation shall occur in the following instances:

a) a credential, or a means to produce a credential, has been reported lost, stolen or otherwise compromised;

b) a credential has expired;

c) the basis for a credential no longer exists (e.g., when an employee leaves her employer);

d) a credential has been used for unauthorized purposes; or

e) a different credential has been issued to replace the credential in question.

The time frame between notice of an event requiring revocation and the completion of the revocation process is determined by organizational policy. At higher LoAs, the time period permitted for revocation is usually shorter. Some credentials, such as those held on smart cards, can be physically destroyed upon revocation. However, the information associated with the credential cannot always be destroyed.

8.2.6 Credential renewal and/or replacement

Renewal is the process whereby the life of an existing credential is extended. Replacement is the process whereby an entity is issued a new credential, or a means to produce a credential, to replace a previously issued credential that has been revoked. An example of a replacement credential is when a CSP sends a temporary password to the entity's email address that enables the entity to create a new password after providing the temporary password. Another example is a PIN unlock code, which should be treated as if it were a PIN. The rigorousness of the processes for the renewal and replacement of credentials varies according to the LoA.

8.2.7 Record-keeping

Appropriate records shall be maintained throughout the lifecycle of a credential. At a minimum, records shall be kept to document the following information:

a) the fact that a credential has been created

b) the identifier of the credential (where applicable)

c) the entity to which the credential has been issued (where applicable)

d) the status of the credential (where applicable).

Records shall be kept for every (applicable) process involved in the credential management phase. Where credentials are issued to human entities, the keeping of records is likely to involve the processing of PII. See Appendix I.

8.3 Entity authentication phase

In the entity authentication phase, the entity uses its credential to attest its identity to an RP. The authentication process is concerned solely with the establishment (or not) of confidence in the claim or assertion of identity, and it has no bearing on, or relationship with, the actions the relying party may choose to take based upon the claim or assertion.

8.3.1 Authentication

The authentication process includes the use of a protocol to demonstrate possession and/or control of a credential in order to establish confidence in an identity. Authentication protocol requirements vary depending on the applicable LoA. For example, for a lower LoA, authentication may involve use of a password. At higher LoAs, authentication may involve using a cryptographic-based challenge-response protocol. Multifactor authentication is required at higher LoAs. Not all authentication factors provide the same strength, and multiple factors are used to increase assurance. See clause 10.

8.3.2 Record-keeping

Monitoring and record-keeping of events in the authentication phase may be necessary for a variety of purposes, such as service provision, compliance, accountability and/or legal requirements.

Where human entities are concerned, the information contained in these records may include sensitive information. These records shall be managed in a manner that takes into account the need for protection and minimization of PII. See also Appendix I.

9 Management and organizational considerations

EAA does not come from technical factors alone, but also from regulations, contractual agreements and consideration of how the service provision is managed and organized. A technically rigorous solution without competent management and operation can fall short of its potential for providing security in the provision of EAA.

This clause is informative and describes organizational and management considerations that affect EAA. It does not provide specific criteria for each LoA. Specific criteria and conformance assessment for management and organizational considerations are outside of the scope of this Recommendation, but should be provided within a trust framework.

9.1 Service establishment

Service establishment addresses both the legal status of the service provider and the status of the functional service provision. For instance, 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).

Although the basic requirements are the same for all LoAs, the higher LoAs should have greater dependency on the service provision being complete and reliable. For instance, at LoA3 and above, greater assurance about the service provision should 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 should understand and comply with any legal requirements incumbent on them in connection with the operation and delivery of the service. This has implications including, but not limited to, the types of information that may be sought, how identity proofing is conducted, and what information may be retained. Handling of PII is a particular legal concern (see Annex A). Account should be taken of all jurisdictions within which actors operate. At LoA2 and higher, specific policy and contractual requirements should also be identified.

9.3 Financial provisions

Where long-term availability of services is a consideration in both an entity's and relying parties' expectations, financial stability should be shown as 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 should address such needs.

9.4 Information security management and audit

At LoA2 and higher, EAAF actors should have in place documented information security management practices, policies, approaches to risk management and other recognized controls, so as to provide assurance that effective practices are in place. For LoA3 and above, a formal information security management system (e.g., [b-ISO/IEC 27000]) should be used.

Depending on the agreements for legal, contractual, and technical compliance, actors should ensure that parties are abiding by their commitments and may provide an avenue for redress in the event that they are not. At LoA2 and higher, this assurance should be supported by security audits, both internal and external, and the secure retention of records of significant events, including those audits. An audit can be used to check that parties' practices are in line with what has been agreed. Dispute resolution services may be used for disagreements.

9.5 External service components

When an organization is dependent upon third parties for parts of its service, how it directs the actions of these parties and oversees them will contribute to the overall assurance of the service provision. The nature and extent of the arrangements should be proportional to the required LoA and to the information security management system being applied. At LoA1, such assurance should have minimal effect, but from LoA2 and up, these measures contribute to the overall assurance being given.

9.6 Operational infrastructure

To enable large-scale networks of trust, a trust framework may be used. In a trust framework, the actors support the information flow between one another. Depending on the agreements, additional actors may be called on to ensure that all actors are abiding by commitments and may provide an avenue for redress in the event that they are not.

9.7 Measuring operational capabilities

Policy makers set out the technical and contractual requirements for trust frameworks. Technical requirements might include, for example, product version levels, system configuration, settings and protocols, while contractual requirements might be geared towards fair information practices. As they establish these requirements, policy makers should include criteria by which potential trust framework entities can be measured. Rather than developing the criteria themselves, policy makers may wish to draw on standard criteria that experts have already elaborated, such as this Recommendation. The more policy makers use standard criteria across different trust frameworks, the easier it will be for entities to understand and apply the criteria consistently. Moreover, named sets of criteria can serve as shorthand to indicate different degrees or types of rigour in requirements or capabilities at various LoAs.

10 Threats and controls

This clause describes threats to each phase of the EAAF and provides required controls for each LoA.

10.1 Threats to, and controls for, the enrolment phase

10.1.1 Enrolment phase threats

Table 10-1 identifies and describes threats to the enrolment phase.

Table 10-1 – Threats to the enrolment phase

Threat	Examples
Impersonation	Some examples of impersonation are when an entity illegitimately uses another entity's identity information, and when a device registers with a network using a spoofed media access control (MAC) address.

10.1.2 Required LoA controls to protect against enrolment phase threats

Table 10-2 identifies the required controls for the enrolment phase according to LoA.

Table 10-2 – Enrolment phase controls for each LoA

Threats	Controls	Required controls			
		LoA1	LoA2	LoA3	LoA4
Impersonation	IdentityProofing: PolicyAdherence	#1	#1	#1	#1
	IdentityProofing: In Person	╱	╱	╱	#2
	IdentityProofing: AuthoritativeInformation	#3	#4	#5	#6

NOTE – In the above table, the identifiers #1 – #6 correspond to the specific controls required to provide protection at each LoA. Each of these controls is described in detail in clause 10.1.2.1. Boxes in the table with a diagonal line indicate that the respective control is not applicable at the indicated LoA.

10.1.2.1 Controls against enrolment phase threats

The following controls against enrolment phase threats correspond to #1 – #6 listed in Table 10-2.

IdentityProofing: PolicyAdherence

#1. Publish the identity proofing policy, and perform all identity proofing in accordance with the published identity proofing policy.

IdentityProofing: In Person

#2. In-person identity proofing shall be used for humans.

IdentityProofing: AuthoritativeInformation

#3. Identity information may be self-claimed or self-asserted.

#4. The following controls apply:

- all controls from #3.

  In addition:

- The entity shall provide identity information from at least one policy-compliant authoritative source of identity information.

  a) For humans

i) In person:

- Ensure that the entity is in possession of an identification document from at least one policy-compliant authoritative source that bears a photographic image of the holder that matches the appearance of the entity; and
- ensure that the presented identification document appears to be a genuine document, properly issued and valid at the time of application.

ii) Not in person:

- The entity shall provide evidence that he/she is in possession of policy-compliant, personal identity information. (Examples of acceptable identity information might include a driver's licence or a passport); and
- the existence and validity of the evidence provided shall be confirmed in accordance with policy requirements.

b) For NPEs:

- Record information from an authoritative source of identity information, such as common name, description, serial number, MAC address, owner, location, manufacturer, etc.

#5. The following controls apply:

- all controls from #4.

In addition:

a) For humans

i) In person:

- Verify the accuracy of contact information listed in the identification document by using it to contact the entity.
- Verify at least one identification document (e.g., document attesting to birth, marriage or immigration) against registers of the relevant authoritative source.
- Corroborate personal information against applicable authoritative information sources and (where possible) sources from other contexts, which are sufficient to ensure a unique identity; and
- verify information previously provided by, or likely to be known only by, the entity.

ii) Not in person:

- Ensure check by a trusted third party of the entity's assertion/claim to the current possession of an LoA3 (or higher) credential from an authoritative source; and/or
- verify information previously provided by, or likely to be known only by, the entity.

b) For NPEs:

– Trusted hardware (e.g., TPM) shall be used at LoA3.

– For NPEs already in use, the NPE shall be physically enrolled with a device RA using an LoA3 human-issued credential. Where trusted hardware is used, it should be enabled.

- NPEs not yet procured shall be ordered using LoA3 human authentication or digital signatures to confirm that the ordering entity is authorized to order the NPE. The manufacturer's RA shall register the NPE, enable any trusted hardware and control the issuance and personalization of the NPE. Trusted hardware will be initialized on connection to the network;
- For NPEs other than computers, the binding between the device, the owner, the network or communication carrier and the RA shall be cryptographically secured in a similar manner to a trusted hardware computer; and
- where software is used, the code shall be digitally signed with an LoA3, human-issued credential before issuance and shall be counter-signed by the RA as proof of acceptance before being taken into use.

#6. The following controls apply:

- all controls from #5.

  In addition:

  a) For humans

  - The entity shall provide identity information from at least one additional policy-compliant authoritative source.

  b) For NPEs:

  - Additional devices connected to a computer, smartphone or similar processor shall be recorded at issuance and cryptographically bound to the anchor device (e.g., trusted hardware enabled device, biometric reader, smart cards, GPS geo-authenticator).
  - Any changes in the binding arrangements between devices shall be managed through the RA. Where possible, the network management capability should alert the RA or network management of any changes in device relationships and any corrective action taken.
  - Capability shall be in place to prevent any altered device relationships from working; and
  - a LoA4 software code shall be digitally signed with an LoA4, human-issued credential and shall be counter-signed by the RA as proof of acceptance before being taken into use.

10.2 Threats to, and controls for, the credential management phase

10.2.1 Credential management threats

Table 10-3 lists threats to the credential management phase.

Table 10-3 – Credential management threats

Threat	Examples
CredentialCreation: Tampering	An attacker alters information as it passes from the enrolment process to the credential creation process.
CredentialCreation: UnauthorizedCreation	An attacker causes a CSP to create a credential based on a fictitious entity.
CredentialIssuance: Disclosure	A credential created by the CSP for an entity is copied by an attacker as it is transported from the CSP to the entity during credential establishment.

Table 10-3 – Credential management threats

Threat	Examples
CredentialActivation: Unauthorized Possession	An attacker obtains a credential that does not belong to him/her, and by masquerading as the rightful entity, causes the CSP to activate the credential.
CredentialActivation: Unavailability	1. The entity associated with a credential, or the means to generate the credential, is not in the usual location and is unable to adequately authenticate its identity to the CSP. 2. Delivery of a credential, or the means to generate the credential, is delayed, and activation within the prescribed period is not possible.
CredentialStorage: Disclosure	Credentials stored in a system file are revealed. For example, a stored record of usernames and passwords is accessed by an attacker.
CredentialStorage: Tampering	The file that maps usernames to credentials is compromised so that the mappings are modified, and existing credentials are replaced by credentials to which the attacker has access.
CredentialStorage: Duplication	An attacker uses stored information to create a duplicate credential (e.g., by duplicating a smart card that can generate the credential) that can be used by an unauthorized entity.
CredentialStorage: DisclosureByEntity	The entity keeps a written record of the username and password in a place that can be accessed by others.
CredentialRevocation: DelayedRevocation	The dissemination of revocation information is not timely leading to a threat of entities with revoked credentials still being able to authenticate before the credential verifier updates the latest revocation information.
CredentialRevocation: UseAfterDecommissioning	User accounts are not deleted when employees leave a company leading to possible misuse of the old accounts by unauthorized persons. – A credential stored in a hardware device is used after its cryptographic keys have been revoked.
CredentialRenewal: Disclosure	Credential renewed by the CSP for an entity is copied by an attacker as it is transported.
CredentialRenewal: Tampering	A new credential created by an entity is modified by an attacker as it is being submitted to the CSP to replace an expired credential.
CredentialRenewal: UnauthorizedRenewal	An attacker is able to take advantage of a weak credential renewal protocol to extend the credential validity period for a current entity. An attacker fools the CSP into issuing a new credential for a current entity, and the new credential binds the current entity's identity to a credential provided by the attacker. For NPE entities, an example can be re-labelling (re-issuing) a system component (e.g., RAM) as new after it has been used.
CredentialRecordkeeping: Repudiation	An entity asserts or claims that a legitimate credential is fraudulent or contains incorrect information in order to falsely deny having used the credential.

10.2.2 Required LoA controls to protect against credential management phase threats

Table 10-4 identifies the required controls against credential management threats according to the LoA.

Table 10-4 – Credential management controls for each LoA

Threats	Controls	Required controls			
		LoA1	LoA2	LoA3	LoA4
CredentialCreation: Tampering	AppropriateCredentialCreation	#1	#1	#2	#2
	HardwareOnly				#3
	StateLocked				#4
CredentialCreation: UnauthorizedCreation	TrackedInventory	#5	#5	#5	#5
CredentialIssuance: Disclosure	AppropriateCredentialIssuance	#6	#7	#7	#8
CredentialActivation: UnauthorizedPossession CredentialActivation: Unavailability	ActivatedByEntity	#9	#9	#10	#11
CredentialStorage: Disclosure CredentialStorage: Tampering CredentialStorage: Duplication CredentialStorage: DisclosureByEntity	CredentialSecureStorage	#12	#13	#14	#15
CredentialRevocation: DelayedRevocation CredentialRevocation: UseAfterDecommissioning	CredentialSecureRevocation &Destruction	#16	#16	#16	#16
CredentialRenewal: Disclosure CredentialRenewal: Tampering CredentialRenewal: UnauthorizedRenewal	CredentialSecureRenewal	#17	#17	#18	#19
CredentialRecordkeeping: Repudiation	RecordRetention	#20	#20	#21	#21

NOTE – In the above table, the identifiers #1-#21 correspond to the specific controls required to provide protection at each LoA. Each of these controls is described in detail in clause 10.2.2.1. Boxes in the table with a diagonal line indicate that the respective control is not applicable at the indicated LoA.

10.2.2.1 Controls against credential management phase threats

The following controls against credential management phase threats correspond to the numbers #1-#21 listed in Table 10-4.

<u>AppropriateCredentialCreation</u>

#1. The following controls apply:

- Formalized and documented processes shall be used for credential creation.
- Prior to finalizing the binding of a credential to an entity, the CSP must have adequate assurance that the credential is bound and remains bound to the correct entity.

#2. The following controls apply:

- all controls from #1.

  In addition:
- Credential binding shall provide protection against tampering by either using:

  a) digital signatures; or

  b) the mechanisms described in StateLocked for credentials held on a hardware device.

HardwareOnly

#3. Credentials shall be contained on a hardware security module.[6]

StateLocked

#4. Credentials held on a hardware device shall be put in a locked state at the end of the creation process.

TrackedInventory

#5. If a credential, or the means to produce credentials, is held on a hardware device, the hardware device shall be kept physically secure and the inventory tracked. For example, non-personalized smart cards should be stored in a secure place and their serial numbers recorded to protect against theft and subsequent attempts to create unauthorised credentials.

AppropriateCredentialIssuance

#6. Formalized and documented processes shall be used for credential issuance.

#7. The following controls apply:

- all controls from #6.

  In addition:

- The issuance process shall include a mechanism to ensure that a credential is provided to the correct entity or an authorized representative. If the credential is not delivered in person, a mechanism shall be used to check that the delivery address exists and is legitimately associated with the entity.

#8. The following controls apply:

- all controls from #7.

  In addition:

- If a credential is not delivered in person, then it shall be delivered using a secure channel and the entity or an authorized representative of the entity shall sign a receipt acknowledging receipt of the credential.

ActivatedByEntity

#9. A procedure shall exist to ensure that a credential, or the means to generate a credential, is activated only if it is under the control of the intended entity. There are no specific requirements for this procedure.

#10. A procedure shall exist to ensure that a credential, or the means to generate a credential, is activated only if it is under the control of the intended entity. This procedure shall prove that the entity is bound to the activation of a credential (e.g., challenge-response protocol).

#11. A procedure shall exist to ensure that a credential, or the means to generate a credential, is activated only if it is under the control of the intended entity. This procedure shall:

a) prove that the entity is bound to the activation of a credential (e.g., challenge-response protocol), and

b) allow activation only within a period of time determined by policy.

[6] The boundary of a hardware security module is defined in ISO/IEC 19790:2012.

CredentialSecureStorage

#12. The following controls apply:

- Credentials based on shared secrets shall be protected by access controls that limit access to only those administrators and applications that require access; and
- Protection policy for stored credentials shall be described in the documentation associated with the use of those credentials that is made available to entities.

#13. The following controls apply:

- all controls from #12.

  In addition:
- Such shared secret files shall not contain the plaintext passwords or secrets; an alternative method may be used to protect the shared secret.

#14. The following controls apply:

- all controls from #13.

  In addition:
- Shared secrets shall be protected by access controls that limit access to only those administrators and applications that require access. Such shared secrets shall be encrypted. The encryption key for the shared secret shall itself be encrypted and stored in a cryptographic module (hardware or software). The encryption key for the shared secret shall be decrypted only as immediately required for an authentication operation; and
- Entities or authorized representatives of entities shall be required to acknowledge that they understand these requirements and agree to protect credentials in accordance with these requirements.

#15. The following controls apply:

- all controls from #14.

  In addition:
- Entities or authorized representatives of entities shall be required to sign a document acknowledging that they understand the requirements for the storage of credentials and agree to protect credentials accordingly.

CredentialSecureRevocation&Destruction

#16. CSPs shall revoke or destroy (if possible) credentials (including those based on shared secrets) within a specific time period for each LoA as defined by organizational policy.

CredentialSecureRenewal

#17. The following controls apply:

- The CSP shall establish suitable policies for the renewal and replacement of credentials.
- Proof-of-possession of the unexpired current credential shall be demonstrated by the entity prior to the CSP allowing renewal and/or replacement.
- Passwords shall meet minimum CSP policy requirements for password strength and re-use.
- After expiry of the current credential, renewal shall not be permitted.
- All interactions shall occur over a protected channel.

#18. The following controls apply:

- all controls from #17.

  In addition:

- They will perform an LoA2 identity proofing in accordance with clause 10.1.2.1 (IdentityProofing: PolicyAdherence, IdentityProofing: AuthoritativeInformation).

#19. The following controls apply:

- all controls from #17.

  In addition:

- The will perform an LoA3 identity proofing in accordance with clause 10.1.2.1 (IdentityProofing: PolicyAdherence, IdentityProofing: AuthoritativeInformation).

<u>RecordRetention</u>

#20. A record of the registration, history and status of each credential (including revocation) shall be maintained by the CSP. The duration of retention shall be specified in the CSP policy.

#21. The following controls apply:

- all controls from #20; and
- formalized and documented procedures shall be developed for the chain of custody for each record.

10.3 Threats to, and controls for, the authentication phase

10.3.1 Authentication phase threats

Threats to the authentication phase include both threats associated with the use of credentials during authentication and general threats to authentication. General threats to authentication include, but are not limited to: malicious software (e.g., viruses, Trojans, keystroke loggers), social engineering (e.g., shoulder surfing, theft of hardware devices and pins); user errors (e.g., weak passwords, failure to protect authentication information), false repudiation, unauthorized interception and/or modification of authentication data during transmission, denial of service, and procedural weaknesses. With the exception of the use of multifactor authentication, controls for general threats to authentication are beyond the scope of this Recommendation. This clause focuses on the threats associated with the use of credentials for authentication, describes those threats and lists controls for each type of threat.

Except for the requirement to use multifactor authentication for LoAs 3 and 4, it is not appropriate to delineate specific controls in terms of LoA for the authentication phase. Some controls may not be appropriate for all contexts. For example, controls for the authentication of users accessing online magazine subscriptions are probably different from controls for medical doctors accessing patient records. Therefore, it is recommended that, as the risk and consequence of exploitation grows more severe, the CSP should consider security in depth (i.e., layering controls appropriate to the operational environment, the application, and the LoA). It is up to the system designer, based on risk analysis, to make the decisions as to how, when, and in what combination to use these controls.

There are many threats to credentials used for authentication. Table 10-5 lists some broad categories of threats to the use of credentials and provides specific examples to illustrate the threats.

Table 10-5 – Summary of threats to the use of credentials in the authentication phase

Threat	Examples
General threats	General threats to authentication include many categories of threat common to any type of ICT. Some examples include keystroke loggers, social engineering, and user errors. Except for the use of multifactor authentication, controls against these threats are beyond the scope of this Recommendation. Note that multifactor authentication does not protect against all possible general threats.
OnlineGuessing	An attacker performs repeated logon attempts by guessing possible values of the credential.
OfflineGuessing	Secrets associated with credential generation are exposed using analytical methods outside the authentication transaction. Password cracking often relies upon brute force methods, such as the use of dictionary attacks. 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. 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.
CredentialDuplication	The entity's credential, or the means to generate credentials, has been illegitimately copied. An example would be the unauthorized copying of a private key.
Phishing	An entity 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 entity. An example is when an entity is sent an email that redirects him or her to a fraudulent website and asks the user to log in using his or her username and password.
Eavesdropping	An attacker listens passively to the authentication transaction to capture information which can be used in a subsequent active attack to masquerade as the entity.
ReplayAttack	An attacker is able to replay previously captured messages (between a legitimate entity and an RP) to authenticate as that entity to the RP.
SessionHijack	An attacker is able to insert himself or herself between an entity and a verifier subsequent to a successful authentication exchange between the latter two parties. The attacker is able to pose as an entity to the relying party or vice versa to control session data exchange. An example is when 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 entity.
ManInTheMiddle	The attacker positions himself or herself between the entity 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 entity and simultaneously impersonates the entity 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.
CredentialTheft	A device that generates or contains credentials is stolen by an attacker.

Table 10-5 – Summary of threats to the use of credentials in the authentication phase

Threat	Examples
SpoofingAndMasquerading	Spoofing and masquerading refer to situations in which an attacker impersonates another entity in order to allow the attacker to perform an action he would otherwise not be able to perform (e.g., gain access to an otherwise inaccessible asset). This may be done by making use of the credential(s) of an entity or otherwise posing as an entity (e.g., by forging a credential). Some examples are when an attacker impersonating an entity spoofs one or more biometric characteristics by creating a "gummy" finger that matches the pattern of the entity; an attacker spoofs a MAC address by having its device broadcast a MAC address that belongs to another device that has permissions on a particular network; or an attacker poses as a legitimate software publisher responsible for downloading on-line software applications and/or updates.

10.3.2 Required LoA controls to protect against threats to the use of credentials

Table 10-6 identifies the required controls to counter credential use threats according to LoA.

Table 10-6 – Summary of controls for threats to the use of credentials according to LoA

Threats	Controls	Required controls				
		LoA*	LoA1	LoA2	LoA3	LoA4
General**	MultiFactorAuthentication				#1	#1
OnlineGuessing	StrongPassword CredentialLockOut DefaultAccountUse AuditAndAnalyze	#2 #3 #4 #5				
OfflineGuessing	HashedPasswordWithSalt	#6				
CredentialDuplication	AntiCounterfeiting	#7				
Phishing	DetectPhishingFromMessages AdoptAntiPhishingPractice MutualAuthentication	#8 #9 #10				
Eavesdropping	NoTransmitPassword EncryptedAuthentication DifferentAuthenticationParameter	#11 #12 #13				
ReplayAttack	DifferentAuthenticationParameter Timestamp PhysicalSecurity	#13 #14 #15				
SessionHijacking	EncryptedSession FixProtocolVulnerabilities CryptographicMutualHandshake	#16 #17 #18				
ManInTheMiddle	MutualAuthentication EncryptedSession	#10 #16				

Table 10-6 – Summary of controls for threats to the use of credentials according to LoA

Threats	Controls	Required controls				
		LoA*	**LoA1**	**LoA2**	**LoA3**	**LoA4**
CredentialTheft	CredentialActivation	#19				
SpoofingAndMasquerading	CodeDigitalSignature LivenessDetection	#20 #21				
LoA* – These controls should be applied as determined necessary by a risk assessment. General** – Not all of the general threats can be resisted by multifactor authentication.						

NOTE – In the above table, the identifiers #1-#21 correspond to the specific controls required to provide protection at each LoA. Each of these controls is described in detail in clause 10.3.2.1.

10.3.2.1 Controls against threats to the use of credentials in the authentication phase

The following controls against threats to the use of a credential during the authentication phase correspond to the numbers #1-#21 listed in Table 10-6.

MultiFactorAuthentication

#1. Two or more credentials implementing different authentication factors shall be used (e.g., something you have combined with something you know).

StrongPassword

#2. Use of strong passwords (e.g., complex, non-dictionary strings that contain mixtures of upper case, lower case, numeric and special characters) shall be enforced.

CredentialLockout

#3. A lockout or slowdown mechanism shall be used after a certain number of failed password attempts.

DefaultAccountUse

#4. Default account names and password (e.g., manufacturer's settings) shall not be used.

AuditAndAnalyze

#5. An audit trail of failed logins shall be used to analyse for patterns of online password guessing attempts.

HashedPasswordWithSalt

#6. Hashed passwords with salt shall be used to deter brute force and rainbow table attacks.

Anticounterfeiting

#7. Anti-counterfeiting measures (e.g., holograms, microprint) shall be used on devices holding credentials.

DetectPhishingFromMessages

#8. Controls shall be implemented that are specifically designed to detect phishing attacks (e.g., Bayesian filters, IP blacklists, URL-based filters, heuristics and fingerprinting schemes).

AdoptAntiPhishingPractice

#8. Practices such as disabling images, disabling hyperlinks from untrusted sources and providing visual cues in email clients shall be used to protect entities against phishing attacks.

MutualAuthentication

#9. Mutual authentication shall be used.

NoTransmitPassword

#11. Authentication mechanisms that do not transmit passwords over the network shall be used (e.g., Kerberos protocol).

EncryptedAuthentication

#12. If authentication exchange over a network is necessary, the data shall be encrypted prior to transit.

DifferentAuthenticationParameter

#13. A different authentication parameter shall be used for each authentication transaction (e.g., one-time password, session credential).

Timestamp

#14. Each message shall be time-stamped with a non-forgeable time stamp.

PhysicalSecurity

#15. Physical security mechanisms shall be used (i.e., tamper evidence, detection and response).

EncryptedSession

#16. Encrypted sessions shall be used.

FixProtocolVulnerabilities

#17. Platform patches to fix protocol vulnerabilities (e.g., TCP/IP) shall be used.

CryptographicMutualHandshake

#18. A mutual handshake exchange based on cryptography (e.g., TLS) shall be used.

CredentialActivation

#19. An activation feature shall be required to use the credential (e.g., entering a PIN or biometric information into the hardware device containing the credential).

CodeDigitalSignature

#20. Digital signatures shall be verified against a trusted source to counter the downloading of software that has been modified by unauthorized parties.

LivenessDetection

#21. Liveness detection techniques shall be used to identify the use of artificial biometric characteristics (e.g., forged fingerprints).

11 Service assurance criteria

Trust framework operators that seek to comply with this framework shall establish specific criteria fulfilling the requirements of 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.

Annex A

Characteristics of a credential

(This annex forms an integral part of this Recommendation.)

a) A credential is data.

A credential does not include any physical container or device that holds the data. Nor does it include a generator for the data that makes up the credential. Thus, a pass code generator is never part of a credential, and neither is a smart card that can sign data, software that generates digital signatures, or paper on which things might be written.

b) A credential must contain data that is evidence of an identity and/or entitlements.

Examples of such evidence are:

1) something known (e.g., static password);

2) a biometric characteristic or a representation of the same; or

3) data produced by something possessed (e.g., one-time pass codes produced by a pass-code generator, data that is digitally signed by hardware or software using a private key presumed to be in the possession of an entity).

c) A credential may be accompanied by other data that can be useful to the authentication and identification processes, but which do not form part of the actual credential.

Examples of this data include the name of an entity and a public key certificate. Neither of these things are necessary as evidence of an identity or entitlements, but they are useful in authentication protocols. Associating the name of the entity with a credential confirms the identity. Associating a public key certificate with a credential provides information that assists in testing the evidence as well as possibly providing information about the identity or entitlements of an entity.

d) A credential can also be a derived credential.

In this case, such a derived credential can be a collection of information derived from a set of credentials, usually created and sent by an entity to authenticate to a credential verifier. For example, for some types of anonymous authentication, the entity transforms the credential issued by the CSP into a derived credential that is used for authentication.

e) Not all data that comprises a credential needs to be kept secret.

f) A credential can be used for authentication, identification or authorisation of the entity, or a combination of all three.

g) A credential must be verified before it can be accepted as authentic and trustworthy for its particular purpose (e.g., authentication, identification, authorization).

h) A credential must go through several steps to be verified. Examples of these steps include:

1) checking the authenticity of the credential to ensure it originated with the purported issuer;

2) confirming the validity and trustworthiness of the credential (e.g., determining if there is a direct link to a trusted root from the credential issuer);

3) confirming the computational accuracy of the mathematics/cryptography.

i) A credential can be authentic but not valid in all contexts (e.g., the credential held on a smart card, such as a pre-paid telephone chip card, can be authentic but it may be valid only for calls made using the facilities of the issuer).

Appendix I

Privacy and protection of PII

(This appendix does not form an integral part of this Recommendation.)

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 entities entails significant risks for organizations, ranging from reputational damage to liability exposure. The use of PII for authentication purposes and its protection, therefore needs to be carefully weighed and considered. This appendix 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 entities are individuals, the majority of authentication approaches will involve the processing of PII during one or more of the following:

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

b) during the creation, issuance and management of credentials of entities;

c) during the use of credentials by the entity and their verification by relying parties and verifiers.

It is possible to have strong authentication and strong privacy. Many cryptographically strong authentication approaches exist, 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 entities, 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 an entity from other possible entities in the context of an authentication. 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 entities in the phases and processes described in this EAAF. In particular, the chosen authentication approach should be designed and implemented in a way that generally minimizes the 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) [b-ISO/IEC 29100] describes basic 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 entity. [b-ISO/IEC 29100] describes the following basic privacy principles: 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 a risk assessment to analyse for threats, organizations should conduct a privacy impact assessment of their authentication approach to assess which components of their systems will require specific attention in terms of privacy protection measures.

b) [b-ISO/IEC 29101] provides an architectural framework for ICT systems that process PII. This architecture framework is expressed in concerns and several architectural views. A set of components is provided for implementing ICT systems processing PII. The framework is meant to be used to construct system architectures that follow the privacy principles addressed in [b-ISO/IEC 29100].

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

Bibliography

[b-ITU-T X.1252] Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions*.

[b-ITU-T Y.2702] Recommendation ITU-T Y.2702 (2008), *Authentication and authorization requirements for NGN release 1*.

[b-ITU-T Y.2720] Recommendation ITU-T Y.2720 (2009), NGN *identity management framework*.

[b-ITU-T Y.2721] Recommendation ITU-T Y.2721 (2010), *NGN identity management requirements and use cases*.

[b-ITU-T Y.2722] Recommendation ITU-T Y.2722 (2010), *NGN identity management mechanisms*.

[b-ISO/IEC 9798] ISO/IEC 9798:2010, *Information technology – Security techniques – Entity authentication*.

[b-ISO/IEC 18014-2] ISO/IEC 18014-2:2009, *Information technology – Security techniques – Time-stamping services – Part 2: Mechanisms producing independent tokens*.

[b-ISO/IEC 19790] ISO/IEC 19790:2012, *Information technology – Security techniques – Security requirements for cryptographic modules*.

[b-ISO/IEC 19792] ISO/IEC 19792:2009, *Information technology – Security techniques – Security evaluation of biometrics*.

[b-ISO/IEC 27000] ISO/IEC 27000:2012, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/IEC 27001] ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management system – Requirements*.

[b-ISO/IEC 29100] ISO/IEC 29100:2011, *Information technology – Security techniques – Privacy framework*.

[b-ISO/IEC 29101] ISO/IEC 29101, *Information technology – Security techniques – Privacy architecture framework*.

[b-ISO/IEC 24760-1] ISO/IEC 24760-1:2011, *Information technology – Security techniques – A framework for identity management – Part 1: Terminology and concepts*.

[b-ISO/IEC 19790] ISO/IEC 19790:2012, *Information technology – Security techniques – Security requirements for cryptographic modules*.

[b-NIST SP800-36] NIST Special Pub 800-36 (2003), *Guide to Selecting Information Technology Security Products*.
<http://csrc.nist.gov/publications/nistpubs/800-36/NIST-SP800-36.pdf>

[b-NIST SP800-63] NIST Special Pub 800-63 (2006), *Electronic Authentication Guideline Version 1.0.2*.
<http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf>

[b-AGGPKI] *Australian Government Gatekeeper Public Key Infrastructure*.
http://www.gatekeeper.gov.au/

[b-DuD] Van Alsenoy B., and De Cock, D. (2008), *'Due processing of personal data in eGovernment? A Case Study of the Belgian electronic identity card'*, *Datenschutz und Datensicherheit*, Vol.32, No.3, pp.178-183.

[b-EoI] New Zealand Standard: *Evidence of Identity Standard Version 2.0, 2009.*
<http://www.dia.govt.nz/EOI/pdf/EOIv2.0.pdf>

[b-ENISA] ENISA, *Mapping (Interoperable Delivery of European e-government services to public Administrations, Businesses and Citizens) IDABC Authentication Assurance Levels to SAML v2.0.*

[b-IAF] *Kantara Initiative Identity Assurance Framework v2.0.*
http://kantarainitiative.org/confluence/display/GI/Identity+Assurance+Framework

[b-MOV] Menezes, A., van Oorschot, P., and Vanstone, S. (1997), '*Handbook of Applied Cryptography*', pp. 3-4.
<http://www.cacr.math.uwaterloo.ca/hac/>

[b-NeAF] *The National e-Authentication Framework.*
<http://www.finance.gov.au/e-government/security-and-authentication/authentication-framework.html>

[b-OECD] OECD (2007), *OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication.*
<http://www.oecd.org/dataoecd/32/45/38921342.pdf>

[b-OMB] OMB M-04-04 (2003), *e-Authentication Guidance for Federal Agencies*
<http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>

[b-PEA] Industry Canada (2004), *Principles for Electronic Authentication: A Canadian Framework.*
<http://strategis.ic.gc.ca/epic/site/ecic-ceac.nsf/en/h_gv00240e.html>

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2013