ISO/IEC JTC 1/SC 27 N10558

ISO/IEC JTC 1/SC 27/WG 5 N510558

REPLACES: N

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE: Text for DIS

TITLE: **Text for ITU-T Recommendation X.1254 | ISO/IEC DIS 29115 -- Information technology – Security techniques – Entity authentication assurance framework**

SOURCE: Project Editors, Erika McCallister (ISO), Richard Brackney (ITU-T)

DATE: 2011-11-xx

PROJECT: **29115 (1.27.57)**

STATUS: In accordance with resolution 1 (contained in SC 27 N10525) of the 12th SC 27/WG 5 meeting held in Nairobi 10-14 October 2011.

PLEASE NOTE: For comments please use THE SC 27 TEMPLATE separately attached to this document.

ACTION: **COM**

DUE DATE: **2012-xx-xx**

DISTRIBUTION: P, O- and L-Members
W. Fumy, SC 27 Chairman
M. De Soete, SC 27 Vice-chair
E. J. Humphreys, K. Naemura, M. Bañón, M.-C. Kang, K. Rannenberg, WG-Conveners

MEDIUM: Livelink-server

NO. OF PAGES: 1 + 36

Secretariat ISO/IEC JTC 1/SC 27 - DIN Deutsches Institut für Normung e. V., Burggrafenstr. 6, 10772 Berlin, Germany, Telephone: + 49 30 2601-2652; Facsimile:+ 49 30 2601-1723; e-mail: krystna.passia@din.de
HTTP://www.jtc1sc27.din.de/en

ITU

International
Telecommunication Union

ISO

International Organization
for Standardization

IEC

International
Electrotechnical
Commission

ITU-T Recommendation X.1254 | International Standard ISO/IEC DIS 29115

Information technology — Security techniques — Entity authentication assurance framework

CONTENTS

Foreword

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardisation 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 standardising telecommunications on a world-wide basis. The World Telecommunication Standardisation Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups that, 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 that fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

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

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

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

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

ISO/IEC 29115 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*. The identical text is published as ITU-T Recommendation X.1254.

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.

This Recommendation | International Standard provides a framework for entity authentication assurance. Assurance within this Recommendation | International Standard refers to the confidence placed in all of the processes, management activities, and technologies used to establish and manage the identity of an entity for use in authentication transactions.

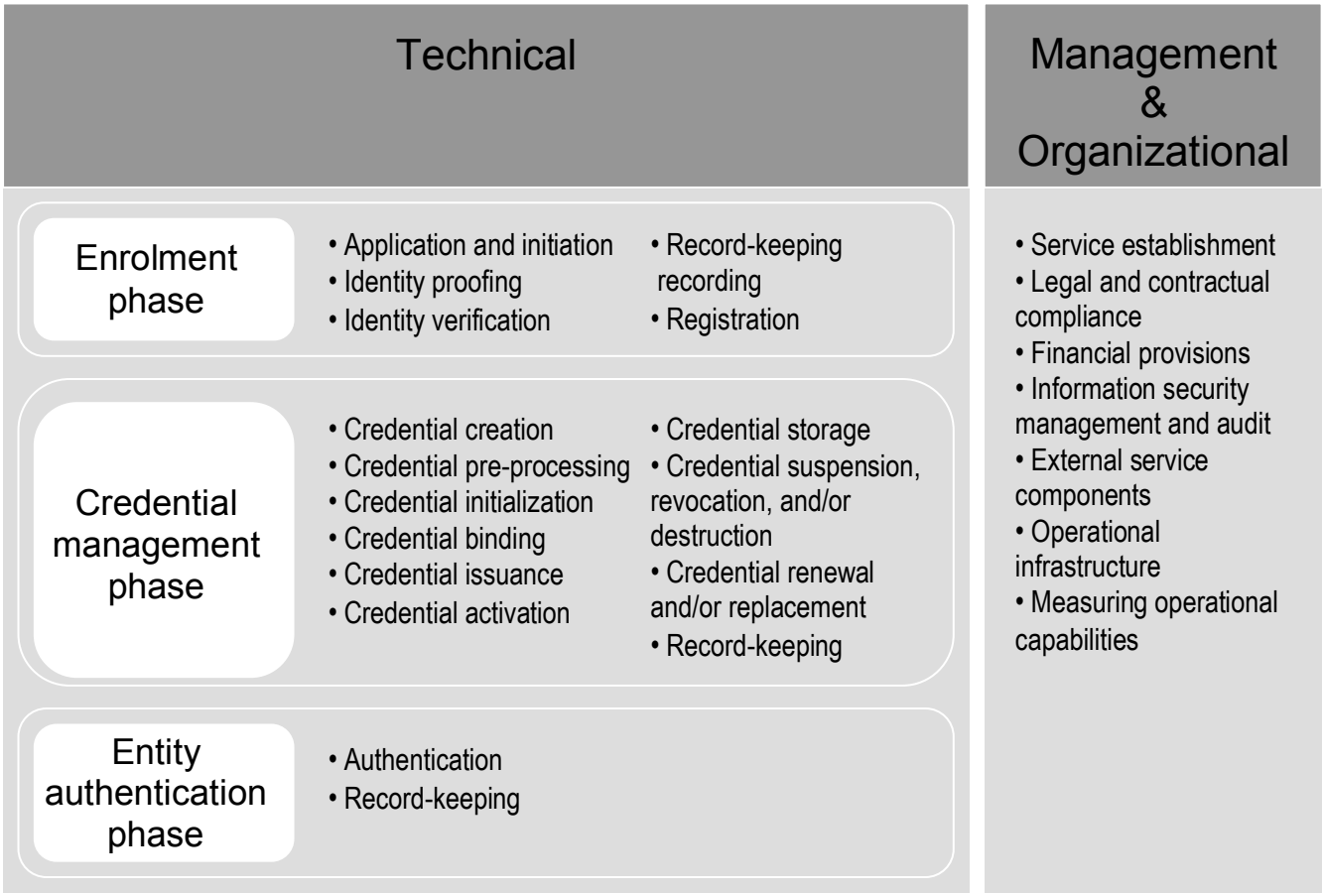

Figure 1 – Overview of the Entity Authentication Assurance Framework

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

This Recommendation | International Standard is intended to be used principally by CSPs and by others having an interest in their services (e.g., RPs, 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 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 | International Standard 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 bilateral or federated legal constellations.

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

Information technology — Security techniques — Entity authentication assurance framework

1 Scope

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

- specifies four levels of entity authentication assurance;
- specifies criteria and guidelines for 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 Normative references

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

2.1 Identical Recommendations | International Standards

None.

2.2 Paired Recommendations | International Standards

None.

2.3 Additional references

None.

3 Definitions

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

3.1 **Assertion:** Statement made by an entity without accompanying evidence of its validity [ITU-T X.1252].

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 | International Standard, an assertion is considered to be a stronger statement than a claim.

3.2 **Authentication:** Provision of assurance in the claimed identity of an entity [ISO/IEC 18014-2].

3.3 **Authentication Factor:** Piece of information and process used to authenticate or verify the identity of an entity [ISO/IEC 19790].

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); or
- something an entity typically does (e.g., behaviour pattern).

3.4 Authentication Protocol: Defined sequence of messages between an entity and a verifier that enables the verifier to corroborate the entity's identity.

3.5 Authoritative Source: Repository which is recognized as being an accurate and up-to-date source of information.

3.6 Claim: Statement that something is the case, without being able to give proof [ITU-T X.1252].

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 | International Standard, an assertion is considered to be a stronger statement than a claim.

3.7 Context: Environment with defined boundary conditions in which entities exist and interact [ITU-T X.1252].

3.8 Credential: Set of data presented as evidence of an asserted identity and/or entitlements [ITU-T X.1252].

NOTE – See Annex A for additional characteristics of a credential.

3.9 Credential Service Provider: Trusted actor that issues and/or manages credentials.

NOTE - The Credential Service Provider (CSP) may encompass Registration Authorities (RAs) and verifiers that it operates. A CSP may be an independent third party, or it may issue credentials for its own use.

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

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

3.11 Entity Authentication Assurance: Degree of confidence reached in the authentication process that the entity is what it claims to be or is expected to be [X.1252].

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

3.12 Identifier: One or more attributes that uniquely characterize an entity in a specific context.

3.13 Identity: Set of attributes related to an entity [ISO/IEC 24760].

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

3.14 Identity Proofing: Process by which the Registration Authority (RA) captures and verifies sufficient information to identify an entity to a specified or understood level of assurance.

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

3.16 Multifactor Authentication: Authentication with at least two independent authentication factors [ISO/IEC 19790].

3.17 Mutual Authentication: Authentication of identities of entities which provides both entities with assurance of each other's identity.

3.18 Non-repudiation: Ability to protect against denial by one of the entities involved in an action of having participated in all or part of the action [X.1252].

3.19 Registration Authority: Trusted actor that establishes and/or verifies and vouches for the identity of an entity to a CSP.

NOTE - The RA may be an integral part of a CSP, or it may be independent from a CSP, but it has a relationship with the CSP.

3.20 Relying Party: Actor that relies on an identity assertion or claim.

3.21 Repudiation: Denial by an entity of a claimed event or action.

3.22 Salt: Non-secret, often random, value that is used in a hashing process.

NOTE - It is also referred to as sand.

3.23 Shared Secret: Secret used in authentication that is known only to the entity and the verifier.

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

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

3.26 Trust Framework: Set of requirements and enforcement mechanisms for parties exchanging identity information.

3.27 Trusted Third Party: Authority or its agent, trusted by other actors with respect to security related activities.

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

3.28 Validity Period: Time period during which an identity or credential may be used in one or more transactions.

3.29 Verification: Process of checking information by comparing the provided information with previously corroborated information and the binding to the entity.

3.30 Verifier: Actor that corroborates identity information.

3.31 Verify: Check information by comparing the provided information with previously corroborated information and the binding to the entity.

4 Abbreviations

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

CSP	Credential Service Provider
EAA	Entity Authentication Assurance
EAAF	Entity Authentication Assurance Framework
IdM	Identity Management
ICT	Information and Communications Technology
IP	Internet Protocol
LoA	Level of Assurance
LoAs	Levels of Assurance
MAC	Media Access Control
NPE	Non-Person Entity
PII	Personally Identifiable Information
PIN	Personal Identification Number
RA	Registration Authority
RP	Relying Party
SAML	Security Assertion Markup Language
SSL	Secure Sockets Layer
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 | International Standard follows the ISO Directive, Part 2, Annex H regarding verbal forms for the expression of provisions.

a) "Shall" indicates a requirement;

b) "Should" indicates a recommendation;

c) "May" indicates a permission;

d) "Can" indicates a possibility and capability.

6 Levels of assurance

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 claiming a particular identity (i.e., the entity) is in fact the entity to which that identity was assigned. For the purposes of this Recommendation | International Standard, LoA is a function of the process 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. Entity Authentication Assurance (EAA) is affected by management and organizational considerations, but this Recommendation | Standard does not provide explicit normative criteria for those considerations. An entity can be a human or a non-person entity (NPE).

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

LoA1 is the lowest level of assurance, and LoA4 is the highest level of assurance. 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 verification, registration);

b) Credential management (e.g., credential issuance, credential activation); and

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[1]

Level	Description
1 – Low	Little or no confidence in the asserted identity

[1] LoA is a function of the process 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.

2 – Medium	Some confidence in the asserted identity
3 – High	High confidence in the asserted identity
4 – Very high	Very high confidence in the asserted identity

This framework contains requirements to achieve a desired LoA for each entity authentication assurance framework phase. The 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 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 authentication requirements for this LoA. This level does not require use of cryptographic methods.

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

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

6.2 Level of assurance 2 (LoA2)

At LoA2, there is some confidence in the 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 shall be in place to reduce the effectiveness of eavesdropper and online guessing attacks. Controls shall be in place to protect against attacks on stored credentials.

For example, an insurance provider might operate a website which enables its customers to change their address of record. The transaction in which a beneficiary changes an address of record may be considered a LoA2 authentication transaction. This transaction involves a moderate risk of inconvenience. Since official notices regarding payment amounts, account status, and records of changes are sent to the beneficiary's address of record, the transaction additionally entails moderate risk of unauthorized release of PII. As a result, the insurance company 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 an asserted identity of the entity. This LoA is used where substantial risk is associated with erroneous authentication. This LoA shall employ multi-factor authentication. Identity proofing procedures shall be dependent upon verification of identity information. Any secret information exchanged in authentication protocols shall be cryptographically protected. There are no requirements concerning the generation or storage of credentials; they may be stored or generated in general purpose computers or special purpose hardware.

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

6.4 Level of assurance 4 (LoA4)

At LoA4, there is very high confidence in an asserted identity of the entity. This LoA is used when a high risk is associated with erroneous authentication. LoA4 provides the highest level of entity authentication assurance defined by this Recommendation | Standard. 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.

For example, dispensation by a pharmacist of a controlled medication may require LoA4 protection. The pharmacist needs full assurance that a qualified doctor prescribed the drug, and the pharmacist may be criminally liable for any failure to verify the prescription and dispense the correct medication in the prescribed amount. Finally, approval by an executive of a significant transfer of funds from an organization's bank accounts may be a LoA4 transaction.

At LoA4, digital certificates (e.g., 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 smart phone enrolment process may require the deployment of digital certificates to the smart phone. 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. Further information on assessing impact levels is provided in Table 6-2.

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

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

Determination of what constitutes insignificant, moderate, significant, and high risk depends on the risk criteria defined by the organization using this standard.

Each LoA shall be determined by the strength and rigor 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 | Standard.

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; and

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 to mitigate fraud and is comfortable accepting the risk of fraud).

The risk assessment of a transaction may be conducted as a part of 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 meets 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.

The organizations concerned shall take steps to:

a) Communicate to their counterparts their expectations of acceptable assurances and, therefore, the LoA which counterparts shall possess;

b) Implement operational policies and technical controls to ensure that those LoAs are upheld within systems that execute the identified transactions (e.g., publication of policies); and

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

6.6 LoA mapping and interoperability

Different domains may define LoAs differently. These LoAs will not necessarily support a 1-to-1 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 standard 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) Levels of impact (i.e., low, medium, high, very high) 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 be carried on a hardware device (e.g., smart card) or specifying requirements for the generation and storage of credentials; and

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 LoA for which it has been certified capable of meeting the requirements associated with that LoA.

Actors to an authentication shall agree on the protocol, semantics, format, and structure of the information to be exchanged. Typical requirements include, but are not limited to, the following:

a) The need for an RP to specify if it will accept any authentication response other than that exactly requested; and

b) The need for an RP to specify requirements for protection of credentials by entities (e.g., whether the credentials shall be stored on or generated by special purpose hardware).

While digital certificates are an established way to convey information concerning 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 URI, 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 credentialing 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 assert 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 characteristics 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 means to produce credentials, to enable later authentication. Credentials, or 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 verifies and 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 verification according to a specified procedure. This is typically done through the evaluation of identity information (e.g., a national identity card, a driver's license) or the verification of records in databases. In order to differentiate the entity from other entities, an entity is typically assigned one or more identifiers, which will allow the entity to later be recognized in the applicable context.

7.4 Relying party

An RP 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 corroborates identity information. The verifier may be a relying party or another party that acts as a trusted third party towards the RP. If the latter is the case, then the verifier will typically, upon successful completion of the verification of the identity information, provide the entity or the relying party with an assertion that contains the result of the verification.

7.6 Trusted third party

A trusted third party (TTP) is an authority or its agent, trusted by other actors with respect to 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 model for 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 and procedures 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; and

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 shall differ according to the rigor required by the applicable LoA. In the case of an entity enrolling under LoA1, these processes shall be 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 only be accepted 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 may record sufficient information to ensure unique identifiability of the entity within a context to which the credential will be issued (e.g., by recording the full name, date and place of birth). For NPEs, such as for a mobile device, enrolment may require initialization through the deployment of credentials to the device, which enables the device to be uniquely identified 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

Identity proofing is the process of capturing and verifying sufficient information to identify an entity to a specified or understood level of assurance. Depending on the context, a variety of identity information (e.g., government identity cards, driver's licenses, biometric information, machine-based attestation, birth certificates) from 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 higher the required LoA, the more stringent the identity proofing requirements shall be. Also, the identity proofing process shall be more stringent for entities claiming 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.[2] 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 using a serial number to check back with the manufacturer.

LoA3 meets 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 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 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.

Table 8-1 – Applying Identity Proofing Objectives to the LoAs

LoA	Description	Objective	Controls	Method of processing[3]
LoA1 - low	Little or no confidence in the asserted identity	Identity is unique within a context	Self-asserted	Local or remote
LoA2 - medium	Some confidence in the 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 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 + verification	Local or remote

[2] This does not exclude the use of pseudonyms.

[3] 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.

LoA4 – very high	Very high confidence in the 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 + verification + entity witnessed in-person[4]	Local only

The impact of the enrolment phase on the LoA shall be determined by the use of the 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 verification purposes. Any implementation of the EAAF shall involve 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.

8.1.3 Identity verification

This is the process of checking information by comparing the provided information with previously corroborated information and the binding to the entity. Both the identity proofing and the verification process are performed in order to achieve a certain level of confidence in the identity of an entity before registering it as a particular entity. Identity verification differs from identity proofing because it involves corroboration of identity information with additional (either internal or external) sources (e.g., issuers of the identity proofing documents presented during enrolment).

8.1.4 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 is created of the enrolment. This record shall include the information and documentation that was collected (and may be retained), information about the identity 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.

8.1.5 Registration

Registration is a process in which an entity requests to use a service or resource. The registration process may be performed during or immediately after enrolment or at a later time after the enrolment phase. Enrolment is only likely to be necessary once, whereas registration may be necessary each time an entity requests access to a service or resource.

8.2 Credential management phase

The credential management phase comprises all processes relevant to the lifecycle management of a credential, or 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.

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

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 prompted for 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. For higher LoAs, this may involve the in-person delivery of a hardware device (e.g., a smart card) that holds a credential. In 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 Credential Service Provider (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 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 activated after a suspension where its validity is 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 use. Credential storage involves the entity associated with a credential and actions required to prevent 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 the part of the credential. 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 timeframe between notice of an event requiring revocation and the completion of the revocation process is determined 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. The rigorousness of the processes for 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); and

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

Records shall be kept of 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 Annex A.

8.3 Entity authentication phase

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

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 a claim of identity. Authentication protocol requirements vary depending on the applicable LoA. For example, for a lower LoA, authentication may involve use of a password. At a higher LoAs, authentication may involve using a cryptographic based challenge-response protocol. Multi-factor 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 Annex A.

9 Management and organizational considerations

EAA comes not 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 | Standard, 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 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 to 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, 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., ISO/IEC 27000-series) should be used.

Depending on the agreements for legal, contractual, and technical compliance, actors should ensure that parties are abiding by commitments and may provide an avenue for redress in the event 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 among entities, identity service providers (e.g., RAs, CSPs), and RPs. Depending on the agreements, these additional actors may be called on to ensure that all parties are abiding by commitments and may provide an avenue for redress in the event they are not.

9.7 Measuring operational capabilities

As noted above, 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 toward 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 | Standard. 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

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

10.1.1 Enrolment phase threats

Table 10-1 provides threats to the enrolment phase.

Table 10-1 – Threats to the enrolment phase

Threat	Description and examples
T.Impersonation	Some examples of impersonation are when an entity illegitimately claims another entity's identity by using a forged driver's license or when a device registers with a network using a spoofed Media Access Control (MAC) address.

10.1.2 Controls against enrolment phase threats by LoA

Table 10-2 provides the required controls for the enrolment phase by LoA.

Table 10-2 – Enrolment phase controls for each LoA

Threats	Controls	Required controls			
		LoA1	LoA2	LoA3	LoA4
T.Impersonation	C.IdentityProofing_Policy	1	1	1	1
	C.IdentityProofing_Local				1
	C.IdentityProofing _AuthoritativeInformation	1	2	3	4

10.1.2.1 Controls against enrolment phase threats

The following controls to enrolment phase threats correspond to the numbers listed in Table 10-2.

C.IdentityProofing_Policy

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

C.IdentityProofing_Local

1. Identity proofing for humans shall only be in-person.

C.IdentityProofing_AuthoritativeInformation

1. Identity information may be self-asserted.
2. The following controls apply:

- All controls from 1.

- Entity shall provide identity information from at least one authoritative source of identity.

a) For humans:

i) Local:

- Ensure that the entity is in possession of an identification document from an 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 by the claimed issuer and valid at the time of application.

ii) Remote:

- Ensure the entity provides a document from another context which includes both contact information and identity information, such as address or phone number from a utility bill or phone bill; and

- Verify the accuracy of contact information listed in one of the aforementioned documents by using it to contact the entity.

b) For NPEs:

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

3. The following controls apply:

- All controls from 2.

- Entity shall provide identity information from at least one authoritative source of identity.

a) For humans:

i) Local:

- Ensure that the entity is in possession of an identification document from an authoritative source that bears a photographic image of the holder that matches the appearance of the entity;

- Ensure the entity provides a document from another context which includes both contact information and identity information, such as address or phone number from a utility bill or phone bill;

- Verify the accuracy of contact information listed in one of the aforementioned documents 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, sufficient to ensure a unique identity; and

- Verify information previously provided by or likely to be known only by the entity.

ii) Remote:

- Ensure check by a trusted third party of the entity's attestation to the current possession of a LoA3 or above credential from an authoritative source;

- Ensure the entity provides a document from another context which includes both contact information and identity information, such as address or phone number from a utility bill or phone bill;

- Verify the accuracy of contact information listed in one of the aforementioned documents by using it to contact the entity; and

- Verify information previously provided by or likely to be known only by the entity.

b) For NPEs:

- Ensure trusted hardware (e.g., TPM) is used at LoA3;

- For NPEs already in use, physically enroll the NPE using a LoA3 human-issued credential with a device RA and trusted hardware enabled. Trusted hardware will be initialized on reconnection to the network;

- For NPEs yet to be issued, order the NPE using a LoA3 human authentication or digital signature. The manufacturer's RA will carry out the registration and enable the trusted hardware. It will then control the issuance and personalization of the NPE. Trusted hardware will be initialized on connection to the network;

- For NPEs other than computers, cryptographically secure the binding between the device, the owner, the network or communication carrier and the RA in a similar manner to a trusted hardware computer; and

- Digitally sign LoA3 software code with a LoA3 human-issued credential before issuance and obtain a counter-signature by the RA for acceptance before being taken into use.

4. The following controls apply:

- All controls from 3.

- Entity shall provide identity information from at least one authoritative source of identity.

a) For humans:

- Ensure that the entity is in possession of an identification document from an authoritative source that bears a photographic image of the holder that matches the appearance of the entity;

- Ensure the entity provides a document from another context which includes both contact information and identity information, such as address or phone number from a utility bill or phone bill;

- Verify the accuracy of contact information listed in one of the aforementioned documents 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, sufficient to ensure a unique identity; and

- Verify information previously provided by or likely to be known only by the entity.

b) For NPEs:

- Ensure that additional devices connected to a computer, smart phone, or similar processor are similarly recorded at issuance and cryptographically bound to the anchor device (e.g., trusted hardware enabled device, biometric reader, smart cards, GPS geo-authenticator);

- Ensure any changes in the binding arrangements between devices are managed through the RA. Where possible, the network management capability should alert the RA or network management of any changes in device relationships and corrective action taken;

- Ensure capability to prevent any altered device relationships from working; and

- Digitally sign LoA4 software code with a LoA4 human-issued credential before issuance and obtain a counter-signature by the RA for acceptance before being taken into use.

10.2 Threats to and controls for the credential management phase

The following subclauses describe threats to and provide 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	Description and examples
T.CredentialCreation_UnauthorizedCreation	An attacker causes a CSP to create a credential based on a fictitious entity.
T.CredentialCreation_Tampering	An attacker alters information as it passes from the enrolment process to the credential creation process.
T.CredentialIssuance_Disclosure	A password 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.
T.CredentialActivation_InThePossession	An attacker obtains a credential that does not belong to him/her and masquerading as the rightful entity causes the CSP to activate the credential.
T.CredentialActivation_Unavailability	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. Also, delivery of a credential, or means to generate the credential, is delayed, and activation within the prescribed period is not possible.
T.CredentialStorage_Disclosure	Usernames and passwords stored in a system file are revealed.
T.CredentialStorage_Tampering	The file that maps usernames to passwords is compromised so that the mappings are modified, and existing passwords are substituted with passwords known to the attacker
T.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 unintended entity.
T.CredentialStorage_DisclosureByEntity	The entity keeps a written record of the username and password in a place that can be accessed by others.
T.CredentialRevocation_DelayedRevocation	Stale certificate revocation lists allow accounts (that should have been locked as a result of credential revocation) to be used by an attacker.

Threat	Description and examples
T.CredentialRevocation_UseAfterDecommissioning	User accounts are not deleted when employees leave a company leading to a possible use of the old accounts by unauthorized persons. A credential stored in a hardware device is used after its cryptographic keys have been revoked.
T.CredentialRenewal_Disclosure	Password renewed by the CSP for an entity is copied by an attacker as it is transported.
T.CredentialRenewal_Tampering	New password created by an entity is modified by an attacker as it is being submitted to the CSP to replace an expired password.
T.CredentialRenewal_UnauthorizedRenewal	Attacker fools the CSP into issuing a new credential for a current entity, and the new credential binds the current entity's identity with a credential provided by the attacker. For NPE entities, an example can be re-labeling (re-issuing) a system component (e.g., RAM) as new after it has been used. Attacker is able to take advantage of a weak credential renewal protocol to extend the credential validity period for a current entity.
T.CredentialManagementRecordkeeping_Repudiation	An entity claims that a legitimate credential is fraudulent or contains incorrect information in order to falsely deny having used the credential.
T. Credential_UnauthorizedControl	Unmitigated threats can result in an attacker gaining control of a credential and masquerading as the entity to which the credential was actually issued.

10.2.2 Controls against credential management phase threats by LoA

Table 10-4 provides the required controls against credential management threats by LoA.

Table 10-4 – Credential management controls for each LoA

Threats	Controls	Required controls			
		LoA1	LoA2	LoA3	LoA4
T.CredentialCreation_Tampering	C.AppropriateCredentialCreation	1	1	2	2
T.CredentialCreation_Tampering	C.StateLocked				1
T.CredentialCreation_Tampering	C. HardwareOnly				1
T.CredentialCreation_UnauthorizedCreation	C.TrackedInventory			1	1
T. CredentialIssuance_ Disclosure	C.AppropriateCredentialIssuance	1	2	2	3
T.CredentialActivation_InThePossession T.CredentialActivation_Unavailability	C.ActivatedFromEntity		1	2	3
T.CredentialStorage_Disclosure T.CredentialStorage_Tampering T.CredentialStorage_Duplication T.CredentialStorage_DisclosureByEntity	C.CredentialSecureStorage	1	2	3	4
T.CredentialRevocation_DelayedRevocation	C.CredentialSecureRevocation &Destruction		1	1	1

T.CredentialRevocation_UseAfterDecommissioning					
T.CredentialRenewal_Disclosure T.CredentialRenewal_Tampering T.CredentialRenewal_UnauthorizedRenewal/re-issuance	C.CredentialSecureRenewal		1	2	3
T.CredentialManagementRecordkeeping_Repudiation	C.RecordRetention		1	2	2

10.2.2.1 Controls against credential management phase threats

The following controls for the credential management phase threats correspond to the numbers listed in Table 10-4.

C.AppropriateCredentialCreation

1. Formalized and documented processes shall be used for credential creation. There are no specific requirements concerning these processes.

2. The following controls apply:

- All controls from 1.

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

a) Digital signatures; or

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

C.HardwareOnly

1. Credential shall be contained on a hardware device.

C.StateLocked

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

C.TrackedInventory

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

C.AppropriateCredentialIssuance

1. Formalized and documented processes shall be used for credential issuance. There are no specific requirements concerning these processes.

2. The following controls apply:

- All controls from 1.

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

3. The following controls apply:

- All controls from 2.

- If a credential is not delivered in person, then it must be delivered using a secure channel (e.g., registered mail), and the entity or a representative of the entity must sign a receipt acknowledging receipt of the credential.

C.ActivatedFromEntity

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

2. A procedure shall exist to ensure that a credential, or means to generate a credential, is only activated if it is under the control of the intended entity. This procedure shall authenticate the identity of the entity in an interaction bound to activation of a credential.

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

a) Authenticate the identity of the entity in an interaction bound to activation of a credential; and

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

C.CredentialSecureStorage

1. The following controls apply:

- Shared secrets shall be protected by access controls that limit access to only those administrators and applications that require access; and

- Requirements for stored credentials protection by entities shall be described in the documentation made available to entities associated with use of credentials.

2. The following controls apply:

- Shared secrets shall be protected by access controls that limit access to only those administrators and applications that require access. Such shared secret files shall not contain the plaintext passwords or secrets; an alternative method may be used to protect the shared secret; and

- Requirements for the protection of stored credentials by entities shall be described in the documentation made available to those entities.

3. The following controls apply:

- Long-term shared secrets shall be protected by access controls that limit access to administrators and only to those 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 only be decrypted as immediately required for an authentication operation;

- Requirements for the protection of stored credentials by entities shall be described in the documentation made available to those entities; and

- Entities or representatives of entities shall be required to acknowledge that they understand these requirements and agree to protect credentials in accordance with these requirements.

4. The following controls apply:

- All controls from 3.

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

C.CredentialSecureRevocation&Destruction

1. CSPs shall revoke or destroy (if possible) credentials within a specific time period for each LoA as defined by organizational policy.

C.CredentialSecureRenewal

1. The following controls apply:

- The CSP shall establish suitable policies for 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 not be reused;

- After expiry of the current credential, renewal shall not be permitted; and

- All interactions shall occur over a protected channel such as SSL/TLS.

2. The following controls apply:

- All controls from 1.

- Perform an LoA2 identity proofing in accordance with 10.1.2.1 (C.IdentityProofing_Policy, C.IdentityProofing_AuthoritativeInformation_2).

3. The following controls apply:

- All controls from 1.

- Perform an LoA3 identity proofing in accordance with 10.1.2.1 (C.IdentityProofing_Policy, C.IdentityProofing_AuthoritativeInformation_3, C.TrustedHardware&Software).

C.RecordRetention

1. A record of the registration, history, and status of each credential (including revocation) shall be maintained by the CSP.

2. The following controls apply:

- All controls from 1.

- 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 to the credential and general threats to authentication. General threats to authentication include: malicious software (e.g., viruses, Trojans, keystroke loggers); social engineering (e.g., shoulder surfing, theft of hardware devices); user errors (e.g., weak passwords, failure to protect credentials); false repudiation; unauthorized interception and/or modification of authentication data during transmission; denial of service; and procedural weaknesses. It is not possible to enumerate all of these general threats to authentication, and multi-factor authentication is required at LoA3 and LoA4 to help mitigate these threats. This clause focuses on the credential threats, describes those threats, and lists controls for each type of threat.

Except for the requirement to use multi-factor 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 organization should consider security in depth (i.e., layering protective measures appropriate to the operational environment, the application, and the LoA deemed necessary). It is up to the organization, based on a risk assessment, to make the decisions as to how, when, and in what combination to use these controls.

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

Table 10-5 – Authentication phase threats

Threat	Description and examples
T.General	General threats to authentication include many categories security threats common to any type of ICT. Some examples include keystroke loggers, social engineering, and user errors.
T.OnlineGuessing	An attacker performs repeated logon attempts by guessing possible values of the credential.
T.OfflineGuessing	Secrets associated with the 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

Threat	Description and examples
	word, and checks the resultant hash value against the database. The use of rainbow tables is another password cracking method that is quicker than typical brute force methods. Rainbow tables are pre-computed tables of clear text/hash value pairs. Rainbow tables are quicker than brute-force attacks because they use reduction functions to decrease the search space. Once generated or obtained, rainbow tables can be used repeatedly by an attacker.
T.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.
T.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.
T.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.
T.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.
T.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 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.
T.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.
T.CredentialTheft	A device that generates or contains credentials is stolen by an attacker.
T.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 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 Controls against authentication phase threats by LoA

Table 10-6 provides the required controls against authentication phase threats by LoA.

Table 10-6 – Authentication phase controls by LoA

Threats	Controls	Required controls				
		LoA*	LoA1	LoA2	LoA3	LoA4
T.General	C.MultiFactorAuthentication				1	1
T.OnlineGuessing	C.StrongPassword C.CredentialLockOut C.DefaultAccountUse C.AuditAndAnalyze	1				
T.OfflineGuessing	C.HashedPasswordWithSalt	1				
T.CredentialDuplication	C.AntiCounterfeiting					
T.Phishing	C.DetectPhishingFromMessages C.AdoptAntiPhishingPractice C.MutualAuthentication	1				
T.Eavesdropping	C.NoTransmitPassword C.EncryptedAuthentication C.DifferentAuthenticationParameter	1				
T.ReplayAttack	C.DifferentAuthenticationParameter C.Timestamp C.PhysicalSecurity	1				
T.SessionHijacking	C.EncryptedSession C.FixTCPIP_Vulnerabilities C.CryptographicMutualHandshake	1				
T.ManInTheMiddle	C.MutualAuthentication C.EncryptedSession	1				
T.Theft	C.CredentialActivation	1				
T.SpoofingAndMasquerading	C.CodeDigitalSignature C.LivenessDetection	1				
LoA* - These controls should be applied as determined necessary by a risk assessment.						

10.3.2.1 Controls against authentication phase threats

The following controls for authentication phase threats correspond to the numbers listed in Table 10-4, if appropriate.

C.MultiFactorAuthentication

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

C.NoTransmitPassword

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

C.EncryptedAuthentication

1. If authentication exchange over a network is necessary, the data shall be encrypted in transit, or an encrypted communication channel (e.g., SSL/TLS) shall be used.

C.DifferentAuthenticationParameter

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

C.Timestamp

1. Each message shall be time-stamped with a non-forgeable timestamp.

C.PhysicalSecurity

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

C.StrongPassword

1. 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.

C.CredentialActivation

1. 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).

C.CredentialLockout

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

C.Anticounterfeiting

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

C.HashedPasswordWithSalt

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

C.ReverseTuringTest[5]

1. Reverse Turing tests shall be used for on-line authentication protocols.

C.DefaultAccountUse

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

C.AuditAndAnalyze

1. An audit trail of failed logins shall be used to analyze for patterns of online password guessing attempts.

C.CodeDigitalSignature

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

C. DetectPhishingFromMessages

1. 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).

C.AdoptAntiPhishingPractice

1. 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.

C.MutualAuthentication

1. Mutual authentication shall be used.

C.EncryptedSession

1. Encrypted sessions shall be used.

---

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

C.FixTCPIPVulnerabilities

1. Platform patches to fix TCP/IP vulnerabilities shall be used.

C.CryptographicMutualHandshake

1. A mutual handshake exchange based on cryptography (e.g., SSL/TLS) shall be used.

C.LivenessDetection

1. Liveness detection techniques shall be used to resist the use of artificial biometric characteristics (e.g., 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

Privacy and protection of PII

(This annex does not form an integral part of this Recommendation | International Standard)

The suitability of a particular authentication approach for a particular use will depend not only on an assessment of authentication effectiveness, but also on the risks and risk tolerance of the organizations involved. Misuse or lack of adequate protection of the PII of 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 section provides informative guidance relating to some of the privacy considerations organizations should take into account when deciding on the use and implementation of a particular authentication approach.

Where entities are individuals, the majority of authentication approaches will involve 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. There exist many cryptographically strong authentication approaches which have limited negative impact on privacy (e.g., anonymous credentials, group signatures). Additionally, it should be noted that the increased strength of the assurance level (e.g., LoA4 versus LoA2) can, but does not necessarily need to, adversely affect the privacy of an individual. Much will depend on the chosen authentication approach and how it is implemented. In making these decisions, every organization should carefully consider the need to protect the PII of 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) 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. IS0/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 analyze 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) ISO/IEC 29101 provides best practice privacy reference architecture guidance for planning and building ICT system architectures to facilitate the proper handling of PII. Using this architecture can facilitate the incorporation of necessary privacy safeguarding controls into an ICT environment.

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

Annex B

Characteristics of a credential

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

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 a claimed identity and/or entitlements.

Examples of such evidence are:

1. Something known (e.g., static password);
2. A biometric characteristic or a representation of 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 is necessary as evidence of a claimed identity or entitlements, but they are useful in authentication protocols. Associating the name of the entity with a credential confirms the claimed 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) Not all data that comprises a credential needs to be kept secret.

For example, credentials that are signed data do not need to be kept secret.

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

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

g) 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; and
3. Confirming the computational accuracy of the mathematics/cryptography.

h) 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 may it be valid only for calls made using the facilities of the issuer).

Annex C

Bibliography

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

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

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

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

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

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

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

[6] Kantara Initiative Identity Assurance Framework v2.0, http://kantarainitiative.org/confluence/display/GI/Identity+Assurance+Framework+v2.0

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

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

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

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

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

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

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

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

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

[16] ITU-T Recommendation X.1252 (2010) Baseline of identity management terms and definitions.

[17] ITU-T Recommendation Y.2702 (2010), Next generation network authentication and authorization requirements.

[18] ITU-T Recommendation Y.2720 (2010), Next generation network identity management framework.

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

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

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

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

[23] ISO/IEC 27001:2005, Information technology – Security techniques – Information security management system.

[24] ISO/IEC 29100:2012, Information technology – Security techniques – Privacy framework.

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