INTERNATIONAL STANDARD

ISO/IEC 29115

First edition
2013-04-01

Information technology — Security techniques — Entity authentication assurance framework

Technologies de l'information — Techniques de sécurité — Cadre d'assurance de l'authentification d'entité

Reference number
ISO/IEC 29115:2013(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

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

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

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

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

ISO/IEC 29115 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

A similar text is published as ITU-T Recommendation X.1254. It differs from this text in three instances: 1) 3.8: the ISO/IEC definition includes asserted identities; 2) Table 10-1: ISO/IEC includes an example for impersonation that includes use of an identity for an entity that does not exist; 3) 10.2.2.1: ISO/IEC describes SSL as an example of a protected channel.

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 International Standard provides a framework for entity authentication assurance. Assurance within this 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.

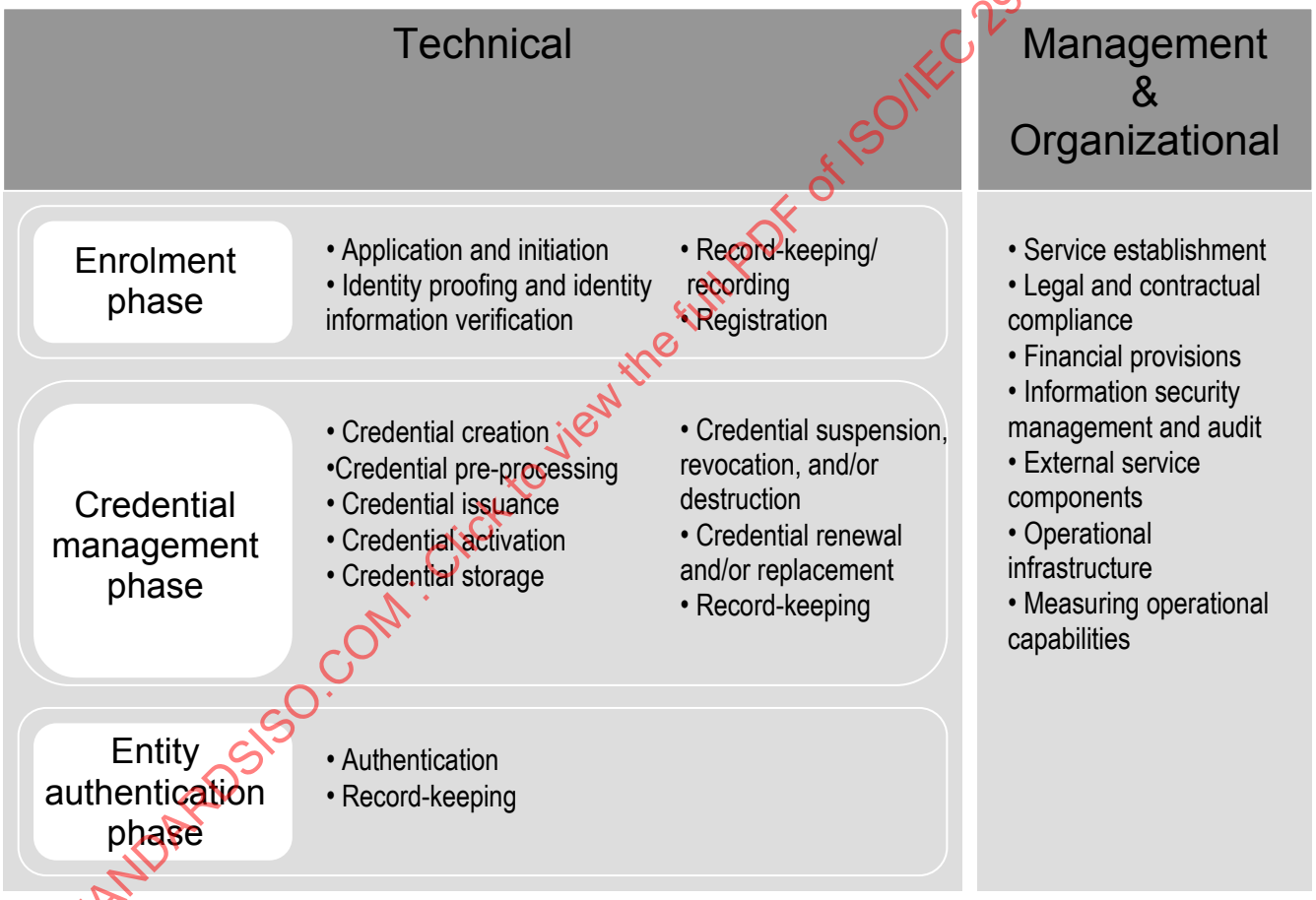

Figure 1 — Overview of the Entity Authentication Assurance Framework

Using four specified Levels of Assurance (LoAs), this 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 International Standard provides informative guidance concerning the protection of personally identifiable information (PII) associated with the authentication process.

This International Standard is intended to be used principally by credential service providers (CSPs) and by others having an interest in their services (e.g., relying parties, assessors and auditors of those services). This Entity Authentication Assurance Framework (EAAF) specifies the minimum technical, management, and process requirements for four LoAs to ensure equivalence among 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 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.

Information technology — Security techniques — Entity authentication assurance framework

1 Scope

This 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 documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

2.1 Identical Recommendations | International Standards

None.

2.2 Paired Recommendations | International Standards

None.

2.3 Additional references

None.

3 Terms and definitions

For the purposes of this document, the following terms and 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 International Standard, an assertion is considered to be a stronger statement than a claim.

3.2
authentication
provision of assurance in the identity of an entity

[ISO/IEC 18014-2]

3.3
authentication factor
piece of information and/or 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 perform authentication of an entity

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 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 a claimed or asserted identity and/or entitlements

NOTE See Annex B for additional characteristics of a credential.

3.9
credential service provider
trusted actor that issues and/or manages credentials

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 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 is, or is expected to be

[ITU-T X.1252]

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

3.12
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 can have one or more identifiers to allow an entity to be uniquely recognized within that context.

3.14
identity information verification
process of checking identity information and credentials against issuers, data sources, or other internal or external resources with respect to authenticity, validity, correctness, and binding to the entity

3.15
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

3.16
man-in-the-middle attack
attack in which an attacker is able to read, insert, and modify messages between two parties without their knowledge

3.17
multifactor authentication
authentication with at least two independent authentication factors

[ISO/IEC 19790]

3.18
mutual authentication
authentication of identities of entities which provides both entities with assurance of each other's identity

3.19
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

[ITU-T X.1252]

3.20
phishing
scam by which an email user is duped into revealing personal or confidential information which the scammer can then use illicitly

3.21
registration authority
trusted actor that establishes and/or vouches for the identity of an entity to a CSP

3.22
relying party
actor that relies on an identity assertion or claim

3.23
repudiation
denial in having participated in all or part of an action by one of the entities involved

[ITU-T X.1252]

3.24
salt
non-secret, often random, value that is used in a hashing process

NOTE It is also referred to as sand.

3.25
shared secret
secret used in authentication that is known only to the entity and the verifier

3.26
time stamp
reliable time variant parameter which denotes a point in time with respect to a common reference

3.27
transaction
discrete event between an entity and service provider that supports a business or programmatic purpose

3.28
trust framework
set of requirements and enforcement mechanisms for parties exchanging identity information

3.29
trusted third party
authority or its agent, trusted by other actors with respect to specified activities (e.g., security-related activities)

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

3.30
validity period
time period during which an identity or credential may be used in one or more transactions

3.31
verification
process of checking information by comparing the provided information with previously corroborated information

3.32
verifier
actor that corroborates identity information

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

4 Abbreviations

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

CAs	Certificate Authorities
CSP	Credential Service Provider
CV	Card Verifier
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 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; and

d) “Can” indicates a possibility and capability.

6 Levels of assurance

This Entity Authentication Assurance Framework (EAAF) defines four levels of assurance (LoAs) for entity authentication. Each LoA describes the degree of confidence in the processes leading up to and including the authentication process itself, thus providing assurance that the entity that uses a particular identity is in fact the entity to which that identity was assigned. For the purposes of this International Standard, LoA is a function of the processes, management activities, and technical controls that have been implemented by a CSP for each of the EAAF phases based on the criteria set forth in Clause 10. Entity Authentication Assurance (EAA) is affected by management and organizational considerations, but this International 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 the LoAs of all components that make up the network and includes NPEs or endpoint devices (e.g., mobile phones, PDAs, set-top boxes, laptops). In some instances, endpoint devices may impersonate legitimate entities. Consequently, the ability to distinguish a trusted device, with some degree of confidence, from a rogue device is fundamental to EAA.

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

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

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

b) Credential management (e.g., credential issuance, credential activation); 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 claimed or asserted identity
2 – Medium	Some confidence in the claimed or asserted identity
3 – High	High confidence in the claimed or asserted identity
4 – Very high	Very high confidence in the claimed or asserted identity

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

6.1 Level of assurance 1 (LoA1)

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

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

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

6.2 Level of assurance 2 (LoA2)

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

For example, a service provider might operate a website that enables its customers to change their address of record. The transaction in which a beneficiary changes an address of record may be considered a LoA2 authentication transaction, as the transaction may involve a moderate risk of inconvenience. Since official notices regarding payment amounts, account status, and records of changes are usually sent to the beneficiary's address of record, the transaction additionally entails moderate risk of unauthorized release of PII. As a result, the service provider should obtain at least some authentication assurance before allowing this transaction to take place.

6.3 Level of assurance 3 (LoA3)

At LoA3, there is high confidence in the claimed or asserted identity of the entity. This LoA is used where substantial risk is associated with erroneous authentication. This LoA shall employ multifactor authentication. Any secret information exchanged in authentication protocols shall be cryptographically protected in transit

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

and at rest (although LoA3 does not require the use of a cryptographic-based challenge-response protocol). There are no requirements concerning the generation or storage of credentials; they may be stored or generated in general purpose computers or in special purpose hardware.

For example, a transaction in which a company submits certain confidential information electronically to a government agency may require a LoA3 authentication transaction. Improper disclosure could result in a substantial risk for financial loss. Other LoA3 transaction examples include online access to accounts that allow the entity to perform certain financial transactions, or use by a third party contractor of a remote system to access potentially sensitive client personal information.

6.4 Level of assurance 4 (LoA4)

At LoA4, there is very high confidence in the claimed or asserted identity of the entity. This LoA is used when high risk is associated with erroneous authentication. LoA4 provides the highest level of entity authentication assurance defined by this International 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 in transit and at rest.

For example, services where there is a potential high risk for harm or distress in case of an authentication failure may require LoA4 protection. The responsible party needs full assurance that the correct entity provided certain critical information, and the responsible party may even be criminally liable for any failure to verify the information. Finally, approval of a transaction involving high risk of financial loss may be 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. Table 6-2 indicates possible consequences and impacts of authentication failure at the various LoAs.

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

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

Determination of what constitutes minimum, moderate, substantial, and high risk depends on the risk criteria defined by the organization using this standard for each of the possible consequences. Additionally, it is possible to have multiple impact scenarios (e.g., consequences could include harm to the organization, as

well as, unauthorized release of sensitive information). In multiple impact scenarios, the highest LoA corresponding to consequences should be used.

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

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

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

6.6 LoA mapping and interoperability

Different domains may define LoAs differently. These LoAs will not necessarily support a 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) Impacts (i.e., min, mod) should threats become reality;

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

d) Recommended security technologies and processes for use in implementing controls at each LoA, such as specifying a credential 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 LoAs for which it has been certified capable of meeting the requirements associated with that LoA.

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

While digital certificates are an established way to convey information concerning 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 attest to its own identity. It is also possible that there is a separate party representing the entity for the purposes of authentication.

7.2 Credential service provider

A credential service provider (CSP) issues and/or manages credentials or the hardware, software, and associated data that can be used to produce credentials. Passwords and biometric 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 vouches for the identity of an entity to a CSP. The RA shall be trusted by the CSP to execute the processes related to the enrolment phase and register entities in a way that allows later assignment of credentials by the CSP.

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

7.4 Relying party

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

7.5 Verifier

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

7.6 Trusted third party

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

8 Entity authentication assurance framework phases

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

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

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

b) Requirements for external or third party assessment of an organization's operational capability within the EAAF; 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 information verification; and record-keeping/recording. These processes may be conducted entirely by a single organization, or they may consist of a variety of relationships and capabilities provided by a number of organizations including shared or interacting components, systems, and services.

The required processes differ according to the rigor required by the applicable LoA. In the case of an entity enrolling under LoA1, these processes are minimal (e.g., an individual may click a “new user” button on a webpage and create a username and password). In other cases, enrolment processes may be extensive. For example, enrolment at LoA4 requires an in-person meeting between the entity and the RA, as well as extensive identity proofing.

8.1.1 Application and initiation

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

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

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

8.1.2 Identity proofing and identity information verification

Identity proofing is the process of capturing and verifying sufficient information to identify an entity to a specified or understood level of assurance. Identity information verification is the process of checking identity information and credentials against issuers, data sources, or other internal or external resources with respect to authenticity, validity, correctness, and binding to the entity. Depending on the context, a variety of identity information (e.g., government identity cards, driver’s 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 identity proofing requirements shall be more stringent the higher the LoA. Also, the identity proofing process shall be more stringent for entities asserting or claiming an identity remotely (e.g., via an online channel) than locally (e.g., in-person with the RA).

The stringency of identity proofing requirements is based on the objectives that must be met for each LoA. At LoA1, the only objective is to ensure the identity is unique within the intended context. The identity should not be associated with two different entities. At LoA2, there are two objectives. First, the identity shall be unique in the context. Second, the entity to which the identity pertains shall exist objectively, which means the identity is not fictitious or intentionally fabricated for fraudulent purposes.[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

2 This does not preclude the use of pseudonyms.

the entity in possession of a birth certificate is the entity to which the birth certificate relates). Similarly, identity proofing at LoA2 for NPEs may include checking a serial number with the manufacturer.

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

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

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 claimed or asserted identity	Identity is unique within a context	Self-claimed or self-asserted	Local or remote
LoA2 - medium	Some confidence in the claimed or asserted identity	Identity is unique within context and the entity to which the identity pertains exists objectively	Proof of identity through use of identity information from an authoritative source	Local or remote
LoA3 - high	High confidence in the claimed or asserted identity	Identity is unique within context, entity to which the identity pertains exists objectively, identity is verified, and identity is used in other contexts	Proof of identity through use of identity information from an authoritative source + identity information verification	Local or remote
LoA4 – very high	Very high confidence in the claimed or asserted identity	Identity is unique within context, entity to which the identity pertains exists objectively, identity is verified, and identity is used in other contexts	Proof of identity through use of identity information from multiple authoritative sources + identity information verification + entity witnessed in-person[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 information 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

[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.

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

overview of the identity information, sources, and/or issuers that are relied upon in support of the enrolment phase.

8.1.3 Record-keeping/recording

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

8.1.4 Registration

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

8.2 Credential management phase

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

8.2.1 Credential creation

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

8.2.2 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.

8.2.2.1 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.

8.2.2.2 Credential binding

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

8.2.3 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.

8.2.4 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.

8.2.5 Credential storage

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

8.2.6 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 by organizational policy. At higher LoAs, the time period permitted for revocation is usually shorter. Some credentials, such as those held on smart cards, can be physically destroyed upon revocation. However, the information associated with the credential cannot always be destroyed.

8.2.7 Credential renewal and/or replacement

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

8.2.8 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 for every (applicable) process involved in the credential management phase. Where credentials are issued to human entities, the keeping of records is likely to involve the processing of PII. See Annex A.

8.3 Entity authentication phase

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

8.3.1 Authentication

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

8.3.2 Record-keeping

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

Where human entities are concerned, the information contained in these records may include sensitive information. These records shall be managed in a manner that takes into account the need for protection and minimization of PII. See also 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 International 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 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 between one another. Depending on the agreements, additional actors may be called on to ensure that all actors are abiding by commitments and may provide an avenue for redress in the event they are not.

9.7 Measuring operational capabilities

Policy makers set out the technical and contractual requirements for trust frameworks. Technical requirements might include, for example, product version levels, system configuration, settings, and protocols, while contractual requirements might be geared 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 International 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

10.1.1 Enrolment phase threats

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

Table 10-1 – Threats to the enrolment phase

Threat	Examples
Impersonation	Some examples of impersonation are when an entity illegitimately uses another entity's identity information by using a forged driver's license describing an individual who does not exist or when a device registers with a network using a spoofed Media Access Control (MAC) address.

10.1.2 Required LoA controls to protect against enrolment phase threats

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

Table 10-2 – Enrolment phase controls for each LoA

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

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

10.1.2.1 Controls against enrolment phase threats

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

IdentityProofing: PolicyAdherence

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

IdentityProofing: InPerson

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

IdentityProofing: AuthoritativeInformation

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

#4. The following controls apply:

- All controls from #3

In addition:

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

  a) For humans:

     i. In-person:

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

     ii. Not-in-person:

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

  b) For NPEs:

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

#5. The following controls apply:

- All controls from #4.

In addition:

a) For humans:

i. In-person:

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

ii. Not-in-person:

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

b) For NPEs:

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

#6. The following controls apply:

- All controls from #5.

  In addition:

  a) For humans:

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

  b) For NPEs:

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

- Any changes in the binding arrangements between devices shall be managed through the RA. Where possible, the network management capability should alert the RA or network management of any changes in device relationships and corrective action taken;
- Capability shall be in place to prevent any altered device relationships from working; and
- LoA4 software code shall be digitally signed with a LoA4, human-issued credential and shall be counter-signed by the RA as proof of acceptance before being taken into use.

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

10.2.1 Credential management threats

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

Table 10-3 – Credential Management Threats

Threat	Examples
CredentialCreation: Tampering	An attacker alters information as it passes from the enrolment process to the credential creation process.
CredentialCreation: UnauthorizedCreation	An attacker causes a CSP to create a credential based on a fictitious entity.
CredentialIssuance: Disclosure	A credential created by the CSP for an entity is copied by an attacker as it is transported from the CSP to the entity during credential establishment.
CredentialActivation: Unauthorized Possession	An attacker obtains a credential that does not belong to him/her and by masquerading as the rightful entity causes the CSP to activate the credential.
CredentialActivation: Unavailability	1. The entity associated with a credential, or the means to generate the credential, is not in the usual location and is unable to adequately authenticate its identity to the CSP. 2. Delivery of a credential, or means to generate the credential, is delayed, and activation within the prescribed period is not possible.
CredentialStorage: Disclosure	Credentials stored in a system file are revealed. For example, a stored record of usernames and passwords is accessed by an attacker.
CredentialStorage: Tampering	The file that maps usernames to credentials is compromised so that the mappings are modified, and existing credentials are replaced by credentials to which the attacker has access.
CredentialStorage: Duplication	An attacker uses stored information to create a duplicate credential (e.g. by duplicating a smart card that can generate the credential) that can be used by an unauthorized entity.
CredentialStorage: DisclosureByEntity	The entity keeps a written record of the username and password in a place that can be accessed by others.
CredentialRevocation: DelayedRevocation	The dissemination of revocation information is not timely leading to a threat of entities with revoked credentials still being able to authenticate before the credential verifier updates the latest revocation information.
CredentialRevocation: UseAfterDecommissioning	User accounts are not deleted when employees leave a company leading to possible misuse of the old accounts by unauthorized persons. A credential stored in a hardware device is used after its cryptographic keys have been revoked.
CredentialRenewal: Disclosure	Credential renewed by the CSP for an entity is copied by an attacker as it is transported.
CredentialRenewal: Tampering	A new credential created by an entity is modified by an attacker as it is being submitted to the CSP to replace an expired credential.

Threat	Examples
CredentialRenewal: UnauthorizedRenewal	An attacker is able to take advantage of a weak credential renewal protocol to extend the credential validity period for a current entity. An attacker fools the CSP into issuing a new credential for a current entity, and the new credential binds the current entity's identity to a credential provided by the attacker. For NPE entities, an example can be re-labeling (re-issuing) a system component (e.g., RAM) as new after it has been used.
CredentialRecordkeeping: Repudiation	An entity asserts or claims that a legitimate credential is fraudulent or contains incorrect information in order to falsely deny having used the credential.

10.2.2 Required LoA controls to protect against credential management phase threats

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

Table 10-4 – Credential management controls for each LoA

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

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

10.2.2.1 Controls against credential management phase threats

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

AppropriateCredentialCreation

#1. The following controls apply:

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

#2. The following controls apply:

- All controls from #1.

  In addition:

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

  a) Digital signatures; or

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

HardwareOnly

#3. Credentials shall be contained on a hardware security module.[5]

StateLocked

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

TrackedInventory

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

AppropriateCredentialIssuance

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

#7. The following controls apply:

---

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

- All controls from #6.

  In addition:

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

#8. The following controls apply:

- All controls from #7.

  In addition:

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

ActivatedByEntity

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

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

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

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

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

CredentialSecureStorage

#12. The following controls apply:

- Credentials based on shared secrets shall be protected by access controls that limit access to only those administrators and applications that require access; and

- Protection policy for stored credentials shall be described in the documentation associated with the use of those credentials that is made available to entities.

#13. The following controls apply:

- All controls from #12.

  In addition:

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

#14. The following controls apply:

- All controls from #13

  In addition:

- Shared secrets shall be protected by access controls that limit access to only those administrators and applications that require access. Such shared secrets shall be encrypted. The encryption key for the shared secret shall itself be encrypted and stored in a cryptographic module (hardware or software). The encryption key for the shared secret shall be decrypted only as immediately required for an authentication operation; and

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

#15. The following controls apply:

- All controls from #14.

  In addition:

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

CredentialSecureRevocation&Destruction

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

CredentialSecureRenewal

#17. The following controls apply:

- The CSP shall establish suitable policies for renewal and replacement of credentials;

- Proof-of-possession of the unexpired current credential shall be demonstrated by the entity prior to the CSP allowing renewal and/or replacement;

- Passwords shall meet minimum CSP policy requirements for password strength and re-use;

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

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

#18. The following controls apply:

- All controls from #17.

  In addition:

- Perform an LoA2 identity proofing in accordance with 10.1.2.1 (IdentityProofing: PolicyAdherence, IdentityProofing: AuthoritativeInformation).

#19. The following controls apply:

- All controls from #17.

  In addition:

- Perform an LoA3 identity proofing in accordance with 10.1.2.1 (IdentityProofing: PolicyAdherence, IdentityProofing: AuthoritativeInformation).

RecordRetention

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

#21. The following controls apply:

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

10.3 Threats to, and controls for, the authentication phase

10.3.1 Authentication phase threats

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

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

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

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

Threat	Description and examples
General threats	General threats to authentication include many categories of security threats common to any type of ICT. Some examples include keystroke loggers, social engineering, and user errors. Except for the use of multifactor authentication, controls against these threats are beyond the scope of this standard. Note that multifactor authentication does not protect against all possible general threats.
OnlineGuessing	An attacker performs repeated logon attempts by guessing possible values of the credential.

Threat	Description and examples
OfflineGuessing	Secrets associated with credential generation are exposed using analytical methods outside the authentication transaction. Password cracking often relies upon brute force methods, such as the use of dictionary attacks. With dictionary attacks, an attacker uses a program to iterate through all of the words in a dictionary (or multiple dictionaries in different languages), computes the hash value for each word, and checks the resultant hash value against the database. The use of rainbow tables is another password cracking method. Rainbow tables are pre-computed tables of clear text/hash value pairs. Rainbow tables are quicker than brute-force attacks because they use reduction functions to decrease the search space. Once generated or obtained, rainbow tables can be used repeatedly by an attacker.
CredentialDuplication	The entity's credential, or the means to generate credentials, has been illegitimately copied. An example would be the unauthorized copying of a private key.
Phishing	An entity is lured to interact with a counterfeit verifier, and tricked into revealing his or her password or sensitive personal data that can be used to masquerade as the entity. An example is when an entity is sent an email that redirects him or her to a fraudulent website and asks the user to log in using his or her username and password.
Eavesdropping	An attacker listens passively to the authentication transaction to capture information which can be used in a subsequent active attack to masquerade as the entity.
ReplayAttack	An attacker is able to replay previously captured messages (between a legitimate entity and an RP) to authenticate as that entity to the RP.
SessionHijack	An attacker is able to insert himself or herself between an entity and a verifier subsequent to a successful authentication exchange between the latter two parties. The attacker is able to pose as an entity to the relying party or vice versa to control session data exchange. An example is when an attacker is able to take over an already authenticated session by eavesdropping on or predicting the value of authentication cookies used to mark HTTP requests sent by the entity.
ManInTheMiddle	The attacker positions himself or herself between the entity and relying party so that he or she can intercept and alter the content of the authentication protocol messages. The attacker typically impersonates the relying party to the entity and simultaneously impersonates the entity to the verifier. Conducting an active exchange with both parties simultaneously may allow the attacker to use authentication messages sent by one legitimate party to successfully authenticate to the other.
CredentialTheft	A device that generates or contains credentials is stolen by an attacker.
SpoofingAndMasquerading	Spoofing and masquerading refer to situations in which an attacker impersonates another entity in order to allow the attacker to perform an action he would otherwise not be able to perform (e.g., gain access to an otherwise inaccessible asset). This may be done by making use of the credential(s) of an entity or otherwise posing as an entity (e.g., by forging a credential). Some examples are when an attacker impersonating an entity spoofs one or more biometric characteristics by creating a "gummy" finger that matches the pattern of the entity; an attacker spoofs a MAC address by having its device broadcast a MAC address that belongs to another device that has permissions on a particular network; or an attacker poses as a legitimate software publisher responsible for downloading on-line software applications and/or updates.

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

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

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

Threats	Controls	Required controls				
		LoA*	LoA1	LoA2	LoA3	LoA4
General**	MultiFactorAuthentication				#1	#1
OnlineGuessing	StrongPassword CredentialLockOut DefaultAccountUse AuditAndAnalyze	#2 #3 #4 #5				
OfflineGuessing	HashedPasswordWithSalt	#6				
CredentialDuplication	AntiCounterfeiting	#7				
Phishing	DetectPhishingFromMessages AdoptAntiPhishingPractice MutualAuthentication	#8 #9 #10				
Eavesdropping	NoTransmitPassword EncryptedAuthentication DifferentAuthenticationParameter	#11 #12 #13				
ReplayAttack	DifferentAuthenticationParameter Timestamp PhysicalSecurity	#13 #14 #15				
SessionHijacking	EncryptedSession FixProtocolVulnerabilities CryptographicMutualHandshake	#16 #17 #18				
ManInTheMiddle	MutualAuthentication EncryptedSession	#10 #16				
CredentialTheft	CredentialActivation	#19				
SpoofingAndMasquerading	CodeDigitalSignature LivenessDetection	#20 #21				

Threats	Controls	Required controls				
		LoA*	LoA1	LoA2	LoA3	LoA4
LoA* - These controls should be applied as determined necessary by a risk assessment. General** - Not all of the general threats can be resisted by multifactor authentication.						

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

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

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

MultiFactorAuthentication

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

StrongPassword

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

CredentialLockout

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

DefaultAccountUse

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

AuditAndAnalyze

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

HashedPasswordWithSalt

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

Anticounterfeiting

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

DetectPhishingFromMessages

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

AdoptAntiPhishingPractice

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

MutualAuthentication

#9. Mutual authentication shall be used.