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.

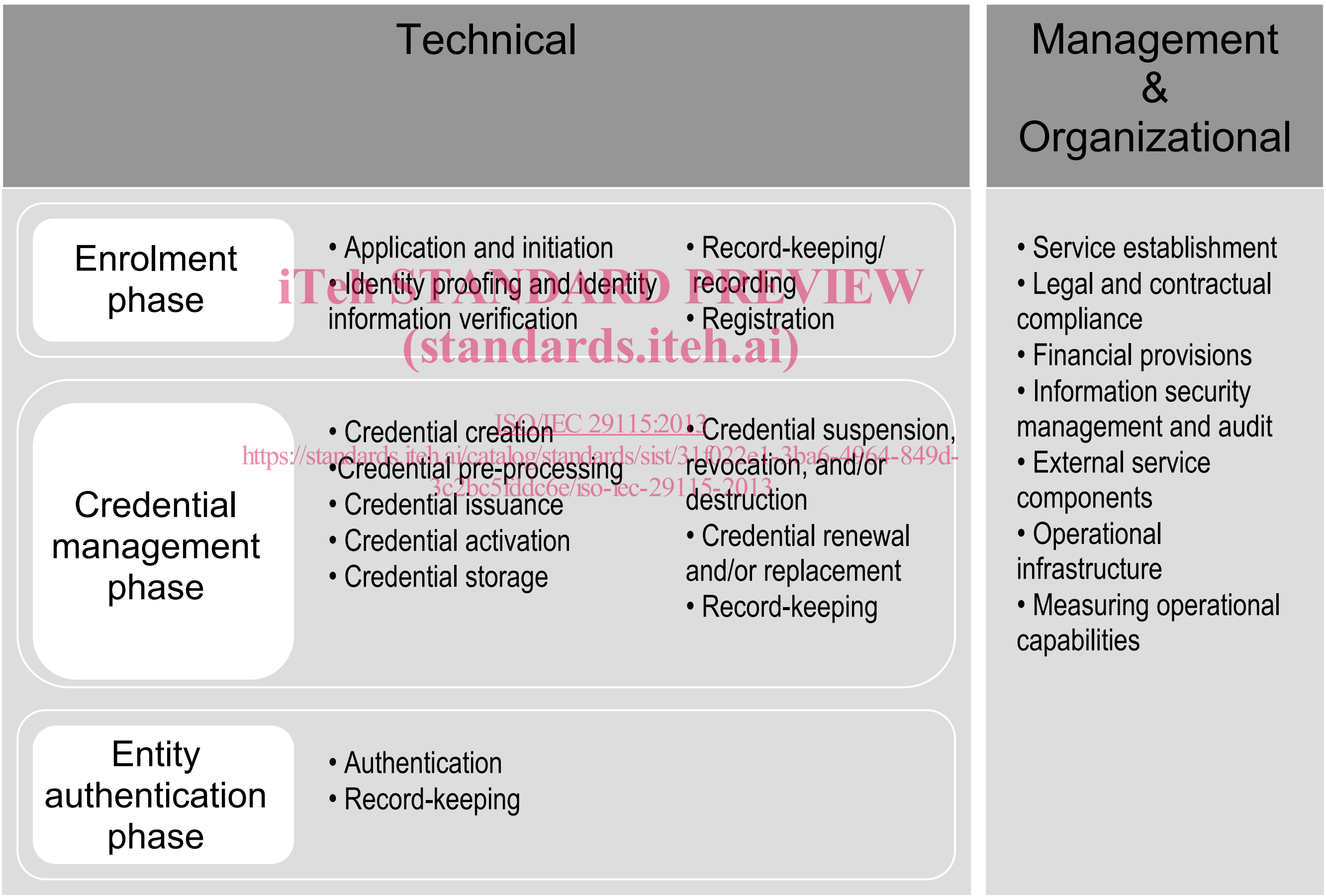
Technical
Management & Organizational
Enrolment phase
• Application and initiation
• Identity proofing and identity information verification
• Record-keeping/ recording
• Registration
Credential management phase
• Credential creation
•Credential pre-processing
• Credential issuance
• Credential activation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

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.