FINAL
DRAFT

AMENDMENT

ISO/IEC 24760-1:2011 FDAM 1

ISO/IEC JTC **1**/SC **27**

Secretariat: DIN

Voting begins on:
2018-08-09

Voting terminates on:
2018-10-04

Information technology — Security techniques — A framework for identity management —

Part 1: Terminology and concepts

AMENDMENT 1: Additional terminology and concepts

Technologies de l'information — Techniques de sécurité — Cadre pour la gestion de l'identité —

Partie 1: Terminologie et concepts

AMENDEMENT 1: Terminologie et concepts additionnels

Reference number
ISO/IEC 24760-1:2011/FDAM 1:2018(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

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

A list of all parts in the ISO/IEC 24760 series can be found on the ISO website.

Information technology — Security techniques — A framework for identity management —

Part 1:
Terminology and concepts

AMENDMENT 1: Additional terminology and concepts

Normative references

Add the following normative reference:

> ISO/IEC 24760-2, *Information technology — Security techniques — A framework for identity management — Part 2: Reference architecture and requirements*

3.1.1

Replace with the following:

3.1.1
entity
item relevant for the purpose of operation of a domain (3.2.3) that has a separate and distinct existence

Note 1 to entry: An entity may have a physical or a logical embodiment.

EXAMPLE A person, an organization, a device, a group of such items, a human subscriber to a telecom service, a SIM card, a passport, a network interface card, a software application, a service or a website.

3.1.3

Remove Note 3 to the terminological entry.

3.1.3

Replace with the following:

3.1.3
attribute
characteristic or property of an *entity* (3.1.1)

3.1.4

Replace with the following:

3.1.4
identifier
attribute or set of *attributes(3.1.3)* that uniquely characterizes an identity (3.1.2) in a domain (3.2.3)

Note 1 to entry: An identifier may be a specifically created attribute with a value assigned to be unique within the domain.

3.1.5

Replace with the following*:*

3.1.5
domain of origin
domain (3.2.3) where an attribute (3.13) value was created or its value has been (re)assigned

Note 1 to entry: The domain of origin may be provided as meta data for an attribute.

Note 2 to entry: The domain of origin typically specifies the meaning and format of the attribute value. Such specification may be based on international standards.

Note 3 to entry: An attribute may contain an explicit value that references the domain of origin, e.g. an ISO country code for a passport number as reference to the issuing country that is the domain of origin of identity information in the passport.

Note 4 to entry: Operationally, a domain of origin may be available as an authoritative source for an attribute (sometimes known as the Attribute Authority). An authoritative source may be operated outside the actual domain of origin. Multiple authoritative sources may exist for the same domain of origin.

EXAMPLE The domain of origin of a club-membership number is the specific club that assigned the number.

3.1.7

Add new terminological entry as follows:

3.1.7
principal
subject
entity (3.1.1) of which identity information is stored and managed by an *identity management system* (3.4.8)

Note 1 to entry: Typically, in a context of privacy protection or where a principal is seen as having agency a principal refers to a person.

[SOURCE: ISO/IEC 24760-2:2015, 3.4, modified — The sense of the word “pertains” has been clarified and Note 1 has been reworded.]

3.2.2

Replace with the following:

3.2.2
verification
process of establishing that identity information (3.2.5) associated with a particular *entity* (3.1.1) is correct

Note 1 to entry: Verification typically involves determining which attributes are needed to recognize an entity in a domain, checking that these required attributes are present, that they have the correct syntax, and exist within a defined validity period and pertain to the entity.

3.2.3

Remove DA as admitted term.

3.3

Change the title as follows:

3.3 Authenticating identity information

3.3.1

Remove Note 3 to the terminological entry.

3.3.5

Replace with the following:

3.3.5
credential
representation of an identity (3.1.2) for use in authentication (3.2.1)

Note 1 to entry: As described in 5.4, customary embodiments of a credential are very diverse. To accommodate this wide range, the definition adopted in this document is very generic.

Note 2 to entry: A credential is typically made to facilitate *data* authentication of the identity information pertaining to the identity it represents. Data authentication is typically used in authorization.

Note 3 to entry: The identity information represented by a credential can, for example, be printed on human-readable media, or stored within a physical token. Typically, such information can be presented in a manner designed to reinforce its perceived validity.

Note 4 to entry: A credential can be a username, username with a password, a PIN, a smartcard, a token, a fingerprint, a passport, etc.

3.3.9

Delete the terminological entry.

3.3.9
identity assurance
(withdrawn)

3.4.2

Replace with the following:

3.4.2
identity proofing
verification (3.2.2) based on *identity evidence* (3.4.4) aimed at achieving a specific level of assurance

Note 1 to entry: Identity proofing is typically performed as part of enrolment. Identity evidence may also be needed during maintenance of registered identity information, e.g. recovery of a user account.

Note 2 to entry: Typically identity proofing involves a verification of provided identity information and may include uniqueness checks, possibly based on biometric techniques.

Note 3 to entry: Verification for identity proofing is usually based on an enrolment policy that includes specification of the verification criteria of the identity evidence to be provided by the entity.

Note 4 to entry: The verified identity information obtained when performing identity proofing may be included in the registration and may serve to facilitate future identification of the entity.

3.4.3

Replace Note 1 with the following text:

Note 1 to entry Enrolment typically comprises the collection and validation of identity information for identification of an entity and the collection of the identity information required for *identity registration* (3.4.6), followed by identity registration itself.

Delete Note 2 to the terminological entry.

3.4.4

Replace with the following:

3.4.4
identity evidence
evidence of identity
information that can support validating identity information

Note 1 to entry: Identity evidence is the presented and gathered information related to an entity that provides the attributes needed for a successful identification or authentication at a specific (high) level of assurance.

3.4.5

Replace the definition with the following text:

repository of *identities* (3.1.2)

Replace Note 3 with the following text:

Note 3 to entry The reliability of the identity information in an identity register is determined by the identity proofing policies used during enrolment.

3.4.6

Add “registration” as an admitted term.

3.4

Add new terminological entries as follows:

3.4.8
identity management system
mechanism comprising of policies, procedures, technology and other resources for maintaining identity information including associated metadata

Note 1 to entry: An identity management system is typically used for identification or authentication of entities. It can be deployed to support other automated decisions based on identity information for an entity recognized in the domain for the identity management system.

3.4.9
registration authority
RA
entity (3.1.1) related to a particular domain (3.2.3) responsible for enrolment (3.4.3), identity proofing (3.4.2) and identity registration (3.4.6)

3.4.10
credential issuer
entity (3.1.1) responsible for provisioning of a *credential* (3.3.5) to a *principal* (3.1.7) in a specific domain (3.2.3)

Note 1 to entry: A credential provisioned by an issuer can have a physical form, e.g. a membership (smart) card.

Note 2 to entry: The issuance of a credential for a principal can be recorded as an attribute for the principal, e.g. by recording the unique number of the token issued.

Note 3 to entry: A credential provisioned by an issuer may be a username and password. A credential in the form of a smart card or similar secure device, can be configured to validate a password off-line.

3.4.11
credential service provider
CSP
trusted *entity* (3.1.1) related to a particular domain (3.2.3) responsible for management of *credentials* (3.3.5) issued in that domain

Note 1 to entry: It is possible that a CSP acts as credential *issuer* (3.4.10).

3.5.1

Replace with the following:

3.5.1
federated identity
identity (3.1.2) for use in multiple domains (3.2.3)

Note 1 to entry: Some or all of the domains where a federated identity can be used may be formally joined as an identity federation. Identity information providers of domains in the federation may jointly manage a federated identity.

Note 2 to entry: The federated identity can be persistent or be a temporary one.

3.5.3

Delete the terminological entry.

3.5.3
single-sign-on identity
(withdrawn)