INTERNATIONAL STANDARD

ISO/IEC 24760-1

Second edition
2019-05

AMENDMENT 1
2023-01

IT Security and Privacy — A framework for identity management —

Part 1: Terminology and concepts

AMENDMENT 1

Reference number
ISO/IEC 24760-1:2019/Amd. 1:2023(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
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.

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 or www.iec.ch/members_experts/refdocs).

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) or the IEC list of patent declarations received (see https://patents.iec.ch).

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. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

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

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 and www.iec.ch/national-committees.

IT Security and Privacy — A framework for identity management —

Part 1: Terminology and concepts

AMENDMENT 1

3.1

Add the following two entries:

3.1.8
readily-verifiable identifier
identifier with a value which is constructed to be easily verified as valid and as referring to a known entity

EXAMPLE The result of solving a cryptographic puzzle with its input can easily be validated as correct, functioning as digital signature on that input.

Note 1 to entry: A readily verifiable identifier can be used as an authenticator.

3.1.9
authoritative identifier
unique identifier referring to an entity, known in a well-trusted domain of origin

Note 1 to entry: An authoritative identifier is typically managed by a well-known organization, e.g. a government.

3.2

Add the following term:

3.2.5
access token
trusted object encapsulating the authority for a principal to access a resource

Note 1 to entry: An access token can be obtained in the result of an authentication.

Note 2 to entry: An access token may contain access permission information for a subject to access the resource and identifying information for the authority of the authorization decision.

Note 3 to entry: An access token may contain information that enables its integrity to be validated.

Note 4 to entry: An access token may take a physical or a virtual form.

[SOURCE: ISO/IEC 29146:2016, 3.3, modified —replaced the word 'subject' by 'principal', and replaced Note 1 to entry.]

3.3

Add the following entries:

3.3.9
authentication factor
distinguishing feature of an authenticator to characterise its use in authentication

Note 1 to entry: Four different authentication factors can be recognized:

— cognition factor, any credential that is formed by something that the principal knows and can reproduce (exclusively): a personal secret;

— possession factor, any credential that is formed by something that the principal possesses, e.g. an authenticator;

— inherent factor, any credential that is formed by a description of something that is inherent to the physical existence of the principal, e.g. a biometric characteristic such as fingerprint, facial image, or 1, iris pattern;

— behaviour factor, any credential that is formed by a description of something that the principal typically does, e.g. a behaviour pattern.

3.3.10
multi-factor authentication
authentication in which multiple authenticators are used of two or more authentication factors

Note 1 to entry: If two or more authenticators are being used in authentication that have the same authentication factor, they should have been issued by different credential issuers.

Note 2 to entry: Using multiple authenticators (that differ in authentication factor can enhance the security of the authentication as that could prompt the principal to act differently with each of them.

[SOURCE: ISO/IEC 19790:2012, 3.74, modified — definition and notes revised to match terminology context.]

3.3.11
authenticator
representation of an entity to demonstrate it is known in a domain of origin

EXAMPLE One-time password (OTP) generator token, transaction authentication number (TAN) generator token, an electronic (identity) card or a mobile phone application with one or more of these functions.

Note 1 to entry: An authenticator can have a physical form, which can be under exclusive operational control of a principal.

Note 2 to entry: As a physical device an authenticator can provide a cryptographically strong identifier for the principal, which can be a pseudonym or ephemeral.

Note 3 to entry: An authenticator is intended to be used by the principal to provide input on its behalf during authentication functioning as a possession factor.

Note 4 to entry: An authenticator can be provided to a principal by a credential issuer which is unrelated to the domain of origin. Upon enrolment in a domain of origin of a principal who has such a third-party authenticator, the (pseudonymous) identifier of the authenticator is typically recorded as attribute for the principal.

Note 5 to entry: An authenticator can either be unconnected, or connected through a computer interface, e.g. a USB port, or can be integrated with a user device, e.g. as application in a smart phone. As a mobile application it could use a secure element in the phone to protect cryptographic secrets or a personal secret.

Note 6 to entry: While under operational control of the principal, an authenticator can also be under secure, remote functional control of its issuer, e.g. to update functional parameters or refresh cryptographic keys.

3.3.12
one-time password
OTP
single-use value randomly generated for use in authentication

Note 1 to entry: An authenticator may be configured to generate a one-time password, typically after its operator has entered a personal secret.

3.3.13
personal secret
knowledge exclusive to a principal that can be validated in a domain of origin where the principal is known

EXAMPLE A password, PIN, selecting pictures from a presented randomized grid with a type of content pre-arranged with the credential issuer.

Note 1 to entry: Each different type of personal secret has an establishment procedure implemented by the credential issuer to provide an associated identity information authority with the information required for future validation.

Note 2 to entry: Each different type of personal secret has a verification procedure implemented by the identity information authority associated with the credential issuer to verify that knowledge based on securely stored information.

Note 3 to entry: In general, data communication during the process to establish or validate a personal secret as a credential is cryptographically protected, e.g. with HTTPS.

3.4

Add the following entries:

3.4.12
entity authentication assurance
assertion that the reliability of identity information pertains to a particular entity

3.4.13
level of assurance
description of the strength of entity authentication assurance

Note 1 to entry: ISO/IEC 29115:2013 specifies multiple levels of assurance.

3.4.14
principal's personal identity management system
PPI
mobile identity
identity management system holding identity information for a single principal, operated by, or under exclusive control of, this principal

Note 1 to entry: The term "mobile identity" has been used, among other concepts, to refer to a PPI, e.g. as implemented on a mobile phone or as a dedicated processing token.

Note 2 to entry: An authenticator can be configured to operate as private IMS for its principal. In that case, some attributes in the identity are exclusively stored in the authenticator, while an external identity information provider may be used for additional attributes, and an external identity information authority may be used to provide (additional) cryptographic assertions on the contained identity information.

Clause 4

Add the following abbreviated terms:

HTTPS	Hypertext transport protocol, secured
OTP	One-time password
PPI	Principal's personal IMS

Clause 5

Add a new subclause after 5.4.1:

5.4.2 Authenticator

An authenticator is a secure device of some kind that is bound to and represents a principal in an authentication process with a relying party.

NOTE 1 Used in multifactor authentication, an authenticator allows to establish higher levels of assurance in the result of an authentication.

NOTE 2 An authenticator is typically realised as an IT device, which can be off-line or online during its use in authentication.

NOTE 3 If implemented as an IT device, an authenticator typically contains a cryptographic secret, e.g. a secret key, and uses that secret in a cryptographic protocol to assert its presence, identity and correctness of other data it can contain.

During authentication, an authenticator can communicate with a device operated by the party relying on the result of the authentication. Additionally, an authenticator can engage in a real-time interaction with the principal that can enhance the level of assurance.

NOTE 4 Typically, the communicate between an authenticator and a relying party during authentication requires the active involvement of the principal, e.g. by copying text in or out of the device or by scanning a QR code.

An authenticator may contain identity information for the principal it represents, which is used during authentication. An authenticator may be configured to be used by multiple principals, in which case it shall only utilize identity information for a single principal during a particular authentication. An authenticator may selectively share some of the information it contains with the relying party with which it interacts in the authentication. An authenticator may support a means for the principal to control which information can be shared. The handling of identity information by an authenticator is beyond the scope of this document.

NOTE 5 ISO/IEC 24760-3:2016, Annex A gives an example of an authenticator being used specifically to selectively and restrictively share identity information with attribute-based credentials.

Renumber the subsequent subclause as 5.4.3.

8.1

At the end of the seventh paragraph, change the last sentence which refers to Clause 9 as follows:

See Clause 9 and ISO/IEC 29146 for requirements on designing access controls.