Date: **2022-~~08-25~~11-04**

ISO/IEC 24760-1:2019/~~DAM~~ Amd. 1:2022(E)

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

Secretariat: **DIN**

IT Security and Privacy —A framework for identity management—Part 1: Terminology and concepts — Amendment 1

Sécurité ~~de l'information, Sécurité cyber~~IT et ~~protection de données personelles~~confidentialité —
Cadre pour la gestion de ~~l’identité,~~l'identité — Partie 1: Terminologie et concepts~~, —~~
Amendement 1~~: Eléments de terminologie~~

~~Copyright notice~~

~~This~~

Style Definition: IneraTableMultiPar: Font: Bold, Font color: Black, French (Switzerland), Tab stops: Not at 19.85 pt + 39.7 pt + 59.55 pt + 79.4 pt + 99.25 pt + 119.05 pt + 138.9 pt + 158.75 pt + 178.6 pt + 198.45 pt

Formatted: English (United States)

Formatted: English (United States)

Formatted: English (United States)

Formatted: English (United States)

Formatted: English (United Kingdom)

Formatted: Line spacing: At least 12 pt, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Line spacing: At least 12 pt, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

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.

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: English (United Kingdom)

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: std_publisher, English (United Kingdom)

Formatted: English (United Kingdom)

Formatted: std_docNumber, English (United Kingdom)

Formatted: English (United Kingdom)

Formatted: std_docPartNumber, English (United Kingdom)

Formatted: English (United Kingdom)

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts — Amendment 1

3.1

Add the following two entries:

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

3.1.8
readily-verifiable identifier
identifier ~~(3.1.4)~~ with a value which is constructed to be easily verified as valid and as referring to a known entity ~~(3.1.1)~~

Formatted: Font: Not Italic

Formatted: Font: Not Italic

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 ~~(3.1.4)~~ referring to an entity ~~(3.1.1),~~, known in a well-trusted domain of origin

Formatted: Font: Not Italic

Formatted: Font: Not Italic

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

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

3.2

Add the following term:

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

3.2.5
access token
trusted object encapsulating the authority for a principal ~~(3.1.7)~~ to access a resource

Formatted: Font: Not Italic

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 ~~(3.3.11)~~ to characterise its use in authentication ~~(3.3.1)~~

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

— cognition factor, any credential ~~(3.3.5)~~ that is formed by something that the principal knows and can reproduce (exclusively): a personal secret ~~(3.3.13);~~;

— 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 ~~(3.3.1)~~ in which multiple authenticators ~~(3.3.11)~~ are used of two or more authentication factors ~~(3.3.9)~~

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 ~~(3.4.10).~~.

Note 2 to entry: Using multiple authenticators (that differ in authentication factor can enhance the security of the authentication ~~(3.3.1)~~ 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 ~~(3.1.1)~~ to demonstrate it is known in a domain of origin ~~(3.1.5)~~

~~EXAMPLES~~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 ~~(3.1.7).~~.

Note 2 to entry: As a physical device an authenticator ~~(3.3.11)~~ can provide a cryptographically strong identifier ~~(3.1.4)~~ for the principal, which can be a pseudonym ~~(3.6.3)~~ or ephemeral ~~(3.6.4).~~.

Note 3 to entry: An authenticator is intended to be used by the principal to provide input on its behalf during authentication ~~(3.3.1)~~ functioning as a possession factor.

Formatted: Default Paragraph Font

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: std_section

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Font: Not Italic

Formatted: Font: Not Italic

Formatted: Font: Not Italic

Formatted: Font: Not Italic

Formatted: Font: Not Italic

Formatted: Font: Not Italic

Formatted: Font: Not Italic

Formatted: Font: Not Italic

Formatted: Font: Not Italic

Formatted: Font: Not Italic

Formatted: Font: Not Italic

Formatted: Font: Not Italic

Formatted: Font: Not Italic

Formatted: Font: Not Italic

Formatted: Font: Not Italic

Formatted: Font: Not Italic

Formatted: Font: Not Italic

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Font: Not Italic

Formatted: Font: Not Italic

Formatted: Font: Not Italic

Formatted: Font: Not Italic

Formatted: Font: Not Italic

Formatted: Font: Not Italic

Formatted: Font: Not Italic

Formatted: Font: Not Italic

Formatted: Font: Not Italic

Formatted: Font: Not Italic

Formatted: Font: Not Italic

Formatted: Font: Not Italic

Formatted Table

Formatted: Font: Bold

Note 4 to entry: An authenticator can be provided to a principal by a credential issuer ~~(3.4.10)~~ 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 ~~(3.1.3)~~ 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 mobile application it could use a secure element in the phone to protect cryptographic secrets or a personal secret ~~(3.3.13).~~.

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 ~~(3.3.1)~~

Note 1 to entry: An authenticator ~~(3.3.11)~~ may be configured to generate a one-time password, typically after its operator has entered a personal secret ~~*(3.3.13)*.~~.

3.3.13
personal secret
knowledge exclusive to a principal ~~(3.1.7)~~ that can be validated in a domain of origin ~~(3.1.5)~~ where the principal is known

~~EXAMPLES~~EXAMPLE A password, PIN, selecting pictures from a presented randomized grid with a type of content pre-arranged with the credential issuer ~~(3.4.10).~~.

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 ~~(3.3.3)~~ 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 ~~(3.2.4)~~ pertains to a particular entity ~~(3.1.1)~~

3.4.13
level of assurance
description of the strength of entity authentication assurance ~~(3.4.12)~~

Formatted: Font: Not Italic
Formatted: Font: Not Italic
Formatted: Font: Not Italic
Formatted: Font: Not Italic
Formatted: Font: Not Italic
Formatted: Font: Not Italic
Formatted: Font: Not Italic
Formatted: Font: Not Italic
Formatted: Font: Not Italic
Formatted: Font: Not Italic
Formatted: Font: Not Italic
Formatted: Font: Not Italic
Formatted: Font: Not Italic
Formatted: Font: Not Italic
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Font: Not Italic
Formatted: Font: Not Italic
Formatted: Don't keep with next
Formatted: Font: Not Italic