~~INTERNATIONAL STANDARD~~

Third edition

ISO/IEC FDIS 24760-1:2024(en)

2024-~~10-31~~12-12

ISO/IEC JTC 1/SC 27/WG5

Secretariat: DIN

Horizontal document

IT Security and Privacy — A framework for identity management —Part 1: ~~Terminology and~~ Core concepts and terminology

~~Sécurité et confidentialité IT — Cadre pour la gestion de l'identité — Partie 1: Terminologie et concepts~~

Formatted: Centered

Style Definition: Heading 1
Style Definition: Heading 2
Style Definition: Heading 3
Style Definition: Heading 4
Style Definition: Heading 5
Style Definition: Heading 6
Style Definition: Default Paragraph Font
Style Definition: ANNEX
Style Definition: AMEND Terms Heading
Style Definition: AMEND Heading 1 Unnumbered
Style Definition: IneraTableMultiPar: Font: Font color: Auto, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted
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: Centered

Formatted

Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Default Paragraph Font

Formatted: Default Paragraph Font

Contents

Foreword ... iv
Introduction ... v
1 Scope ... 11
2 Normative references ... 11
3 Terms and definitions ... 22
3.1 General terms ... 2
3.2 Identification ... 44
3.3 Authenticating identity information ... 4
3.4 Management of identity ... 88
3.5 Federation ... 10
3.6 Privacy protection ... 11
4 Symbols and abbreviated terms ... 12
5 Identity ... 12
5.1 General ... 1212
5.2 Identity information ... 13
5.3 Identifier ... 14
5.4 Credential ... 14
6 Attributes ... 17
6.1 General ... 17
6.2 Types of attributeattributes ... 17
6.3 Domain of origin ... 1818
7 Managing identity information ... 19
7.1 General ... 19
7.2 Identity lifecycle ... 20
8 Identification ... 2222
8.1 General ... 2222
8.2 Verification ... 2323
8.3 Enrolment ... 23
8.4 Registration ... 24
8.5 Identity proofing ... 24
9 Authentication ... 25
10 Maintenance ... 26
11 Implementation aspects ... 26
12 Privacy ... 27
Bibliography ... 2828
Index of terms ... 3131

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 ~~documents~~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~~www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at ~~www.iso.org/patents and https://patents.iec.ch~~www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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~~www.iso.org/iso/foreword.html. In the IEC, see ~~www.iec.ch/understanding-standards~~www.iec.ch/understanding-standards.

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

This ~~second~~third edition cancels and replaces the ~~first~~second edition (ISO/IEC 24760-1:~~2011~~2019), which has been technically revised. It also incorporates the Amendment ISO/IEC 24760-1:2019/Amd 1:2023.

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

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~~www.iso.org/members.html and ~~www.iec.ch/national-committees~~www.iec.ch/national-committees.

~~This document has been given the status of a horizontal document in accordance with the ISO/IEC Directives, Part 1.~~

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

Formatted: English (United Kingdom)

Formatted: std_suppl

Formatted: std_suppl

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

Introduction

Data processing systems commonly gather a range of information on their users, be it a person, piece of equipment, or piece of software connected to them, and make decisions based on the gathered information. Such identity-based decisions can concern access to applications or other resources.

To address the need to efficiently and effectively implement systems that make identity-based decisions, the ISO/IEC 24760 series specifies a framework for the issuance, administration, and use of data that serves to characterize individuals, organizations or information technology components which operate on behalf of individuals or organizations.

For many organizations, the proper management of identity information is crucial for maintaining security within organizational processes. For individuals, correct identity management is important for protecting privacy.

The ISO/IEC 24760 series specifies fundamental concepts and operational structures for identity management and provides a framework on which information systems can meet business, contractual, regulatory, and legal obligations.

This document specifies the terminology and concepts for identity management, in order to promote a common understanding in the field of identity management.

This document is intended to provide a foundation for the terminology and concepts ~~to~~in other international standards related to identity information processing including other parts of the ISO/IEC 24760 series, ISO/IEC 29100, ISO/IEC 29101, ISO/IEC 29115, and ISO/IEC 29146.

Formatted: Font: 11.5 pt, Bold
Formatted: Font: 11.5 pt, Bold
Formatted: Font: 11.5 pt, Bold
Formatted: Normal, Centered, Space After: 36 pt, Line spacing: Exactly 12 pt, Tab stops: 0.71 cm, Left
Formatted: Font: 11.5 pt, Bold
Formatted: Font: 12 pt, Bold
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Body Text, Space After: 0 pt, Tab stops: Not at 0.7 cm + 1.4 cm + 2.1 cm + 2.8 cm + 3.5 cm + 4.2 cm + 4.9 cm + 5.6 cm + 6.3 cm + 7 cm
Formatted: Default Paragraph Font
Formatted: Font: 9 pt
Formatted: Normal, Centered, Space After: 24 pt, Tab stops: 17.2 cm, Right

Information technology — Security techniques — A framework for identity management — Part 1: ~~Terminology and~~ Core concepts and terminology

1 Scope

This document:

— defines terms for identity management and specifies core concepts of identity and identity management, and their relationships;

— is applicable to any information system where information relating to identity is processed or stored;

— ~~has been given the status of~~is considered to be a horizontal document~~, as~~ for the following reasons:

— it applies concepts such as distinguishing the term "identity" from the term "identifier" on the implementation of systems for the management of identity information and on the requirements for the implementation and operation of a framework for identity management, ~~as~~

— it provides an important contribution to assess identity management systems with regard to their privacy-friendliness and their ability to assure the relevant attributes of an identity, and consequently it provides a foundation and a common understanding for any other standard addressing identity, identity information, and identity management.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

Formatted: Font: 11.5 pt
Formatted: Font: 11.5 pt
Formatted: Font: 11.5 pt
Formatted: Font: 11.5 pt
Formatted: Font: 11.5 pt
Formatted: Header
Formatted: Body Text, Tab stops: Not at 0.7 cm + 1.4 cm + 2.1 cm + 2.8 cm + 3.5 cm + 4.2 cm + 4.9 cm + 5.6 cm + 6.3 cm + 7 cm
Formatted: Font: Cambria, 11 pt
Formatted: Font: Cambria, 11 pt
Formatted: List Continue 2 (-), Bulleted + Level: 1 + Aligned at: 1.32 cm + Indent at: 1.96 cm, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers, Tab stops: Not at 0.7 cm + 1.4 cm + 2.1 cm + 2.8 cm + 3.5 cm + 4.2 cm + 4.9 cm + 5.6 cm + 6.3 cm + 7 cm
Formatted: Font: 9 pt
Formatted: Centered, Space After: 24 pt, Tab stops: 17.2 cm, Right

ISO/IEC 24760-2:—,[1] *Information technology — Security techniques — A framework for identity management — Part 2: Reference architecture and requirements*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1 General terms

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

Note 1 to entry: An entity can 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.

3.1.2
identity
partial identity
set of *attributes* (3.1.3) related to an *entity* (3.1.1)

Note 1 to entry: An entity can have more than one identity.

Note 2 to entry: Several entities can have the same identity.

Note 3 to entry: ITU-T X1252 specifies the distinguishing use of an identity. In this document, the term *identifier* (3.1.4) implies this aspect.

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

EXAMPLE An entity type, address information, telephone number, a privilege, a MAC address, a domain name are possible attributes.

3.1.4
identifier

[1] Under preparation. Stage at the time of publication: ISO/IEC/FDIS 24760-2:2024.

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 0.7 cm, Left + 1.4 cm, Left + 2.1 cm, Left + 2.8 cm, Left + 3.5 cm, Left + 4.2 cm, Left + 4.9 cm, Left + 5.6 cm, Left + 6.3 cm, Left + 7 cm, Left

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

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

EXAMPLE A name of a club with a club-membership number, a health insurance card number together with a name of the insurance company, an email address, or a Universal Unique Identifier (UUID) can all be used as identifiers. In a voter's register, the combination of attributes name, address and date of birth is sufficient to unambiguously distinguish a voter.

3.1.5
domain of origin
domain (3.2.3) where an *attribute* (3.1.3) value was created or its value has been (re)assigned

Note 1 to entry: The domain of origin can 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 can be based on international standards.

Note 3 to entry: An attribute can 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* (3.2.4) in the passport.

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

3.1.6
reference identifier
RI
identifier (3.1.4) in a *domain* (3.2.3) that is intended to remain the same for the duration an *entity* (3.1.1) is known in the domain and is not associated with another entity for a period specified in a policy after the entity ceases to be known in that domain

Note 1 to entry: A reference identifier persists at least for the existence of the entity in a domain and can exist longer than the entity, e.g. for archival purposes.

Note 2 to entry: A reference identifier for an entity can change during the lifetime of an entity, at which point the old reference identifier is no longer applicable for that entity.

EXAMPLE A driver license number that stays the same for an individual driver's driving life is a persistent identifier, which references additional *identity information* (3.2.4) and that is a reference identifier. An IP address is not a reference identifier as it can be assigned to other entities.

3.1.7
principal

Formatted: Font: 11.5 pt
Formatted: Font: 11.5 pt
Formatted: Font: 11.5 pt
Formatted: Header, Centered
Formatted: Centered, Space After: 24 pt, Tab stops: 17.2 cm, Right
Formatted: Font: 9 pt

subject
entity (3.1.1) of which *identity information* (3.2.4) 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.

3.2 Identification

3.2.1
identification
process of recognizing an *entity* (3.1.1) in a particular *domain* (3.2.3) as distinct from other entities

Note 1 to entry: The process of identification applies verification to claimed or observed attributes.

Note 2 to entry: Identification typically is part of the interactions between an entity and the services in a domain and to access resources. Identification can occur multiple times while the entity is known in the domain.

3.2.2
verification
process of establishing that *identity information* (3.2.4) 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* (3.2.3), 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.

Formatted: Font: Not Italic

3.2.3
domain
domain of applicability
context
environment where an *entity* (3.1.1) can use a set of *attributes* (3.1.3) for *identification* (3.2.1) and other purposes

Note 1 to entry: In general, the domain of an *identity* (3.1.2) is well defined in relation to the particular set of attributes.

Note 2 to entry: ITU-T X1252 uses the term context; this document prefers the term domain.

EXAMPLE An IT system deployed by an organization that allows users to login is the domain for the user's login name.

3.2.4
identity information
set of values of *attributes* (3.1.3) optionally with any associated metadata in an *identity* (3.1.2)

Note 1 to entry: In an information and communication technology system, an identity is present as identity information.

3.3 Authenticating identity information

3.3.1

Formatted: Font: 11.5 pt
Formatted: Font: 11.5 pt
Formatted: Font: 11.5 pt
Formatted: Header, Centered

en)

authentication
formalized process of *verification* (3.2.2) that, if successful, results in an *authenticated identity* (3.3.2) for an *entity* (3.1.1)

Note 1 to entry: The authentication process involves tests by a verifier of one or more identity attributes provided by an entity to determine, with the required level of assurance, their correctness.

Note 2 to entry: Authentication typically involves the use of a policy to specify a required level of assurance for the result of a successful completion.

3.3.2
authenticated identity
identity information (3.2.4) for an *entity* (3.1.1) created to record the result of *authentication* (3.3.1)

Note 1 to entry: An authenticated identity typically contains information obtained in the authentication process, e.g. the level of assurance attained.

Note 2 to entry: The existence of an authenticated identity in a particular domain denotes that an entity has been recognized in that domain.

Note 3 to entry: An authenticated identity typically has a lifespan restricted by an authentication policy.

3.3.3
identity information authority
IIA
entity (3.1.1) related to a particular *domain* (3.2.3) that can make provable statements on the validity and/or correctness of one or more *attribute* (3.1.3) values in an *identity* (3.1.2)

Note 1 to entry: An identity information authority is typically associated with the domain, for instance the *domain of origin* (3.1.5), in which the attributes, which the IIA can make assertions on, have a particular significance.

Formatted: Font: Not Italic

Note 2 to entry: The activity of an identity information authority can be subject to a policy on privacy protection.

Note 3 to entry: An entity can combine the functions of *identity information provider* (3.3.4) and identity information authority.

3.3.4
identity information provider
IIP
identity provider
entity (3.1.1) that makes available *identity information* (3.2.4)

Note 1 to entry: Typical operations performed by an identity information provider are to create and maintain identity information for entities known in a particular domain. An identity information provider and an *identity information authority* (3.3.3) can be the same entity.

3.3.5
credential

Formatted: Centered, Space After: 24 pt, Tab stops: 17.2 cm, Right
Formatted: Font: 9 pt

representation of an *identity* (3.1.2) for use in *authentication* (3.3.1)

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* (3.2.4) 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.

EXAMPLE A credential can be a username, username with a password, a PIN, a smartcard, a token, a fingerprint, a passport, etc.

Formatted: Example, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers, Tab stops: Not at 0.7 cm + 1.4 cm + 2.1 cm + 2.8 cm + 3.5 cm + 4.2 cm + 4.9 cm + 5.6 cm + 6.3 cm + 7 cm

3.3.6
verifier
entity (3.1.1) that performs *verification* (3.2.2)

Note 1 to entry: A verifier can be the same as, or act on behalf of, the entity that controls identification of entities for a particular domain.

3.3.7
relying party
RP
entity (3.1.1) that relies on the *verification* (3.2.2) of *identity information* (3.2.4) for a particular entity

Note 1 to entry: A relying party is exposed to risk caused by incorrect identity information. Typically, it has a trust relationship with one or more *identity information authorities* (3.3.3).

Formatted: Font: Not Italic

3.3.8
identity assertion
statement by an *identity information authority* (3.3.3) used by a *relying party* (3.3.7) for *authentication* (3.3.1)

Note 1 to entry: An identity assertion can be the cryptographic proof of a successful authentication, created with algorithms and keys agreed between parties, e.g. in an identity federation.

3.3.9
authentication factor
distinguishing feature of an authenticator to characterize its use in *authentication* (3.3.1)

Formatted: Font: Not Italic

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* (3.1.7) knows and can reproduce (exclusively): a *personal secret* (3.3.13);

Formatted: Font: Not Italic

— 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;

