INTERNATIONAL STANDARD

ISO/IEC 24760-1

Second edition
2019-05

IT Security and Privacy — A framework for identity management —

Part 1: Terminology and concepts

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

Reference number
ISO/IEC 24760-1:2019(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

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.

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) or the IEC list of patent declarations received (see http://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.

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

This second edition cancels and replaces the first edition (ISO/IEC 24760-1:2011) which has been technically revised. The main changes compared to the previous edition are as follows:

— new terms have been added to Clause 3;

— some definitions have been simplified and corrected;

— some terms have been deleted and some replaced;

— the introductory paragraphs of Subclause 5.1 have been reworded;

— new subclauses 5.4 and 8.5 has been created;

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.

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 to maintain security of the organizational processes. For individuals, correct identity management is important to protect privacy.

The ISO/IEC 24760 series specifies fundamental concepts and operational structures of identity management with the purpose to realize information system management so that information systems can meet business, contractual, regulatory and legal obligations.

The goal of this document is to specify the terminology and concepts for identity management, in order to promote a common understanding in the field of identity management.

IT Security and Privacy — A framework for identity management —

Part 1: Terminology and concepts

1 Scope

This document defines terms for identity management, and specifies core concepts of identity and identity management and their relationships.

It is applicable to any information system that processes identity information.

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.

ISO/IEC 24760-2:2015, *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 terminological databases for use in standardization at the following addresses:

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

— IEC Electropedia: available at http://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[13] specifies the distinguishing use of an *identity*. In this document, the term *identifier* 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
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 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 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). 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 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
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 word "pertains" has been clarified and Note 1 to entry has been reworded.]

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, 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
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 is well defined in relation to the particular set of attributes.

Note 2 to entry: ITU-T X1252[13] 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
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 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, in which the attributes, which the IIA can make assertions on, have a particular significance.

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 and identity information authority.

3.3.4
identity information provider
identity provider
IIP
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 can be the same entity.

3.3.5
credential
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 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.

3.3.6
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.

3.3.8
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.

3.4 Management of identity

3.4.1
identity management
IDM
processes and policies involved in managing the lifecycle and value, type and optional metadata of *attributes* (3.1.3) in *identities* (3.1.2) known in a particular *domain* (3.2.3)

Note 1 to entry: In general identity management is involved in interactions between parties where *identity information* (3.2.4) is processed.

Note 2 to entry: Processes and policies in identity management support the functions of an *identity information authority* (3.3.3)where applicable, in particular to handle the interaction between an entity for which an identity is managed and the identity information authority.

3.4.2
identity proofing
initial entity authentication
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 can 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 can 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* (3.2.4) obtained when performing identity proofing can be included in the registration and can serve to facilitate future identification of the entity.

3.4.3
enrolment
process to make an *entity* (3.1.1) known within a particular *domain* (3.2.3)

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.

3.4.4
identity evidence
evidence of identity
information that can support validating *identity information* (3.2.4)

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
identity register
IMS register
repository of *identities* (3.1.2)

Note 1 to entry: A typical identity register is indexed by a reference identifier.

Note 2 to entry: The identity information authority in a particular domain typically uses its own identity register. However, an identity register can be shared between related domains, e.g. within the same commercial entity.

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
identity registration
registration
process of recording an *entity's* (3.1.1) *identity information* (3.2.4) in an *identity register* (3.4.5)

3.4.7
reference-identifier generator
tool used during *enrolment* (3.4.3) to provide a fresh unique value for a *reference identifier* (3.1.6)

EXAMPLE A database management system can be the reference identifier generator when it assigns a unique record number to a new record being added to a table and the record number is used as reference identifier.

3.4.8
identity management system
mechanism comprising of policies, procedures, technology and other resources for maintaining *identity information* (3.2.4) including associated metadata

Note 1 to entry: An identity management system is typically used for *identification* (3.2.1) or *authentication* (3.3.1) 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.

[SOURCE: ISO/IEC 24760-2:2015, 3.3, modified — "of application" has been deleted after "domain" in Note 1 to entry.]

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* (3.3.5) provisioned by a credential issuer can have a physical form, e.g. a membership (smart) card.

Note 2 to entry: The issuance of a *credential* (3.3.5) for a *principal* (3.1.7) can be recorded as an *attribute* (3.1.3) for the principal, e.g. by recording the unique number of the token issued.

Note 3 to entry: A *credential* (3.3.5) provisioned by an issuer can be a username and password. A credential in the form of a smart card or similar security 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).

