International Standard

ISO/IEC 24760-1

Third edition
2025-09

Information security, cybersecurity and privacy protection — A framework for identity management —

Part 1: Core concepts and terminology

Sécurité de l'information, cybersécurité et protection de la vie privée — Cadre pour la gestion de l'identité —

Partie 1: Concepts fondamentaux et terminologie

Reference number
ISO/IEC 24760-1:2025(en)

Horizontal document

© ISO/IEC 2025



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2025

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
3.1 General terms ... 1
3.2 Identification ... 3
3.3 Authenticating identity information ... 3
3.4 Management of identity ... 6
3.5 Federation ... 8
3.6 Privacy protection ... 8
4 Symbols and abbreviated terms ... **9**
5 Identity ... **9**
5.1 General ... 9
5.2 Identity information ... 10
5.3 Identifier ... 11
5.4 Credential ... 11
5.4.1 General ... 11
5.4.2 Authenticator ... 12
5.4.3 Credential management ... 13
6 Attributes ... **13**
6.1 General ... 13
6.2 Types of attributes ... 13
6.3 Domain of origin ... 14
7 Managing identity information ... **15**
7.1 General ... 15
7.2 Identity lifecycle ... 15
8 Identification ... **17**
8.1 General ... 17
8.2 Verification ... 18
8.3 Enrolment ... 18
8.4 Registration ... 18
8.5 Identity proofing ... 19
8.5.1 General ... 19
8.5.2 Identity evidence ... 19
9 Authentication ... **20**
10 Maintenance ... **20**
11 Implementation aspects ... **20**
12 Privacy ... **21**
Bibliography ... **22**
Index of terms ... **24**

© ISO/IEC 2025 – All rights reserved

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).

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

The main changes are as follows:

— title has been updated;

— the document has been editorially revised.

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

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

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.

© ISO/IEC 2025 – All rights reserved

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 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.

© ISO/IEC 2025 – All rights reserved

Information security, cybersecurity and privacy protection — A framework for identity management —

Part 1: 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;

— is considered to be a horizontal document 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,

  — 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.

ISO/IEC 24760-2, *Information security, cybersecurity and privacy protection — 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.

© ISO/IEC 2025 – All rights reserved

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
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). 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.

© ISO/IEC 2025 – All rights reserved

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
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.

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
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.

© ISO/IEC 2025 – All rights reserved

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.

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
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.

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.

© ISO/IEC 2025 – All rights reserved

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).

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)

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);

— 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 as that could prompt the *principal* (3.1.7) to act differently with each of them.

[SOURCE: ISO/IEC 19790:2012,[1)] 3.74, modified — definition and notes to entry have been updated to align with the context of this document.]

3.3.11
authenticator
representation of an *entity* (3.1.1) to demonstrate it is known in a *domain of origin* (3.1.5)

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 can provide a cryptographically strong identifier for the principal, which can be a pseudonym 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.

1) Cancelled and replaced by ISO/IEC 19790:2025.

© ISO/IEC 2025 – All rights reserved

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 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* (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 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

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* (3.2.2) 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* (3.3.5) is cryptographically protected, e.g. with HTTPS.

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* (3.4.3). 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.

© ISO/IEC 2025 – All rights reserved

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* (3.1.1).

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* (3.2.4) for identification of an entity and the collection of the *identity information* (3.2.4) 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* (3.1.3) needed for a successful identification or *authentication* (3.3.1) 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* (3.3.3) in a particular *domain* (3.2.3) 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* (3.2.4) in an identity register is determined by the identity proofing policies used during *enrolment* (3.4.3).

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
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.

3.4.8
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)

3.4.9
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 a credential 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* (3.1.3) for the principal, e.g. by recording the unique number of the token issued.

© ISO/IEC 2025 – All rights reserved

Note 3 to entry: A credential 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.

3.4.10
entity authentication assurance
assertion that the reliability of *identity information* (3.2.4) pertains to a particular entity

3.4.11
level of assurance
description of the strength of entity authentication assurance

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

3.4.12
principal's personal identity management system
PPI
mobile identity
identity management system (3.4.8) holding *identity information* (3.2.4) for a single *principal* (3.1.7), 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* (3.3.4) 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.

3.5 Federation

3.5.1
identity federation
agreement between two or more *domains* (3.2.3) specifying how *identity information* (3.2.4) will be exchanged and managed for cross-domain *identification* (3.2.1) purposes

Note 1 to entry: Establishing an identity federation typically includes an agreement on the use of common protocols and procedures for privacy control, data protection and auditing. The federation agreement can specify the use of standardized data formats and cryptographic techniques.

Note 2 to entry: The federation agreement can be the basis for identity authorities in each of the domains of applicability to mutually recognize credentials for authorization.

3.6 Privacy protection

3.6.1
selective disclosure
principle of *identity management* (3.4.1) that gives a person a measure of control over the *identity information* (3.2.4) that can be transferred to a third party, e.g. during *authentication* (3.3.1)

Note 1 to entry: In jurisdictions where certain types of legal entities are granted the right of privacy protection, the term "person" should be interpreted to include such entities, otherwise the term "person" is used in relation to a single human individual.

3.6.2
minimal disclosure
principle of *identity management* (3.4.1) to restrict the request or transfer of *identity information* (3.2.4) to a third party to the minimum information strictly required for a particular purpose

Note 1 to entry: The principle of proportionality is related to minimal disclosure in so far as the effort of control intervention is reasonable in relation to the activity.

© ISO/IEC 2025 – All rights reserved

3.6.3
pseudonym
identifier (3.1.4) that contains the minimal *identity information* (3.2.4) sufficient to allow a *verifier* (3.3.6) to establish it as a link to a known *identity* (3.1.2)

Note 1 to entry: A pseudonym can be used to reduce privacy risks that are associated with the use of identifiers with fixed or known values.

Note 2 to entry: A pseudonym can be an identifier with a value chosen by the person or assigned randomly.

Note 3 to entry: In jurisdictions where certain types of legal entities are granted the right of privacy protection, the term "person" should be interpreted to include such entities, otherwise the term "person" is used in relation to a single human individual.

3.6.4
ephemeral identifier
identifier (3.1.4) with a restricted validity period

Note 1 to entry: Typically, an ephemeral identifier is provided to a subject as a cryptographic credential to represent an *authenticated identity* (3.3.2).

Note 2 to entry: Typically, an ephemeral identifier can only be verified in the *domain* (3.2.3) that created it, possibly also in domains federated with this domain.

4 Symbols and abbreviated terms

HTTPS	Hypertext transport protocol, secured
MAC	Media access control
ICT	Information and communication technology
URI	Uniform resource identifier

5 Identity

5.1 General

An identity represents an entity in an ICT system as data to be stored or processed. The (business) purposes of a particular domain of application served by an ICT system determine which of the attributes pertaining to an entity shall be used in its identity. A persistently stored identity is the basis for identification of a principal. If a persistent identity is not an identifier, identification can require additional information from the principal.

An identity can, in part or fully, be represented by a credential issued to the principal. If an identity is represented by such a credential, an identifier for the credential can be included in the registered identity.

This document considers any set of attributes that describe a particular entity as an identity for the entity. In some domains, the persistently stored identity information for different entities can be the same. In this case, additional information is used in identification to recognize an entity as distinct, where needed. In other standards, e.g. ITU-T X1252,[15] the explicit purpose of an identity is the capability of the identity information to distinguish entities from each other to the extent relevant for applications in a domain (“in context”).

An entity can have multiple identities, each identity relating to at least one domain. An entity can have multiple identities relating to the same domain. Some identities of an entity cannot be unique in any domain.

NOTE 1 The term entity is taken in a broad sense. It represents a physical person, a moral or legal person (institution, company), an object (information, a system, a device), or a group of these individual entities.

© ISO/IEC 2025 – All rights reserved