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

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://patentsiec. 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).

3.5 Federation

3.5.1
federated identity
identity (3.1.2) for use in multiple *domains* (3.2.3)

Note 1 to entry: Some or all of the domains where a federated identity can be used can be formally joined as an identity federation. Identity information providers of domains in the federation can jointly manage a federated identity.

Note 2 to entry: The federated identity can be persistent or be a temporary one.

3.5.2
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

In jurisdictions where certain types of legal entities are granted the right of privacy protection, the term ‘person’ in the following definitions should be interpreted to include such entities, otherwise the term ‘person’ is used in relation to a single human individual.

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)

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.

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.

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.

3.6.5
blinded affirmation
principle of *identity management* (3.4.1) of not providing *identity information* (3.2.4) for an *entity* (3.1.1) to a third party except a statement that the entity is known in a *domain* (3.2.3)

Note 1 to entry: Blinded affirmation provides a strong level of protection for the privacy of a *principal* (3.1.7).

Note 2 to entry: Blinded affirmation can be realized with an *ephemeral identifier* (3.6.4) or pseudonym.

4 Symbols and abbreviated terms

ICT	Information and Communication Technology
IDM	Identity Management
IIP	Identity Information Provider
IIA	Identity Information Authority
RI	Reference Identifier
RP	Relying Party
SSO	Single Sign On
URI	Uniform Resource Identifier
UUID	Universal Unique 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 are to 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[13], 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.

NOTE 2 A human is an entity in this document and has a single, whole existence. It can be described by many different attributes. Different sets of these attributes form different identities for the same human entity.

If an identity is not unique in a particular domain, it can serve to distinguish a group of entities in that domain that share one or more characteristics from other entities that do not have such a characteristic.

The identity of an entity serves to make known relevant information of the entity in its interactions with the services and access of resources provided by a domain. A domain specifies the type and range of permissible values of attributes to be used for identification or other purposes.

NOTE 3 In some cases the term "partial identity" can be used to refer to a particular set of attributes taken from a larger set of attributes, which in contrast can be referred to as the full identity — all available attributes — of an entity in a domain. The preferred term in this document is identity.

A domain should deploy an identity management system conforming to the ISO/IEC 24760 series to manage the identity information of the entities it intends to recognize.

5.2 Identity information

Information pertaining to a particular entity in a domain is called identity information.

If given identity information sufficiently distinguishes an entity from others in the context of a given use case, then this identity information is a *distinguishing identity*.

If the combination of values contained in identity information is unique in the domain, then this identity information is an *identifier* of the entity.

When a new identity is created for an entity in a domain, an identity information provider for the domain can create values for required attributes of the new identity. The new attributes can consist of:

- Any information required to facilitate the interaction between the domain and the entity for which the identity is created;
- Any information required for future identification of the entity, including description of aspects of the physical existence of the entity;
- Any information required for future authentication of the entity’s identity; or
- One or more reference identifiers.

The new identity information can be derived from identity information for the entity created in the current or another domain. Deriving information can involve copying, collating, or creating a pseudonym.

The domain shall ascertain that the created identity information accurately pertains to the entity.

Identity information can be associated with metadata specifying, for instance, its origin, scope of use, and period of validity. Identity information metadata can itself be identity information and can be included in the identity it relates to.

Identity information and its associated metadata can be changed. Procedures and conditions for changing, updating, and creating identity information shall be specified in appropriate policies. These policies can include keeping records for auditing. These policies can distinguish between a number of tasks and activities relating to the identity lifecycle (see 7.2), including:

- requesting and receiving information from external sources;
- verifying and validating;
- qualifying and categorizing;
- recording;
- provisioning;
- archiving; and

— deleting.

5.3 Identifier

The unique attribute or attributes in an identity used as an identifier can be:

— available to the entity for exclusive use in the domain of origin; or

— suitable for use in domains other than the domain of origin.

An identifier can be constructed in a domain of origin from scratch, can be the result of observation, or can be based on presented identifiers.

NOTE 1 In some cases, e.g. single sign on, an identifier can be created with the purpose of being also used outside the domain of origin.

NOTE 2 In some cases, the identifier alone cannot be sufficient to distinguish the entity from another entity in a domain different from the originating domain. In this case, the other domain can, depending on the use of the identifier, need additional identity information. An example of this can be a library membership card containing the membership number as identifier that also gives regular access to a museum, where, if the museum has an exhibit accessible over a certain age, this additional information is being asked.

5.4 Credential

5.4.1 General

A credential can exist in different formats:

— as information only known to the principal and the identity management system, e.g. a password, a PIN, a passphrase;

— non-secret information known to the principal and possibly other entities, e.g. a username;

— as a digital record containing identity information;

— as a document with printed identity information possibly machine readable;

— as a portable processing device, e.g. smart card., with identity information stored in its (persistent) memory; or

— as a combination of these formats.

NOTE 1 For human entities (persons), credentials are often in the form of physical objects held by the person whose identity is represented by the credential. Credentials indirectly represent the domain of the identity it represents, e.g. for a secret context as the context where the secret can be validated.

NOTE 2 If a secret credential does not have an unique value, additional information such as a username or a biometric sample can be required for authentication. This information can be provided by a separate credential.

NOTE 3 A physical credential can be unique in the domain of the issuer. For example, a passport uniquely identifies a person (entity) as a citizen of a country (domain).

NOTE 4 A credential can also be viewed as an entity in its own right with a specific identifier, e.g. a passport identified by a unique passport number.

A credential can contain information that facilitates verification of the contained identity information at a given level of assurance. Appropriate verification techniques will depend on the application and the form of the credential used, and can include:

— a reference to the domain of origin, e.g. a name or a URL;

— a reference to the credential issuer, e.g. a name or a URL;

- secret information only known to the entity, e.g. a password;
- biometric reference data;
- physical characteristics that are difficult to copy such as
  - a watermark,
  - security printing,
  - a hologram, or
  - a physically unclonable function (PUF);
- a secret cryptographic key;
- a cryptographic public key;
- a public key certificate;
- a description of the parameters for cryptographic keys; or
- a reference to a specification for identity proofing or the level of assurance of contained identity information, e.g. an international standard.

NOTE 5 The information in a credential intended to support verification allows a third party to assert the physical integrity of the credential or the logical integrity of the identity information it contains. This supporting information allows a verifier to gain assurance in any information it obtains from the credential. A verifier can use additional information, e.g. obtained from the domain where the credential was issued, in order to make the determination of integrity of the credential and the information it contains.

To the extent permitted by relevant legislation or regulation, information in a credential that is used to support verification information in a credential pertaining to a person should be chosen to protect privacy, e.g. to enable anonymous or pseudonymous cryptographic operations.

A credential can additionally support cryptographic methods to authenticate and protect the confidentiality of the identity information the credential represents. These cryptographic methods can support selective disclosure of this information.

A credential can act as an identifier for an entity in the domain where the credential is issued. A credential can be used as identity evidence for enrolment in another domain.

5.4.2 Credential management

A credential shall be associated with the entity it represents and any identity information it contains shall be correct at the time of its issuance. A domain where credentials are issued in a physical form can associate each credential with a unique identifier and issuance of a credential can be recorded in a register. A credential register shall be implemented in accordance with ISO/IEC 24760-2.

NOTE To enhance protection of privacy, a credential register can be disjoint from the identity register in the domain of issuance.

Principles for the management of a credential are described in ISO/IEC 29115.

6 Attributes

6.1 General

An attribute of an identity describes the state, appearance or other qualities of an entity relevant in a domain. Each attribute has its own semantics to govern the interpretation of the values the attribute can take. The semantics of an attribute can be explicitly defined, e.g. by reference to an international standard for the equipment to establish its value.

An attribute has a type, value, and an operational context. An attribute can have a name that can be used to reference it. Depending on the use of the value of an attribute, its operational context is its domain of origin or the domain of applicability.

Clearly defined and documented semantics and syntax shall be specified for attributes.

NOTE For an IT system that implements identity management, it is mandatory that for each data element that represents an attribute, its internal and external representation (syntax) and the ways it can be processed (semantics) are explicitly defined in the system's design documents.

6.2 Types of attribute

Attributes can be classified into one or more types, which include, but are not limited to, the following:

NOTE The classification of attributes here is given as an example. Some attributes can be classified under multiple types.

- Information about physical existence, such as:
  - biographical details;
  - home or business address;
  - employer;
  - employment history;
  - device location;
- Information describing the entity’s evolution over time such as:
  - educational degree;
  - competency qualifications;
  - awards;
  - installed applications;
  - device configuration;
- Information intrinsic to the physical existence of the entity, such as biometrics;
- Information assigned to the entity, such as:
  - title;
  - role;
  - digital signature;
  - social security number;
  - citizenship number;
  - passport number;
  - manufacturer’s serial number;
  - network (mac) address;

  - cryptographic key;
- Reference to an object that represents identity information for the entity, such as:
  - passport;
  - educational diploma;
  - business card;
  - articles of incorporation;
  - vehicle registration.

6.3 Domain of origin

The domain of origin of an attribute can provide metadata for an attribute to indicate:

- the range of values of an attribute;
- uniqueness of attribute values;
- the encoding of the attribute value;
- the time of creation or verification of attributes or identities;
- the time of expiration of attributes or identities;
- the method of establishing the value of attributes or identities;
- the method of verification of the value of attributes;
- the mechanism to obtain a human readable representation of an attribute value.

The domain of origin of an attribute, or any of the information specified by the domain of origin, can be explicitly specified as part of the attribute value, e.g. with a reference to a system specification document or to applicable standards.

NOTE 1 An explicit domain of origin can be specified as part of the value of the attribute or be determined when needed, e.g. in a discovery process.

NOTE 2 Attribute properties indicated by a domain of origin can be indicated with a unique reference, e.g. URI, to a system specification document that is included in the attribute type definition.

NOTE 3 The value of an attribute that includes metadata can be called a composite value.

7 Managing identity information

7.1 General

A domain can use an identity management system to support its interaction with entities, e.g. authentication.

Identity Management covers the lifecycle of identity information from initial enrolment to archiving or deletion.

Identity Management includes the governance, policies, processes, data, technology, and standards, which can include:

- application(s) implementing an identity register;
- authenticating the identity;

- establishing provenance of identity information;
- establishing the link between identity information and an entity;
- maintaining the identity information;
- ensuring integrity of the identity information;
- providing credentials and services to facilitate authentication of an entity as a known identity;
- mitigating the risk of identity information theft or misuse.

7.2 Identity lifecycle

Figure 1 shows the lifecycle of an identity in an identity management system. Initially no information is present, and an entity is unknown. After deleting all identity information for an entity, it is unknown again.

NOTE From the perspective of an identity management system, an unknown entity does not exist.

The following stages in the identity lifecycle have been identified:

- **Unknown**: no information is present in the identity register that can be used to identify an entity which is hence unknown.
- **Established**: required identity information has been verified during the enrolment process (see 8.3), additional information, e.g. a reference identifier, has been generated, and the information has been registered (see 8.4).
- **Active**: identity information is present in the identity management system, which allows the entity to interact with services and utilize the resources available in a domain of applicability, for instance, the entity can be entitled to initiate an active session in an IT system.
- **Suspended**: identity information is present in the identity management system specifically to indicate that the entity cannot utilize the resources of the domain.
- **Archived**: identity information for an entity is still present in the identity register, even though the entity no longer exists in the domain. Archived information is not available for recognizing the entity except possibly during re-enrolment. When the entity re-enrols, the archived information can be used to establish a new identity for the entity, which can include some of the archived information (restore).

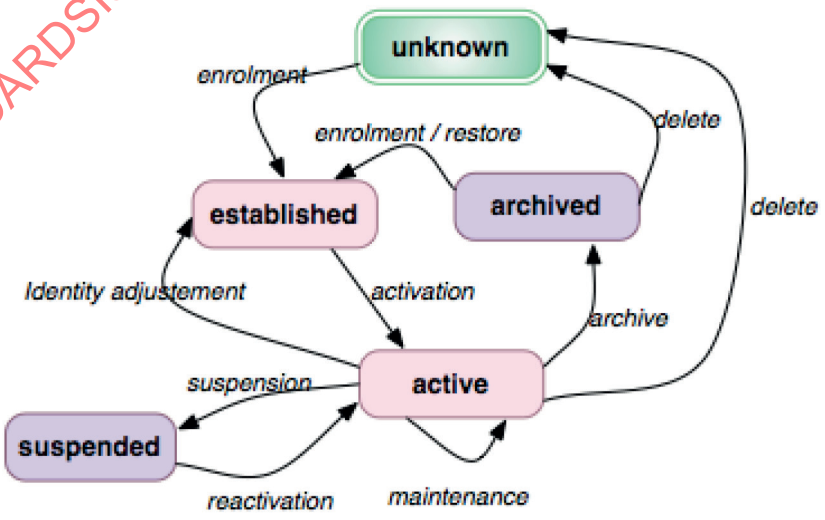

Figure 1 — Identity lifecycle

The following transitions can be applied in managing the lifecycle:

- **Enrolment** includes identity proofing and registration of an identity with verified and generated identity information. See 8.3.
- **Activation** is the addition of identity information to the information stored in the identity register for an entity specifically to enable the entity to access resources and interact with services provided by a domain.
- **Maintenance** is the update of identity information stored in the identity register for an entity. See Clause 10.
- **Identity adjustment** is an update of the information in the identity register for an entity, where the new information gives rise to the modification of activation information.
- **Suspension** is marking some of the identity information stored in the identity register for an entity as being temporarily unavailable for use. Suspension can be achieved by removing access rights expressed in the stored identity information.
- **Reactivation** is the reversion of the suspension.
- **Delete** is the complete removal of the identity information in a registered identity.
- **Archive** is the partial removal of identity information from the identity register for an entity, such that the information is only available for statistical processing and can only be accessed as pertaining to an entity with additional information provided by the entity.
- **Enrolment/restore** is an enrolment process, where some of the identity information used as identity proof is obtained from the identity register.

8 Identification

8.1 General

Identification determines that a presented identity contains the information required to establish that

- the entity is already known in the domain; or
- the entity qualifies to become known in the domain.

Identification can use the identity information associated with a particular entity to determine if

- an identity already exists for the entity;
- the entity matches the known or presented or observed identity information;
- the entity is uniquely associated with the identity.

After identification, the domain can actively distinguish the entity and the entity's interactions with the domain from any other entity it has also identified.

NOTE 1 This document presents identification from the perspective of a domain. In mutual identification both parties are both entity and domain.

Identification involves associating a set of attributes both with an entity and an identity. The value of these attributes can be:

- determined by observation;
- provided by the entity;
- retrieved from the identity register;

- provided by another source; or
- assigned during the process.

Identification can be followed by authorization in establishing entitlements for the entity to access resources and interact with services provided by the domain. See 7.2.

In a system where access to resources or interaction with services involves identity-related risks, the required level of assurance in identification shall be specified based on the type and level of identity risk to the resource, and the type of interaction with the service for which an entitlement can be established. See Clause 9.

Identification can be for a single purpose, specific to the domain, or for multiple different purposes. Identification is part of many identity management processes, for instance as defined in ISO/IEC 29115[11] for IT systems.

A process for identification shall be specified with the following principles:

- **Risk** Risks associated with the use of the identity of entities shall be assessed and treated to the degree necessary for them to be acceptable;

  NOTE 1 Different levels of assurance in identification can be associated with different levels of risk associated with the access to different resources and interaction with different services.

- **Quality of Information** Identity information shall be verified to provide sufficient level of assurance in the correctness for the purposes of its use;
- Data minimization When identifying people, no more identity information shall be collected than necessary.

NOTE 2 Assessing risks involves consideration of the quality of the available information and of the means to establish its correctness.

NOTE 3 Selection of suitable risk mitigation options includes ensuring that the cost is proportional to the risk.

8.2 Verification

New identity information shall be verified. Verification can also be performed for identity information that is retrieved from an identity register or from an identity information provider.

Verification of identity information shall ensure that it:

- is present in an approved format;
- contains a value that meets criteria specific to the domain or the purpose of identification;
- originated within a required validity period; or
- originated from a reliable source.

NOTE Verification can also provide input to identification and its result can be specific to the particular circumstances, e.g. location and time of that process.

Verification can also establish that an attribute pertains to the physical existence of an entity, e.g. match a biometric sample from the entity with a biometric template contained in its identity.

Verification can establish that all the presented attributes pertain to the same entity and are consistent with its physical existence.

Verification can include an examination of the validity of attributes not required for the identification process which can be used during interaction with services and access to resources provided by the domain after identification, e.g. a language preference, an account number.

8.3 Enrolment

Enrolment can result in the creation of one or more identities for the enrolled entity. In particular, a reference identifier can be created. Created identity information is registered as the enrolled entity's identity in a domain; identity information selected from the identity evidence can also be registered with this identity at the time of enrolment.

The value of the unique attribute(s) in a created identity can be chosen by the entity or can be assigned by the identity management system, e.g. based on the reference identifier created at registration of the identity for the enrolled entity.

Enrolment can include the capture of biometric data as identity information for the enrolled entity.

If the entity determines the value of an identifier created during enrolment, the IDMS should ensure its uniqueness.

NOTE A physical object, e.g. a membership card, can contain an identifier that has been created during enrolment.

8.4 Registration

An identity management system can enter identity information for the entities it intends to recognize in an identity register. Enrolment includes the first registration of identity information. Further registration can happen at other occasions.

NOTE 1 After registration, an entity has become known in the domain and the lifecycle of its identity has started.

Registration can be for a specific or indefinite duration. National legislation can impose restrictions on the actual duration of indefinite registration, including when and how indefinite registration can end.

Unless prevented by legal requirements, registration shall end at a request by, or on behalf of, the entity for removal. With the deletion of all identity information for the entity, the entity shall be removed from the identity register. However as determined by an appropriate policy, a domain can retain some identity information for archival and auditing purposes, and, in this case, the identity will be in the lifecycle stage *archived* (see 7.2). In particular, a reference identifier can be retained to prevent its reuse as a reference to another entity.

The identity stored in an identity register shall have a reference identifier that is unique amongst all stored identities. A reference identifier shall have the same value for the duration of registration of identity information for a particular identity.

A reference identifier can be intended for exclusive use inside the domain that operates the identity management system.

NOTE 2 A reference identifier, if not used exclusively by a domain, can be available for use as an attribute in the identity an entity presents for identification in another domain.

The identity information stored in an identity register can include multiple reference identifiers. A reference identifier can be used to indicate a particular partial identity for the entity in a domain.

8.5 Identity proofing

8.5.1 General

The purpose of identity proofing for a domain is to establish a specific level of assurance that:

- selected attributes for an entity have a particular value;
- these attributes actually pertain to a particular entity;

- where required in a domain, no other entity is known in the domain to whom the same attributes pertain.

NOTE 1 In a domain where the persistently stored identity information is not unique, it can be required to only create an identity for entity that is not already identified. In this case, the identity management system can store additional persistent information, not linkable to the identity information, to support determining that the identity for an entity being proofed is unique.

NOTE 2 A registration authority is responsible for identity proofing.

NOTE 3 Requirements for identity proofing are specified in ISO/IEC TS 29003.

8.5.2 Identity evidence

Identity evidence shall be used to establish attribute values for registration of an entity in a domain. Credentials issued in a domain can be used as identity evidence in another domain. These credentials can be presented by an entity. Alternatively, they can be obtained from an identity information provider in another domain where the identity is known based on information provided by the entity.

Attribute aggregation, verifying multiple credentials from the same or different domains, where each of the credentials provides a level of assurance less than required for the result, can be applied to achieve a required level of assurance in an attribute value and in establishing the value as pertaining to a specific entity.

The identity information authority for a domain where a credential has been issued can support the verification of identity information during identity proofing by:

- providing a limited, authenticated set of valid attribute values, e.g. a list of street names, district numbers or neighbourhood names;
- publishing format and other physical or logical properties of valid credentials issued by its domain;
- publishing policies applied to identity proofing and identity information maintenance;
- providing a public key in a public key infrastructure shared with the proofing registration authority to validate digital signatures used to authenticate a credential or data represented by it;
- providing an on-line service to validate presented attributes as about an entity known in its domain; or
- providing an on-line service to obtain additional attributes for an entity known in its domain.

9 Authentication

Successful authentication of an entity in a domain, at a specific level of assurance, gives a relying party confidence in the correctness and applicability of the verification result. ISO/IEC 29115[11] specifies levels of assurance.

An identity management system conforming to ISO/IEC 24760 shall specify for each of its authentication processes:

- policies for verification of identity information;
- mechanisms for establishing the validity and correctness of an authenticated identity;
- the period of validity of an authenticated identity;
- mechanisms for the recording and auditing; processing steps and (intermediate) processing results.

NOTE Authentication relates to a security model of perimeter control where a strict verification at the entrance gives authorization to enter a specific area of activity for a specific period of time.

10 Maintenance

An identity management system can perform maintenance on identity information it has registered by changing one or more of the attribute values in an identity.

An identity management system shall specify mechanisms for maintaining the integrity and accuracy of attributes it stores. It shall maintain the identity information stored in the register as an accurate representation of the identity.

An identity information authority shall provide the most accurate data available for an identity in a process that respects privacy.

11 Implementation aspects

An identity management system can be:

— centralized — A fully centralized system has a single identity register and a single point of control over enrolment and access to the stored identity information;

— distributed — An identity management system can have multiple identity registers and multiple points of control over enrolment and access to registered identity information;

NOTE 1 A more centralized system typically displays less complexity but is more rigid in structure.

— user-centric — An identity management system is user-centred when it allows the entities to play an active role in the management of the identity information stored in the identity register (see 8.4);

— federated — Federation allows an identity management system that does not contain required identity information in its own register to trust identity information from, and identity assertions made by, another identity management system. In this case, the other identity management system acts as an identity information authority.

In situations where entities interact with multiple domains, identity federation is intended to:

— facilitate identity proofing;

— facilitate authentication;

— facilitate enrolment;

— improve user experience.

NOTE 2 Identity federation is especially suitable for entities (and domains) that interact with domains on the Internet.

12 Privacy

An identity management system conforming to the ISO/IEC 24760 series shall implement measures to protect the privacy of the human entities it interacts with. The design of such a system shall clearly specify any sensitive information it processes.

An identity management system conforming to the ISO/IEC 24760 series should provide privacy-related capabilities to:

— implement mechanisms, including policies, processes; and technology, for minimal disclosure;

— authenticate entities that use identity information;

— minimize the ability to link identities;

— record and audit the use of identity information;