INTERNATIONAL STANDARD

ISO/IEC 24760-1

First edition
2011-12-15

Information technology — Security techniques — A framework for identity management —

Part 1: Terminology and concepts

Technologies de l'information — Techniques de sécurité — Cadre pour la gestion de l'identité —

Partie 1: Terminologie et concepts

Reference number
ISO/IEC 24760-1:2011(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web 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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 24760-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

ISO/IEC 24760 consists of the following parts, under the general title *Information technology — Security techniques — A framework for identity management*:

— *Part 1: Terminology and concepts*

The following parts are under preparation:

— *Part 2: Reference architecture and requirements*

— *Part 3: Practice*

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 may concern access to applications or other resources.

To address the need to efficiently and effectively implement systems that make identity-based decisions, ISO/IEC 24760 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.

ISO/IEC 24760 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.

This part of ISO/IEC 24760 specifies the terminology and concepts for identity management, to promote a common understanding in the field of identity management. It also provides a bibliography of documents related to standardization of various aspects of identity management.

Information technology — Security techniques — A framework for identity management —

Part 1: Terminology and concepts

1 Scope

This part of ISO/IEC 24760

— defines terms for identity management, and

— specifies core concepts of identity and identity management and their relationships.

This part of ISO/IEC 24760 is applicable to any information system that processes identity information.

A bibliography of documents describing various aspects of identity information management is provided.

2 Normative references

The following referenced documents are indispensable for the application 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.

No normative references are cited.

3 Terms and definitions

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

NOTE The terms and definitions in this part of ISO/IEC 24760 are drafted in accordance with ISO/IEC 10241, *International terminology standards — Preparation and layout*, which specifies that alternative term(s), often used for the term expressed in a bold typeface, may be placed on a separate line before the text defining the term. This part of ISO/IEC 24760 uses only the term in bold face.

3.1 General terms

3.1.1
entity
item inside or outside an information and communication technology system, such as a person, an organization, a device, a subsystem, or a group of such items that has recognizably distinct existence

EXAMPLE A human subscriber to a telecom service, a government agency, a SIM card, a passport, a network interface card, a website.

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

NOTE 1 An entity can have more than one identity.

NOTE 2 Several entities can have the same identity.

NOTE 3 In a particular domain of applicability an identity can become a distinguishing identity or an identifier to allow entities to be distinguished or uniquely recognized within that domain.

NOTE 4 ITU-T X1252[13] specifies the distinguishing use of an *identity*. In this part of ISO/IEC 24760 the term *identifier* implies this aspect.

3.1.3
attribute
characteristic or property of an **entity** (**3.1.1**) that can be used to describe its state, appearance, or other aspects

NOTE The primary function of the concept of an attribute in this part of ISO/IEC 24760 is to be a particular, well-defined aspect of the description of an entity in an identity management system. The values of attributes in an identity together describe the entity in a domain.

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

3.1.4
identifier
unique identity
distinguishing identity
identity information (**3.2.4**) that unambiguously distinguishes one **entity** (**3.1.1**) from another one in a given **domain** (**3.2.3**)

NOTE 1 An identifier may be suitable for use outside the domain.

NOTE 2 An identifier may be an attribute with an assigned value.

NOTE 3 An identifier may be the one or more attributes that determine if an identity passes or fails specific criteria.

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
feature of an **attribute** (**3.1.3**) that specifies the **domain** (**3.2.3**) where the attribute was created or its value (re)assigned

NOTE 1 The domain of origin typically specifies the meaning and format of the attribute value. Such specification may be based on international standards.

NOTE 2 An attribute may 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 3 Operationally, a domain of origin may be available as an authoritative source for an attribute (sometimes known as the Attribute Authority). An authoritative source may be operated outside the actual domain of origin. Multiple authoritative sources may 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 A reference identifier persists at least for the existence of the entity in a domain and may exist longer than the entity, e.g. for archival purposes.

NOTE 2 A reference identifier for an entity may 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.

3.2 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 The process of identification applies verification to claimed or observed attributes.

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

3.2.2
verification
process to determine that presented **identity information** (**3.2.4**) associated with a particular **entity** (**3.1.1**) is applicable for the entity to be recognized in a particular **domain** (**3.2.3**) at some point in time

NOTE Verification can involve checking that the required attributes are present, have the correct syntax, and exist within a defined validity period.

3.2.3
domain
domain of applicability
context
DA
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 In general the domain of an identity is well defined in relation to the particular set of attributes.

NOTE 2 ITU-T X1252[13] uses the term context; this part of ISO/IEC 24760 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 In an information and communication technology system an identity is present as identity information.

3.3 Authenticating an identity

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

NOTE 3 Identification is usually done as authentication to obtain a specific level of assurance in the result.

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 An authenticated identity typically contains information obtained in the authentication process, e.g. the level of assurance attained.

NOTE 2 The existence of an authenticated identity in a particular domain denotes that an entity has been recognized in that domain.

NOTE 3 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 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 The activity of an identity information authority may be subject to a policy on privacy protection.

NOTE 3 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 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 may be the same entity.

3.3.5
credential
representation of an **identity** (**3.1.2**)

NOTE 1 A credential is typically made to facilitate *data* authentication of the identity information in the identity it represents.

NOTE 2 The identity information represented by a credential can be printed on paper or stored within a physical token that typically has been prepared in a manner to assert the information as valid.

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 A verifier may 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 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 An identity assertion may 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
identity assurance
level of assurance in the result of **identification** (**3.2.1**)

NOTE Identity assurance expresses the level of confidence in provenance, integrity and applicability of identity information including confidence in identity information maintenance.

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

NOTE 1 In general identity management is involved in interactions between parties where identity information is processed.

NOTE 2 Processes and policies in identity management support the functions of an identity information authority 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
particular form of **authentication** (**3.3.1**) based on **identity evidence** (**3.4.4**) that is performed as the condition for **enrolment** (**3.4.3**)

NOTE 1 Typically identity proofing involves an extensive verification of provided identity information and may include screening, vetting and uniqueness checks, possibly based on biometric techniques.

NOTE 2 Authentication, at the heart of identity proofing, typically is based on an enrolment policy that includes specification of the verification criteria of the identity evidence provided by the entity.

NOTE 3 The authenticated identity that is the result of the authentication in identity proofing may during subsequent enrolment be included in the registration and may 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 Enrolment leads to identity registration. Identity proofing is typically performed to establish the identity information to be registered for a particular entity.

NOTE 2 In general enrolment collates and creates identity information for storage in an identity register to be used in subsequent identification of the entity in the domain. It is the start of the lifecycle of an identity in the domain for an entity.

3.4.4
identity evidence
evidence of identity
identity information (**3.2.4**) for an **entity** (**3.1.1**) required for **authentication** (**3.3.1**) of that **entity** (**3.1.1**)

NOTE Identity evidence includes the presented and gathered information related to a claimant that is needed for a successful authentication. Any such information may be part of the authenticated identity for the claimant.

3.4.5
identity register
IMS register
repository of **identities** (**3.1.2**) for different **entities** (**3.1.1**)

NOTE 1 A typical identity register is indexed by a reference identifier.

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

NOTE 3 The reliability of the identity information in an identity register is determined by the authentication policies used during enrolment.

3.4.6
identity 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.

3.5 Federation

3.5.1
federated identity
identity (**3.1.2**) for use in multiple **domains** (**3.2.3**), which together form an **identity federation** (**3.5.2**)

NOTE 1 A federated identity may be jointly managed by identity information providers of the federated domains.

NOTE 2 The shared attributes used in the federated domains may in particular be used for identification, e.g. to support single-sign-on (SSO).

NOTE 3 The federated identity may persist or may be a temporary one, e.g. as single-sign-on identity.

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 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 may specify the use of standardized data formats and cryptographic techniques.

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

3.5.3
single-sign-on identity
SSO identity
identity (**3.1.2**) that includes a single **identity assertion** (**3.3.8**) that can be verified (**3.2.2**) by a **relying party** (**3.3.7**) in multiple **domains** (**3.2.3**)

NOTE The identity assertion in a single-sign-on identity is created during authentication of an entity in one domain and can be used in authentication of the entity in any other domain in the same identity federation.

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

NOTE 2 A pseudonym can be an identifier with a value chosen by the person, or assigned randomly.

3.6.4
anonymity
Condition in **identification** (**3.2.1**) whereby an **entity** (**3.1.1**) can be recognized as distinct, without sufficient **identity information** (**3.2.4**) to establish a link to a known **identity** (**3.1.2**)

NOTE Anonymous identification typically involves the use of special credentials that can be cryptographically validated. Cryptographic protocols for validation of an anonymous credential exist that can be configured to provide a verifier with required identity information. The identity obtained in this way may have multiple attributes.

4 Symbols and abbreviated terms

DA Domain (of applicability)

ICT Information and Communication Technology

IDM Identity Management

IMS Identity Management System

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 is the information used to represent an entity in an ICT system. The purpose of the ICT system determines which of the attributes describing an entity are used for an identity. Within an ICT system an identity shall be the set of those attributes related to an entity which are relevant to the particular domain of application served by the ICT system. Depending on the specific requirements of this domain, this set of attributes related to the entity (the identity) may, but does not have to be, uniquely distinguishable from other identities in the ICT system.

This part of ISO/IEC 24760 considers any set of attributes that describes a particular entity as an identity for the entity. In some domains, the identity information for different entities may be the same. 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 sufficiently from each other to the extent relevant for applications in a domain ("in context").

NOTE 1 If the purpose of identity management in a particular domain is to hold entities responsible, or to provide a specific privilege exclusively to a particular entity, uniqueness of identity is essential.

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

NOTE 2 The term entity should be 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 3 A human is an entity in this standard 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 may serve to distinguish a group of entities in that domain that share one or more characteristics from other entities that don't 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 4 In some cases the term 'partial identity' could 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 part of ISO/IEC 24760 is identity.

A domain should deploy an identity management system conforming to ISO/IEC 24760 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 may create values for required attributes of the new identity. The new attributes may 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 may be derived from identity information for the entity created in the current or another domain. Deriving information may involve copying, collating, or creating a pseudonym.

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

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

Identity information and its associated metadata may be changed. Procedures and conditions for changing, updating, and creating identity information shall be specified in appropriate policies. These policies may include keeping records for auditing. These policies may 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 may 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 may be constructed in a domain of origin from scratch, may be the result of observation, or may 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.

An identifier may be recorded onto, or in, a physical object. This physical object may be equipped with security features to

— Assert the integrity of the attribute values in the identifier,

— Allow a verifier to gain assurance that the identifier is legitimately associated with an entity,

— Protect the confidentiality of attribute values, or

— Facilitate verification of the identity information contained, e.g. by providing a cryptographic data authentication mechanism or embedded physical security characteristics.

NOTE 2 In some cases the identifier alone may not be sufficient to distinguish the entity from another entity in a domain different from the originating domain. In this case the other domain may, depending on the use of the identifier, need additional identity information. An example of this could 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.

NOTE 3 A physical object may represent the identifier. The physical object is a form of a credential, and may itself be an entity (as used in this part of ISO/IEC 24760) with its own attribute to uniquely distinguish it from another identifier object originating from the same domain. For example, a passport containing an identifier of a person (entity) as a citizen of a country (domain) may be considered an entity that has an identity consisting of a unique passport number.

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 may take. The semantics of an attribute may 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 may 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 may 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 could 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
  - Biometric;
- 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 may 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, may 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 may 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 may 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 may 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 may 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 may 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 may be used to establish a new identity for the entity, which may include some of the archived information (restore).

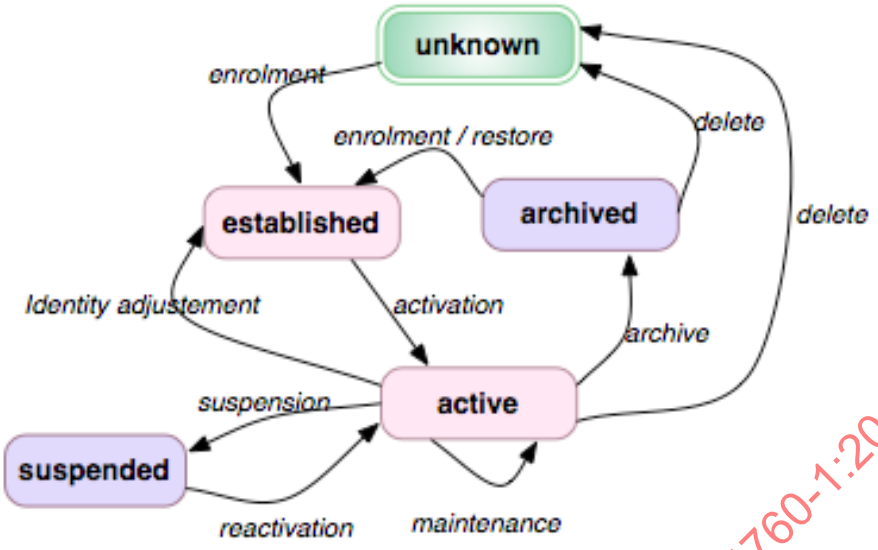

Figure 1 — Identity lifecycle

The following transitions may 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 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 may 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 may 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 part of ISO/IEC 24760 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 may be followed by authorization in establishing entitlements for the entity to access resources and interact with services provided by the domain. See 7.2: activation.

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 may be established. See 9.

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

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

Verification may include an examination of the validity of attributes not required for the identification process which may 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

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

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

Enrollment may include the capture of biometric data as identity information for the enrolled entity.

NOTE 1 If the entity determines the value of an identifier created during enrollment, the IDMS should ensure its uniqueness.

NOTE 2 A physical object, e.g. a membership card, may contain an identifier that has been created during enrollment.

8.4 Registration

An identity management system may enter identity information for the entities it intends to recognize in an identity register. Enrollment includes the first registration of identity information. Further registration may 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 may be for a specific or indefinite duration. National legislation may impose restrictions on the actual duration of indefinite registration, including when and how indefinite registration may end.

Unless prevented by legal requirements, indefinite 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 may 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 may 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 may 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, may 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 may include multiple reference identifiers. A reference identifier may be used to indicate a particular partial identity for the entity in a 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. International Standard 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 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.

An identity management system may support authentication of an identity at multiple distinct levels of assurance, e.g. to meet specific system design objectives in subsequent access control.

10 Maintenance

An identity management system may 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 may be:

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

Distributed — An identity management system may have multiple identity registers and multiple points of control over enrollment and access to registered identity information.

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

