ISO/IEC JTC 1/WG 7
Working Group on Sensor Networks

Document Number:	N048
Date:	2010-07-05
Replace:	
Document Type:	Liaison Organization Contribution
Document Title:	Liaison Statement from JTC 1/SC 27/WG 5 to JTC 1/WG 7 on the ISO/IEC 3rd CD 24760-1
Document Source:	JTC 1/SC 27/WG 5
Document Status:	For consideration at the 2nd WG 7 meeting in US.
Action ID:	FYI
Due Date:	
No. of Pages:	26

ISO/IEC JTC 1/WG 7 Convenor:
Dr. Yongjin Kim, Modacom Co., Ltd (Email: cap@modacom.co.kr)
ISO/IEC JTC 1/WG 7 Secretariat:
Ms. Jooran Lee, Korean Standards Association (Email: jooran@kisi.or.kr)

Committee Draft **ISO/IEC 3rd CD 24760-1 2)**	Reference number: ISO/IEC JTC 1/SC 27 **N8804**
Date:**2010-06-11**	Supersedes document SC 27 N8160

THIS DOCUMENT IS STILL UNDER STUDY AND SUBJECT TO CHANGE. IT SHOULD NOT BE USED FOR REFERENCE PURPOSES.

ISO/IEC JTC 1/SC 27 Information technology - Security techniques Secretariat: Germany (DIN)	Circulated to P- and O-members, and to technical committees and organizations in liaison for voting (P-members only) by: **2010-09-12** Please submit your votes and comments via the online balloting application by the due date indicated.

ISO/IEC 3rd CD 24760-1 2)

Title: Information technology -- Security techniques – A framework for identity management -- Part 1: Terminology and concepts

Project: 24760-1 2) (1.27.50.01 2))

Explanatory Report

Status	SC 27 Decision	Reference documents	
		Input	Output
For details related to Study Period and NWIP of this project please see the next page of this document.			
1st WD 24760 Study Period (SP)	Recommendations of Ad Hoc (N5184), May 2006		Report of Ad Hoc (N5184), May 2006; DoC (N5074r); Text f. Prelim. Draft (N5056r)
	18th SC 27 Plenary May 2006, Resolution 2 (N5199); Transfer to WG 5 as per res. 41 (N5199)	Rappoertuer's presentation / Report (N5182, N5184)	Text f. 1st WD (N5056rev1).
2nd WD 24760	1st WG 5 meeting, Nov. 2006, resolution 6 (N5513)	SoCom (N5271)	DoC (N5518); Text 2nd WD (N5517).
3rd WD 24760	2nd WG 5 meeting, May 2007, Resolutions 1 & 6 (N5873) and Resolutions 2 of 19th SC 27 May 2007 Plenary (N5939).	SoCom (N5662); DE, JP com (N5665); ITU-T SG17 LSs (N5603, N5751rev1, N5644); JP 1) contr. (N5869rev2).	DoC (N5876draft); Text for 3rd WD (N5877).
4th WD 24760	3rd WG 5 meeting, Oct. 2007, resolutions 1, 8 (N6251).	SoCom. (N6051); US com.(N6083); FIDIS com. (N6107).	DoC (N6249); Text f. 4th WD (N6248).
5th WD 24760	5th WG 5 meeting, April 2008, resolutions (N6726); 20th SC 27 April 2008 Plenary, resolution 2 (N6799).	SoCom. (N6250); FIDIS liaison (N6503); TC 215 liaison (N6786); AU 1) com. (N6536); SD6 Editor's com. (N6560, Att. 3).	Liaison to FIDIS (N6742); DoC (N6766); Text f. 5th WD (N6730) N/A.
6th WD 24760	6th WG 5 meeting, Oct. 2008, resolutions 1, 3, 8, 10 (N6726).	Text for 5th WD (N6730); AU com. (N6978); BR 1) com.(N7071); CA com (N7070); NZ 1) com (N7065); FIDIS com (N7060); SoCom on REV 5th WD (N7359); US com on REV 5th WD (N7376r1); FIDIS com on REV 5th WD (N379).	Liaison to FIDIS (N7102); REVISED text of. 5th WD (N7109); DoC (N7236); Text f. 6th WD (N7237).
1st CD 24760	7th WG 5 meeting, May 2009, resolutions 1, 3, 8, 10 (N). 21st SC 27 Plenary, May 2009, resolution 8 (N7777).	SoCom (N7542); FR com (N7547); FIDIS com (N7541).	Liaison to FIDIS (N7729); DoC (N7741); Text f. 1st CD (N7742).
2nd CD 24760	8th WG 5 meeting, Nov 2009, resolutions 1, 8 10, 11, 17 (N8138)	SC 37 (N8045); ITU-T SG17 (N8075); PrimeLife (N8096); SoV (N8047rev1); LU 1) (N8091); AU 1) (N8110).	Liaisons to SC 37 (N8141r1); to SC 31 (N8140); to PrimeLife (N8151); ITU-T SG17 (N8354); DoC (N8159); Text f. 2nd CD (N8160).
3rd CD 24760-1 2)	9th WG 5 meeting, April 2010, resolutions 4, P4, P8 (subdivision) (N8828rev).	SoV (N8566); ES notification RE co-editorship (N8588); US support f. N8588 (N8688); PrimeLife com.(N8696).	Editor's report (N8924); DoC (N8803); Text f. 3rd CD (N8804).

3rd CD Consideration

In accordance with resolution 4 (in SC 27 N8828rev) of the 9th SC 27/WG 5 meeting held in Melaka, Malaysia (April 2010), the attached document is hereby circulated for a 3-month 3rd CD letter ballot closing by **2010-09-12.**

1) Member body (for country code according to ISO 3166, e.g. CN for China.)

Secretariat ISO/IEC JTC 1/SC 27
DIN Deutsches Institut für Normung e.V., Burggrafenstrasse 6, 10787 Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile: + 49 30 2601-1723; E-mail: krystyna.passia@din.de; HTTP://www.jtc1sc27.din.de/en

Explanatory Report (2nd page)			
Status	**SC 27 Decision**	**Reference Documents**	
		Input	**Output**
Study Period (SP)	Recommendation 15 of SC 27 Heads of Delegation meeting (N4340), Oct. 2004.	US NWIP (N4252)	Call f. Contr. (N4xxx); Call f. Rapporteur (N4xxx).
Study Period (SP)	Recommendation of Ad Hoc meeting on IdM (N4580), Apr. 2005	SoContr (N4377); BE contr. (N4448); US contr. (N4458); DE nomination f. Rapporteur (N4391); TC 68/SC 2 Letter (N4458); TC 215 LO's Report (N4457).	Report of Ad Hoc, Apr. 2005 (N5480); Draft Text f. NWIP (N4581)
Study Period (SP)	*17th SC 27 Plenary Resolutions 32 & 39 (N4599).*		Appointment of Rapporteurs; Extention of SP by 6 months; 1st outline f. 1st WD (N4721)
New Work Item Proposal (NWIP)	17th SC 27 Plenary , Apr. 2005, resolution 18 (N4599).	Report on Ad Hoc, Apr. 2005 (N4580)	*Call f. Project Editor (N4615); Text for NWIP (N4581)*
NP 24760 (Outline f. 1st WD) Study Period (SP)	Recommendations of Ad Hoc (N4879), Nov. 2005	Rapporteurs' Report (N4776); SoV (N4670); SoCom. (N4785); US com. (N4722); The Open Group contr. (N4780).	*Report of Ad Hoc (N4879), Nov. 2005.*
1st WD 24760 Study Period (SP)	Recommendations of Ad Hoc (N5184), May 2006		*Report of Ad Hoc (N5184), May 2006; DoC (N5074r); Text f. Prelim. Draft (N5056r)*
	18th SC 27 Plenary May 2006, Resolution 2 (N5199); Transfer to WG 5 as per res. 41 (N5199)	*Rappoertuer's presentation / Report (N5182, N5184)*	*Text f. 1st WD (N5056rev1).*

[2] Subdivision subject to JTC 1 endorsement

ISO/IEC JTC 1/SC 27 N8804

Date: 2010-06-11

ISO/IEC CD 24760-1.3

ISO/IEC JTC 1/SC 27/WG 5

Secretariat: DIN

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

Technologies de l'information — Techniques de sécurité — Gestion d'identité cadre — Partie 1: Terminologie et concepts

Error! AutoText entry not defined.

Contents

Page

Figures

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*.

This second/third/... edition cancels and replaces the first/second/... edition (), [clause(s) / subclause(s) / table(s) / figure(s) / annex(es)] of which [has / have] been technically revised.

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*

— *Part 2*): Reference architecture and requirements*

— *Part 3*):Practice*

*) *Subject to JTC 1 endorsement on the on the subdivision of the project*

Introduction

It is common for computer systems to make automated decisions based on the *identity* of a person, piece of equipment or piece of software connected to it. Such decisions may concern access to applications or other resources.

To address the need to efficiently and effectively implement systems that make identity based decisions this series of International Standards specify a framework for the issuance, administration, and use of data that serves to identify individuals, organizations and information technology components operating 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.

This series of International Standard specifies fundamental concepts and operational structures of identity management with the purpose to realize information systems that can meet business, contractual, regulatory and legal obligations.

This International Standard specifies the terminology and concepts for identity management, to promote a common understanding in the field of identity management and privacy protection. It also provides a bibliography of documents related to standardization of various aspects of identity management.

This series of international standards consist of the following parts:

- Part 1: Terminology and concepts
- Part 2: Reference architecture and requirements
- Part 3: Practise

This series of International Standard is also intended to provide foundations for other identity management related international standards including:

- ISO/IEC 29100 Privacy framework,
- ISO/IEC 29101 Privacy Reference Architecture,
- ISO.IEC 29146 A framework for access management,
- ISO/IEC 29155 Entity Authentication Assurance.

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

1 Scope

This International Standard:

— defines terms for identity management,

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

This International Standard is applicable to any information system where information relating to identities is processed or stored.

A bibliography of documents describing various aspects of managing identity information 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.

ISO/IEC 10181:1996	Information technology — Open Systems Interconnection — Security frameworks for open systems: Security audit and alarms framework
ISO/IEC 24760-2 —†	Information technology — A framework for identity management — Part 2: Reference architecture and concepts
ISO/IEC 24760-3 —†	Information technology — A framework for identity management — Part 3: Practice
ISO/IEC 29100 —†	Information technology — Security techniques — Privacy framework
ISO/IEC 29101 —†	Information technology — Security techniques — Privacy reference architecture
ISO/IEC 29115 —†	Information technology — Security techniques — Entity authentication assurance

3 Terms and definitions

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

3.1 General terms

3.1.1
entity
item of interest, inside or outside an ICT 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 network interface card, a website.

† to be published.

3.1.2
identity
partial identity
ID
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 Usually an identity allows entities to be distinguished within a domain of applicability.

NOTE 3 ITU-T X1252[[9]] specifies the unique distinguishing use of an identity, in this document the term identifier implies this aspect.

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

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

3.1.4
identifier
one or more **attributes (3.1.3)** that uniquely characterize an entity in a specific **domain (3.2.3)**

NOTE An identifier may be suitable for use outside 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 IP address, or a Universal Unique Identifier (UUID) can all be used as identifiers.

3.1.5
domain of origin
property of a**n attribute (3.1.3)** that specifies the domain where the attribute value has been created

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 to reference its domain of origin, e.g. an ISO country code for a passport number.

EXAMPLE The domain of origin of a club-membership number is the specific club that assigned the number.

3.1.6
reference identifier
IR
identifier (3.1.4) in a **domain (3.2.3)** with a value that remains the same for the duration of the existence of the **entity (3.1.1)** and is not associated with another entity for a period specified in a policy after the entity ceases to exist

NOTE 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.

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

3.2 Use of identity

3.2.1
identification
recognition of an **entity (3.1.1)** in a particular **domain (3.2.3)**

NOTE 1 The process of identification uses claimed, observed or assigned attributes.

NOTE 2 Recognition is a process to determine that presented identity information associated with a particular entity meets all the requirements for the entity to be recognized as distinct from other entities in a particular domain.

NOTE 3 Identification is usually an authentication process to obtain a specific level of confidence in the result.

3.2.2
validation
process to determine that presented **identity information (3.2.5)** 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 Validation 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 ITU-T X1252[[9]] uses the term context, this document prefers the term domain.

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

3.2.4
indirect identifier
attribute (3.1.3) associated with in an **entity (3.1.1)** in a **domain (3.2.3** that is based on an unique values in an **identifier (3.1.4)** for the same **entity (3.1.1)** from a different **domain**

EXAMPLE The number of a driver's license in a membership record.

3.2.5
identity information
set of values of **attributes (3.1.3)** in an **identity (3.1.2)**

3.2.6
role
specification of the interactions available to an **entity (3.1.1)** in a **domain (3.2.3**)

NOTE 1 A role of an entity can be made explicit as an attribute, e.g. by a credential.

NOTE 2 A role typically implies a collection of privileges to access services or use resources available in a domain.

3.2.7
authorization
approval of a request by an **entity (3.1.1)** to perform an action upon evaluation of applicable policy

NOTE 1 Authorization often happens in a successful authentication process as may be specified in the authorization policy.

NOTE 2 Authorization may be made explicit with the addition of a set of attributes that are valid for the duration of the approval.

NOTE 3 The activity permitted after authorization typically involves the access or use of a resource pertaining to the domain.

3.3 Authenticating Identity

3.3.1
claimant
entity (3.1.1) that is the subject in an **authentication** (**3.3.2**)

NOTE A possible interaction between a claimant and a verifier is specified in ISO/IEC 9798, *Entity Authentication***.**

3.3.2
authentication
formalized process of **identification (3.2.1)** that if successful results in an **authenticated identity (3.3.3)** for a **claimant, (3.3.1)**

NOTE 1 The authentication process involves tests by a verifier on one or more identity attributes provided by a claimant to determine (with the required degree of assurance) their correctness.

NOTE 2 Authentication typically involves the use of a policy to specify a required assurance level for the result after a successful completion.

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

NOTE 4 Adapted from ISO/IEC10181-2.

3.3.3
authenticated identity
identity (3.1.2) for an **entity (3.1.1)** created as result of **authentication (**3.3.2**)**

NOTE 1 An authenticated identity typically contains information obtained in the authentication process, e.g., the assurance level 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.

3.3.4
identity information authority
IIA
entity (3.1.1) related to a particular **domain (3.2.3)** that can make assertions 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 a domain in which the attributes it can make assertions on have a particular significance, for instance the domain of origin.

NOTE 2 The activity of an identity information authority may be subject to a policy on privacy protection.

3.3.5
identity information provider
IIP
entity (3.1.1) that makes available **identity information (3.2.5)**

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.

3.3.6
credential
attribute (3.1.2) constructed to facilitate **authentication(**3.3.2**)**

NOTE 1 A credential is typically constructed to facilitate *data* authentication of its value and possibly of other identity information in an identity.

NOTE 2 A credential can be printed on paper that typically has been prepared in a manner to assert it as valid.

NOTE 3 In this document the term credential is used in a specific sense referring to an attribute, and not an identity that contains such an attribute.

NOTE 4 The data authentication supported by a credential usually allows asserting the scope of application and the timeliness of the value.

3.3.7
verifier
entity (3.1.1) that operates the functions necessary to complete **authentication (3.3.2**)

NOTE A verifier may be the same as or act on behalf of the entity that controls identification of entities for a particular domain.

3.3.8
relying party
entity (3.1.1) that relies on the validity of **identity information (3.2.5***)*

NOTE A relying party is exposed to risk caused by incorrect identity information. Typically it has a trust relationship with identity information authorities.

3.4 Management of identity

3.4.1
identity management
IM
processes and policies involved in managing the value and life cycle of **attributes (3.1.3**) of **identities (3.1.2)** known in a particular domain

NOTE 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 (**3.3.2**)** based on **identity evidence (3.4.4)** that is performed as the condition for **enrolment (3.4.3)**

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

NOTE 1 Enrolment involves identity registration typically preceded by identity proofing

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 (3.2.5) for an **entity (3.1.1)** required for **authentication(**3.3.2**)** of an **entity**

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 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 quality 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(3.1.1**) 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 an **reference identifier (3.1.6**)

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

3.5 Federation

3.5.1
federated identity
identity (3.1.2**)** with **attributes (3.1.3)** 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 (3.2.5)** 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 and 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
identity assertion
statement by an **identity information authority (**3.3.4**)** used by a **relying party (**3.3.8**)** for **authentication (**3.3.2**)** of an **identity (3.1.2)**

NOTE An identity assertion may be the cryptographic proof of a successful authentication, created with algorithms and keys agreed in the identity federation.

3.5.4
single-sign-on identity
SSO identity
identity (3.1.2) that includes an **identity assertion (3.5.3)**

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

The terms defined in this clause relate to entities that are human individuals, in jurisdictions where other 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.

3.6.1
Personally identifiable information
PII
information (a) that uniquely links to an **person** or (b) can be used to create a unique link, to, contact, or to locate the **person** to which this information pertains, or (c) from which identification or contact

information of a **person** can be derived, or (d) that is linked with PII, including personal characteristics or preferences

NOTE Adapted from ISO/IEC 29100 to conform to the definition of terms in this document.

3.6.2
selective disclosure
principle of **identity management (3.4.1)** that gives an **person** a measure of control over the **identity information** (3.2.5) that may be transferred to a receiver, e.g. during **authentication (**3.3.2**)**

3.6.3
minimal disclosure
principle of **identity management (3.4.1)** to restrict the transfer of **identity information (3.2.5)** to the minimal number of attributes strictly required for a particular purpose

3.6.4
pseudonym
identifier (3.1.4) that contains no **PII (3.6.1)** yet containing sufficient **identity information (3.2.5)** to allow a **verifier (3.3.7)** to link to a known **identity (3.1.2)**

NOTE 1 A pseudonyms can be used to reduce privacy risks 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 or a pseudonymous credential.

3.6.5
anonymous identifier
identifier (3.1.4) that contains no **PII (3.6.1)**

NOTE An anonymous identifier contains sufficient identity information to allow a verifier to distinguish two entities while not being able to link to a specific known identity.

EXAMPLE A pseudonym created in one domain might be used as an anonymous identifier in another domain.

4 Symbols and abbreviated terms

DA	Domain (of applicability)
ICT	Information and Communication Technology
ID	Identity
IM	Identity Management
IMS	Identity Management System
IIP	Identity Information Provider
IIA	Identity Information Authority
ISMS	Information Security Management System
PII	Personally Identifiable Information
RI	Reference identifier
RP	Relying Party
SSO	Single Sign On
UUID	Universal Unique Identifier

5 Identity

5.1 General

An identity of an entity may serve to uniquely characterize the entity in a particular domain (of applicability).

NOTE This aspect of uniqueness is widely understood as the essence of identity, however in this document uniqueness is only one of the factors considered.

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 1 The term entity must be taken in a broad sense and 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 may be seen as entity in this standard and has a single, whole existence. It can be described by many different attributes, and different sets of these attributes form different identities for the same human entity.

The identity of an entity serves to make known relevant information of the entity in its interactions with the services and 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 In some cases the term partial identity may 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 of an entity in a domain. The preferred term in this document is identity.

A domain should deploy an identity management system conforming to this International Standard to manage the identity information of the entities it intends to recognize.

5.2 Identifier

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

- For exclusive use in the domain of origin in which it has been constructed to distinguish the entity as unique,
- Available to the entity for exclusive use in the domain of origin,
- Suitable for use in domains other than the domain of origin.

A physical object may represent an identifier. This physical object may be equipped with security features to

- Assert the integrity of the attribute values in the identifier,
- Provide a specific level of assurance when the identifier is used in authentication,
- Protect confidentiality of attribute values, or
- Facilitate validation of the identity information contained.

NOTE 1 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.

NOTE 2 A physical object representing an identifier may itself be an entity (as used in this document) with an attribute to uniquely distinguish it from another identifier object originating from the same domain. For example, a passport as identifier of a person (entity) as a citizen of a country (domain) may be considered an entity that has an identity containing a unique passport number.

5.3 Identity information

When a new identity is created for an entity a domain may create new attributes for the new identity. Identity information contained in new attributes may be:

- Any information to facilitate the interaction between the entity and the domain for which the identity is created,
- Any information that can facilitate future identification of the entity, including description of aspects of the physical existence of the entity,
- Any information that can facilitate 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 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. The metadata may be included in the identity information.

Identity information and its associated metadata may be changed.

An identity management system in accordance with this International Standard shall specify the conditions and procedures for creating and modifying identity information and associated metadata (see clause 9). These specifications may distinguish between a number of tasks and activities, relating to the identity lifecycle (see clause 9.2), including:

- Requesting and receiving information from out-side sources,
- Verifying and validating,
- Qualifying and categorizing,
- Recording,
- Provisioning,
- Archiving, and
- Deleting.

NOTE In this document the existence of identity information for an entity in an IMS can be considered as establishing the ***existence*** of the entity in the domain supported by that IMS The physical existence of the entity is only loosely related to this use of existence in a domain. Archived information, however, means that the entity no longer exists in that domain.

6 Attributes

6.1 General

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

A clearly defined and documented semantics and syntax shall be specified for attributes.

6.2 Types of attribute

Attributes may be:

- Information about physical existence such as:
  - Biographical details,
  - Home or business address,
  - Employer,
  - Employment history,
  - Device location;
- Information describing the entities 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,
  - Social security number,
  - Citizenship number,
  - Passport number,
  - Manufacturer's serial number,
  - Network (MAC) address;
- Information assigned to the entity such as:
  - Title,
  - Role,
  - Digital signature,
  - 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 indicate:

- The range of values of an attribute,
- That its value is unique,
- The encoding of the attribute value,
- The time of creation,
- The time of expiration,
- The method of establishing the value,
- The mechanism to obtain a human readable representation of an attribute value.

The domain of origin of an attribute may be explicitly specified as part of the (composite) attribute value, e.g. as a unique reference to a system specification document.

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.

7 Identification

7.1 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.

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

Identification may result in establishing entitlements for the entity when interacting with services and resources provided by the domain. In a system where access to resources or services involves identity-related risks the required assurance level in identification shall be specified based on the type of resource and the type of access to the resource for which an entitlement may be established (see clause 7.2).

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

Identification may be for a single purpose specific to the domain or for multiple different purposes.

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

- (Risk-Based) A determination of the identity related risks associated with different resources and services and the different modes of access to them;
- (Equivalency) The assurance level in the identification result is based in equal measure on the quality of the identity information and on the mechanisms and algorithms to assert their correctness;
- (Proportionality) A particular assurance level specified mitigates the determined risks;
- (Minimal) Identification shall make its determination from a minimal set of attributes required for a purpose.

7.2 Authentication

Authentication of an identity of an entity gives relying parties a specific assurance level in the correctness and applicability of the identification result. International Standard ISO/IEC 29115 specifies levels of assurance.

NOTE The term identity assurance is often used instead of *identification at a specific assurance level*.

An identity management system conforming to this International Standard that provides authentication shall specify:

- Policies for validation,
- Mechanisms for establishing the validity and correctness of an authenticated identity,
- The period of validity of an authenticated identity,
- Mechanisms for recording and auditing.

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.

8 Privacy

An identity management system conforming to this International Standard shall obey all statutory and regulatory requirements to protect the privacy of the human entities it interacts with. The design of such a system shall clearly specify any PII it handles.

An identity management system conforming to this International Standard may provide capabilities to:

- Implement policies for minimal disclosure,
- Authenticate users of identity information,
- Minimize the ability to link identities,
- Record and audit the use of identity information,
- Protect against inadvertently generating information, for example in logs and audit trails
- Implement policies for selective disclosure,
- Implement policies to engage the user for explicit direction or consent for activities related to their PII.

An identity management system conforming to this standard should support the use of pseudonyms.

Requirements for the handling of PII are given in:

- ISO/IEC 29100, Privacy framework;
- ISO/IEC 29101, Privacy Architecture.

In contrast, systems that use identifiers containing PII would not be constrained by the requirements above. Full disclosure and conveyance of identity information would characterize such systems

9 Managing Identity Information

9.1 General

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

9.2 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 In the perspective of an identity management system an unknown entity does not exist.

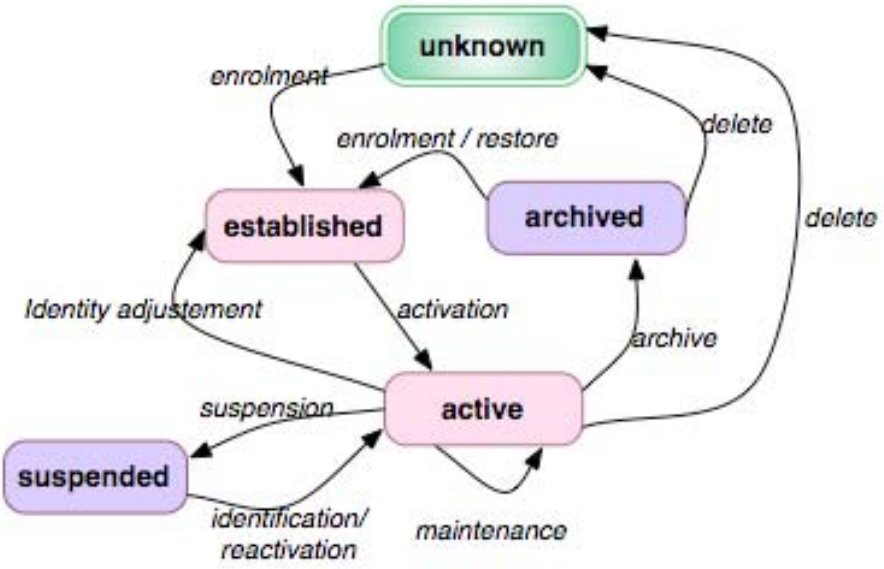

Figure 1: Identity lifecycle

The following stages in the lifecycle may be distinguished:

Established, required identity information has been validated in the enrolment (see clause 9.5) and additional information, e.g. a reference identifier, has been generated and the information has been registered (see clause 9.3).

Active, identity information is present in the identity management system that allows the entity to utilize the resources available in a domain of applicability, for instance the entity is engaged in an active session in an IT system.

Suspended, identity information is present in the identity management system indicating that the entity cannot utilize the resources of the domain.

Archived, identity information for an entity is present in the identity register where the entity no longer exists in the domain. When the entity re-enrols the archived information may be used to establish its new identity.

9.3 Validation

A new attribute handled by an identity management system shall be examined to ensure 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,
- Originates from a reliable source.

NOTE Validation provides input to identification and its result is specific to the particular circumstances, e.g. location and time of that process.

Validation 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.

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

Validation may include an examination of the validity of attributes not required for the identification process proper that may be used in the domain after identification.

9.4 Registration

An identity management system may enter identity information for the entities it intends to recognize in an identity register.

NOTE After registration an entity has become known in the domain by way of the identity register and the lifecycle of its identity has started. The identity information that is stored in the register is the registered identity of an entity.

Registration may be for a single use, for a specific duration or indefinite.

Unless prevented by legal requirements indefinite registration shall end at a request by or on behalf of the entity for removal. After deletion all identity information for the entity shall be removed from the identity register. However, a domain may retain some information for archival and auditing purposes, and the identity remains registered in the life-cycle stage *archived*. In particular a reference identifier may be retained to prevent its reuse as 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 managements system.

NOTE If an reference identifier is not used internally for a domain it may be available for use as an attribute in the identity an entity can be present to other domains during identification.

The identity stored in an identity register may have multiple unique reference identifiers an additional reference identifier may indicate a partial identity.

NOTE A particular domain may allow multiple distinct registrations of an identity for the same entity. In this case each registered identity effectively belongs to a different entity.

An identity register shall provide one specific reference identifier to refer to the complete identity information stored for a particular identity.

9.5 Enrolment

Enrolment may result in the creation of one or more identifiers for the enrolled entity. The value of the unique attribute(s) in a created identifier 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.

NOTE 1 If the entity determines the value of an identifier created by enrolment the IMS must ensure its uniqueness.

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

9.6 Maintenance

In maintenance one or more of the attributes or attribute values may be changed.

An identity management system shall specify mechanisms for maintaining the integrity and accuracy of attributes it stores. It shall maintain the stored identity 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.

9.7 Implementation Aspects

The following aspects may characterize an identity management system.

Centralization — 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 may have multiple identity registers and multiple points of control over enrolment and access to registered identity information.

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

User focus — An identity management system is user focused when it allows the entities to play an active role in the management of the identity information stored in the identity register (see clause 8).

User focus is important in the implementation of privacy policies.

Federation — Federation allows an identity management system that does not contain the required identity information in its own register to trust statements with identity information made by another identity management system. In this case the other identity managements system acts as an identity information authority.

Identity federation is intended for identity management in a context where entities interact with multiple domains in order to:

- Facilitate identity proofing,
- Facilitate authentication,
- Facilitate enrolment,
- Improve user experience.

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

Bibliography

[1] ISO/IEC 9594-2, ITU-T X.501 Information technology - Open Systems Interconnection - The Directory: Models

[2] ISO/IEC 9594-8, Information technology | ITU-T Recommendation X.509, Open Systems Interconnection -- The Directory: Authentication framework

[3] ISO 19092:2008 Financial services - Biometrics - Security framework

[4] ANSI INCITS 359-2004, Role Based Access Control

[5] ISO/IEC 29100 Privacy framework

[6] ISO/IEC 29101 Privacy Reference Architecture

[7] ISO/IEC 29155 Entity Authentication Assurance

[8] ISO/IEC 29146 A framework for access management

[9] ITU-T recommendation X1252 Baseline identity management terms and definitions

[10] ITU-T recommendation Y 2720 NGN identity management framework <http://www.itu.int/rec/T-REC-Y.2720-200901-I>

[11] Identity Management, Document No: W041, Copyright © [March 2004] The Open Group (Skip Slone and The Open Group Identity Management Forum), <www.opengroup.org/onlinepubs/7699959899/toc.pdf>

[12] EU Project FIDIS (Future of Identity in the Information Society): Inventory of topics and clusters; D 2.1, 2004; www.fidis.net

[13] EU Project FIDIS (Future of Identity in the Information Society): Set of use cases and scenarios; D 2.2; 2005; <www.fidis.net>

[14] EU Project FIDIS (Future of Identity in the Information Society): Models; D 2.3; 2005; <www.fidis.net>

[15] EU Project FIDIS (Future of Identity in the Information Society: Structured Overview on Prototypes and Concepts of Identity Management Systems, D 3.1, 2005; <www.fidis.net>

[16] EU Project FIDIS (Future of Identity in the Information Society: Study on Mobile Identity Management, D 3.3, 2005; <www.fidis.net>

[17] US Office of Management and Budget, 2003. E-authentication guidance for federal agencies (M-04-04); <www.whitehouse.gov>

[18] US National Institute of standards and Technology, 2006. Electronic authentication guideline (NIST 800-63), version 1.0.2; <www.csrc.nist.gov>

[19] US National Institute of standards and Technology, 2005. Information Processing Standard (FIPS) 201, Personal Identity Verification (PIV) of Federal Employees and Contractors; <www.csrc.nist.gov>

Index of terms