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 iv
Introduction v
1 Scope 1
2 Normative references 1
3 Terms and definitions 1
3.1 General terms 1
3.2 Identification 3
3.3 Authenticating an identity 4
3.4 Management of identity 5
3.5 Federation 6
3.6 Privacy protection 7
4 Symbols and abbreviated terms 8
5 Identity 8
5.1 General 8
5.2 Identity information 9
5.3 Identifier 10
6 Attributes 10
6.1 General 10
6.2 Types of attribute 11
6.3 Domain of origin 11
7 Managing identity information 12
7.1 General 12
7.2 Identity lifecycle 12
8 Identification 14
8.1 General 14
8.2 Verification 15
8.3 Enrolment 15
8.4 Registration 15
9 Authentication 16
10 Maintenance 16
11 Implementation aspects 16
12 Privacy 17
Bibliography 18
Index of terms 20

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.