INTERNATIONAL STANDARD

ISO/IEC 24760-2

First edition
2015-06-01

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

Part 2: Reference architecture and requirements

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

Partie 2: Architecture de référence et exigences

Reference number
ISO/IEC 24760-2:2015(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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT), see the following URL: Foreword — Supplementary information.

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee, SC 27, *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*

— *Part 2: Reference architecture and requirements*

The following part is under preparation:

— *Part 3: Practice*

Further parts may follow.

Introduction

Data processing systems commonly gather a range of information on its users be it a person, piece of equipment, or piece of software connected to it 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, this part of 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 defines a reference architecture for an identity management system that includes key architectural elements and their interrelationships. These architectural elements are described in respect to identity management deployments models. This part of ISO/IEC 24760 specifies requirements for the design and implementation of an identity management system so that it can meet the objectives of stakeholders involved in the deployment and operation of that system.

This part of ISO/IEC 24760 is intended to provide a foundation for the implementation of other International Standards related to identity information processing such as

— 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 framework*, and

— ISO/IEC 29146, *Information technology — Security techniques — A framework for access management.*

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

Part 2: Reference architecture and requirements

1 Scope

This part of ISO/IEC 24760

— provides guidelines for the implementation of systems for the management of identity information, and

— specifies requirements for the implementation and operation of a framework for identity management.

This part of ISO/IEC 24760 is applicable to any information system where information relating to identity is processed or stored.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 24760-1, *Information technology — Security techniques — A framework for identity management — Part 1: Terminology and concepts*

ISO/IEC 29115, *Information technology — Security techniques — Entity authentication assurance framework*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 24760-1 and the following apply.

3.1
documented design
authoritative description of structural, functional, and operational system aspects

Note 1 to entry: A documented design is the documentation created to serve as guidance for the implementation of an ICT system.

Note 2 to entry: A documented design typically includes the description of a concrete architecture of the ICT system.

3.2
identity management authority
entity responsible for setting and enforcing operational policies for an *identity management system* (3.3)

Note 1 to entry: An identity management authority typically commissions the design, implementation, and deployment of an identity management system.

EXAMPLE The executive management of a company deploying an identity management system in support of its services.

3.3
identity management system
mechanism comprising policies, procedures, technology, and other resources for maintaining identity information including metadata

Note 1 to entry: An identity management is typically used for identification or authentication of entities. It can be deployed to support other automated decisions based on identity information for an entity recognized in the domain of application for the identity management system.

3.4
principal
subject
entity to which identity information in an *identity management system* (3.3) pertains

Note 1 to entry: In the context of privacy protection requirements, a principal refers to a person.

3.5
invalidation
process performed in an *identity management system* (3.3) when a particular attribute is no longer valid for a particular entity to mark the attribute invalid for future use

Note 1 to entry: Invalidation of attributes may be part of updating the attribute value, for instance, with a change of address.

Note 2 to entry: Invalidation typically takes place for an attribute that is determined as no longer valid before the end of a validity period that had previously been associated with it.

Note 3 to entry: The term "revocation" is commonly used for invalidation of attributes that are credentials.

Note 4 to entry: Invalidation typically happens immediately after the determination that an attribute is no longer valid for a particular entity.

3.6
regulatory body
body tasked and empowered by law, regulation, or agreement to supervise the operation of *identity management systems* (3.3)

3.7
stakeholder
individual, team, organization, or classes thereof having an interest in a system

[SOURCE: ISO/IEC 42010]

4 Symbols and abbreviated terms

ICT Information and Communication Technology

IMS Identity management system

PII Personal identifiable information

5 Reference Architecture

5.1 General

This clause describes the architectural elements of an identity management system and their interrelationships.

The documented design for the architecture of an identity management system should be based on ISO/IEC 42010.

NOTE The reference architecture and architecture description defined in this standard are based on ISO/IEC 42010

The documented design for the architecture of an identity management system should specify the system in its deployed context based on *stakeholders* and *actors* defined in this part of ISO/IEC 24760. Business-level actors are stakeholders. Some stakeholders do not interact with the system. The documented design shall address requirements for both actor and non-actor stakeholders. The documented design shall exhaustively describe the actors.

A documented design of an identity management system conforming to this part of ISO/IEC 24760 should use an appropriate architecture description language and reference architecture components and functions by terms defined in this International Standards.

5.2 Architecture elements

5.2.1 Overview

Elements in this reference architecture are

— stakeholders (5.3.1),

— actors (5.3.2),

— views (5.3, 5.4),

— models (5.3.3, 5.3.4, 5.3.5, 5.4.1, 5.4.3),

— components (5.4.1),

— processes (5.4.2), and

— information flows and actions (5.4.2).

5.2.2 Viewpoints

5.2.2.1 General

The documented design of an identity management system shall include a context view and a functional view. It may include a physical view. The documented design may contain other views, e.g. an information view.

NOTE The required minimal set of viewpoints describes the system's interactions with its environment and the system's internal components and interactions.

The description of a view should be focused. Diagrams in the view descriptions should be accompanied with text defining the elements shown.

NOTE The description of viewpoints in this clause is based on Reference [2].

5.2.2.2 Context viewpoint

Definition — In the documented design the context viewpoint describes relationships, dependencies, and interactions between the system and its environment (the people, systems, and external entities with which it interacts).

Concerns — System scope and responsibilities, identity of external entities and services and data used, nature and characteristics of external entities, identity and responsibilities of external interfaces, nature

and characteristics of external interfaces, other external interdependencies, impact of the system on its environment, and overall completeness, consistency, and coherence.

Models — A context viewpoint may contain a context model, use cases and interaction scenarios. The context model is an informal box-and-line diagram that shows the system under discussion as a black box with interfaces, top-level interactions and dependencies on external entities. See 5.3.3.

Points to take care of — Missing or incorrect external entities, missing implicit dependencies, loose or inaccurate interface descriptions, inappropriate level of detail, scope creep, implicit or assumed context or scope, overcomplicated interactions, overuse of jargon.

5.2.2.3 Functional viewpoint

Definition — In the documented design the functional viewpoint describes the key functional elements with operational responsibilities, interfaces, and primary interactions.

Concerns — Refers to functional capabilities, external interfaces, internal structure, and functional design philosophy.

Models — A functional viewpoint may contain a component model, physical model or an infrastructure model.

In the documented design the functional viewpoint shall identify standards and guidelines applicable to each of the functions it describes.

See 5.4 for guidance on specifying a function viewpoint.

5.3 Context view

5.3.1 Stakeholders

5.3.1.1 General

This part of ISO/IEC 24760 recognizes the following direct and indirect stakeholders of primary importance

— principal,

— identity management authority,

— identity information authority,

— relying party,

— regulatory body,

— auditor, and

— consumer/citizen representative or advocate.

Each stakeholder performs a separate function in the identity management system. These functions imply specific responsibilities and liabilities. With the exception of regulatory bodies and consumer representatives, stakeholders interact with an identity management system, and thus are present in the reference architecture as actors (see 5.3.2).

Concerns of stakeholders in an identity management system are described in the following sub-clauses and should be addressed in the design, implementation and operation of the system.

5.3.1.2 Principal

Concerns of a principal in an identity management system include

— correctness of identity information collected, processed and stored,

— protection of privacy,

— minimisation of identity information collected, processed and stored by the identity management system,

— minimisation of identity information usage by the identity management system in its domain of applicability,

— errors in identification including false negative and false positive identification and the detection and handling of errors,

— knowledge of and consent to, identity information sharing with third parties,

— being correctly represented by identity information captured, processed or stored,

— correctness of operations in the delivery of services and the access to resources made available based on the attributes presented in a specific situation,

— collection, processing and storage of identity information only occurs with its informed consent,

— equitable treatment in its interactions with the system, and

— an easily understandable, effective, appropriate user interface.

NOTE a concern of a principal that relates to a third party service using identity information obtained from the identity management system is not a concern about the identity management system and therefore not in scope for this standard.

5.3.1.3 Identity management authority

Concerns of the identity management authority in an identity management system include

— definition of identity management objectives for the domain(s) served by the identity management system,

— specification of policies to maintain identity management objectives for the domain(s) served by the identity management system,

— fulfilling the business objectives of the identity management system with respect to principals and users of identity information,

— that the identity information provided by each principal is accurate and pertains to that principal to a specific level of assurance, and

— compliance with regulation.

5.3.1.4 Identity information authority

Concerns of an identity information authority in an identity management system include

— correctness of identity information,

— meeting requirements from relying parties,

— compliance with regulation, and

— meeting business obligations with principals.

5.3.1.5 Relying party

Concerns of a relying party in an identity management system include

— confidentiality, availability and integrity and applicability to a principal of identity information,

— provisioning of accurate identity information pertaining to relevant principals at the required level of assurance,

— effective, documented and secure interfaces,

— conformance to regulation applicable to its operations, and

— effective mechanism and procedures for auditing.

5.3.1.6 Regulatory body

As an external independent organization, concerns of a regulatory body in an identity management system include

— the proper documentation of operating policies,

— correctness of operation, in particular, in applying operational polices,

— proper accountability and audit of system operations,

— compliance of operational policy and operational practice with legal and regulatory requirements,

— effective reporting on system operations, including control effectiveness, incidents, and actions taken in overcoming incidents, and

— effective response to incidents that violate, or have a potential to violate privacy protection.

NOTE Effectively, auditors, as actors in an identity management system (see 5.3.2.9), in inspecting the operations of an identity management system (see 5.4) may represent the interests of regulatory bodies.

5.3.1.7 Consumer/citizen representative or advocate

Consumer/citizen advocates are individuals or groups that emerge from civil society and try to protect consumers and citizens from surveillance and lobby for improved privacy regulations.

Consumer/citizen representatives are individuals appointed by a principal or selected by consumer organisations to represent a consumer or citizen in its rights with respect to privacy.

Consumer/citizen representative and advocates' main concerns are

— transparency, notification, compliance and protection against complex legal language, and

— access of services to disadvantaged populations

NOTE 1 Consumer and citizen representatives participate in recognised multi-stakeholder societal processes such as governance and establish good practices and requirements to be met by those providing goods and services to consumers and citizens.

NOTE 2 Consumer and citizen representatives are selected, briefed and where necessary trained to ensure that they participate through reasonable and reasoned discussion, based wherever possible on good quality evidence.

5.3.2 Actors

5.3.2.1 General

An actor interacts with an identity management system to participate in identity management operations. An entity may interact with the same identity management system as multiple, different actors. The document design shall define all interactions by any actor supported by the system.

The documented design should describe actor interactions in terms of the functions that the interactions relate to. Where an actor that interacts with the identity management system needs to be authenticated before interactions are allowed to proceed, the documented design shall specify the basis for authentication (e.g. entity based; role based etc. authentication), the authentication method and the assurance level required for each interaction as defined in ISO/IEC 29115.

NOTE One purpose of specifying actors in the design of an identity management system is to be able to describe all intended interactions with the system.

A documented design may recognize the following actors:

— principal;

— identity management authority;

— identity registration authority

— relying party;

— identity information provider;

— identity information authority;

— verifier;

— auditor.

The documented design shall specify the level of assurance needed to identify and authenticate entities requesting access to identity information contained in its identity management system as specified in ISO/IEC 29115. The level of assurance may be different for different types of information and the type of access granted i.e. read, write etc. Authorization may be implemented as specified in ISO/IEC 29146.

5.3.2.2 Principal

A principal is an actor who provides identification information to establish and validate its identity within identification management processes. The Principal has the following responsibilities

— as an entity when applying to become registered in a domain of applicability, to provide accurate identity information for enrolment as a new principal,

— as system user once enrolled, to request to be recognized by the identity management system and to be approved for access to services or use of resources available in the domain of applicability associated with the identity management system, and

— as the subject of observation to obtain identity information, to facilitate the observation;.

NOTE As a subject of observation the identity information obtained is anonymous, until its relation to the principal has been established.

A principal can use an identity management system to

— request to be recognized by information in the identity management system and to be approved for access to services or use of resources available in the domain of applicability associated with the identity management system, and

— be informed, as human, of the identity information pertaining to itself is held in the identity management system and to request any errors in the identity information to be corrected

NOTE In appropriately defined circumstances, a legally authorised representative may act on behalf of a principal.

5.3.2.3 Identity management authority

An identity management authority is associated with a domain of applicability with the duty and capabilities to define and adjust business objectives for identity management in that domain and set management policies to meet these objectives.

An identity management authority uses policies to regulate the use of registered identity information. Policies may specify levels of service to provide including the level of assurance on identity information that may be provided by the identity management system. Policies may also specify how to obtain authorisation for access and modification of identity information in unforeseen circumstances.

The identity management authority shall define identity management objectives for a domain of applicability served by the identity management system operating under its authority. The identity management authority shall specify policies to meet identity management objectives for an associated domain.

Responsibilities of an identity management authority include

— to create, modify or revoke operational policies,

— to ensure legal and regulatory compliance of the policies and operation of the identity management system,

— to require and approve modification of mechanisms to establish a required level of assurance in entity authentication for access to identity information and system control functions

— to respond to incidents,

— to approve changes in the type of information recorded in the identity register

— to initiate regular audits, and

— to evaluate audit reports, in particular on the effectiveness of policies,

An identity management authority may enter into formal association with one or more other identity management authorities to form a "*federation*."

NOTE The purpose is to extend the domain of applicability for principals with the other domains of applicability in a federation. This extension is achieved with strictly controlled sharing of identity information.

In a federation, responsibilities of each identity management authority include:

— to provide a level of assurance of identity information that meets the specified requirement of any other member of the federation,

— to maintain control over access to the identity information contained in its identity management system,

— to ascertain that the level of assurance realized by any other member of the federation in authorizing access to identity information in the federated identity management systems meets its requirements for access to its own identity information,

— to operate with common policies for information sharing, and

— to specify policies to maintain its trust in the level of assurance of identity authentication.

