SLOVENSKI STANDARD
SIST EN ISO/IEC 24760-2:2023

01-januar-2023

Informacijska tehnologija - Varnostne tehnike - Okvir za upravljanje identitete - 2. del: Referenčna arhitektura in zahteve (ISO/IEC 24760-2:2015)

Information technology - Security techniques - A framework for identity management - Part 2: Reference architecture and requirements (ISO/IEC 24760-2:2015)

Informationstechnik - Sicherheitsverfahren - Rahmenwerk für Identitätsmanagement - Teil2: Referenzarchitektur und Anforderungen (ISO/IEC24760-2:2015)

Technologies de l'information - Techniques de sécurité - Cadre pour la gestion de l'identité - Partie 2: Architecture de référence et exigences (ISO/IEC 24760-2:2015)

Ta slovenski standard je istoveten z: **EN ISO/IEC 24760-2:2022**

ICS:

35.030	Informacijska varnost	IT Security

SIST EN ISO/IEC 24760-2:2023 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN ISO/IEC 24760-2

September 2022

ICS 35.030

English version

Information technology - Security techniques - A framework for identity management - Part 2: Reference architecture and requirements (ISO/IEC 24760-2:2015)

Technologies de l'information - Techniques de sécurité - Cadre pour la gestion de l'identité - Partie 2: Architecture de référence et exigences (ISO/IEC 24760-2:2015)

Informationstechnik - Sicherheitsverfahren - Rahmenwerk für Identitätsmanagement - Teil2: Referenzarchitektur und Anforderungen (ISO/IEC 24760-2:2015)

This European Standard was approved by CEN on 5 September 2022.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.

CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

Contents

Page

European foreword

The text of ISO/IEC 24760-2:2015 has been prepared by Technical Committee ISO/IEC JTC 1 "Information technology" of the International Organization for Standardization (ISO) and has been taken over as EN ISO/IEC 24760-2:2022 by Technical Committee CEN-CENELEC/ JTC 13 "Cybersecurity and Data Protection" the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by March 2023, and conflicting national standards shall be withdrawn at the latest by March 2023.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN-CENELEC shall not be held responsible for identifying any or all such patent rights.

Any feedback and questions on this document should be directed to the users' national standards body. A complete listing of these bodies can be found on the CEN and CENELEC websites.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

Endorsement notice

The text of ISO/IEC 24760-2:2015 has been approved by CEN-CENELEC as EN ISO/IEC 24760-2:2022 without any modification.

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)

COPYRIGHT PROTECTED DOCUMENT

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