Information technology - Security techniques - A framework for identity management - Part 3: Practice (ISO/IEC 24760-3:2016)

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

See Eesti standard EVS-EN ISO/IEC 24760-3:2022 sisaldab Euroopa standardi EN ISO/IEC 24760-3:2022 ingliskeelset teksti.	This Estonian standard EVS-EN ISO/IEC 24760-3:2022 consists of the English text of the European standard EN ISO/IEC 24760-3:2022.
Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas.	This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation and Accreditation.
Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 21.09.2022.	Date of Availability of the European standard is 21.09.2022.
Standard on kättesaadav Eesti Standardimis-ja Akrediteerimiskeskusest.	The standard is available from the Estonian Centre for Standardisation and Accreditation.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 35.030

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN ISO/IEC 24760-3

September 2022

ICS 35.030

English version

Information technology - Security techniques - A framework for identity management - Part 3: Practice (ISO/IEC 24760-3:2016)

Technologies de l'information - Techniques de sécurité - Cadre pour la gestion de l'identité - Partie 3: Mise en oeuvre (ISO/IEC 24760-3:2016)

Informationstechnik - Sicherheitsverfahren - Rahmenwerk für Identitätsmanagement - Teil 3: Umsetzung (ISO/IEC 24760-3:2016)

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

European foreword

The text of ISO/IEC 24760-3:2016 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 24760-3:2022 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 24760-3:2016 has been approved by CEN-CENELEC as EN ISO/IEC 24760-3:2022 without any modification.

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*, 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*

— *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 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, 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.

This part of 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 presents practices for identity management. These practices cover assurance in controlling identity information use, controlling the access to identity information and other resources based on identity information, and controlling objectives that should be implemented when establishing and maintaining an identity management system.

This part of ISO/IEC 24760 consists of the following parts:

— ISO/IEC 24760-1: Terminology and concepts;

— ISO/IEC 24760-2: Reference architecture and requirements;

— ISO/IEC 24760-3: Practice.

ISO/IEC 24760 is intended to provide foundations for other identity management related International Standards including the following:

— ISO/IEC 29100, Privacy framework;

— ISO/IEC 29101, Privacy reference architecture;

— ISO/IEC 29115, Entity authentication assurance framework;

— ISO/IEC 29146, A framework for access management.

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

Part 3: Practice

1 Scope

This part of ISO/IEC 24760 provides guidance for the management of identity information and for ensuring that an identity management system conforms to ISO/IEC 24760-1 and ISO/IEC 24760-2.

This part of ISO/IEC 24760 is applicable to an identity management system where identifiers or PII relating to entities are acquired, processed, stored, transferred or used for the purposes of identifying or authenticating entities and/or for the purpose of decision making using attributes of entities. Practices for identity management can also be addressed in other standards.

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*

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
identity management system
system comprising of policies, procedures, technology and other resources for maintaining identity information including meta data

[SOURCE: ISO/IEC 24760-2:2015, 3.3]

3.2
identity profile
identity containing attributes specified by an identity template

3.3
identity template
definition of a specific set of attributes

Note 1 to entry: Typically, the attributes in a profile are to support a particular technical or business purpose as needed by relying parties.

3.4
identity theft
result of a successful false claim of identity