International Standard

ISO/IEC 24760-3

Second edition
2025-09

Information security, cybersecurity and privacy protection — A framework for identity management —

Part 3: Practice

Sécurité de l'information, cybersécurité et protection de la vie privée — Cadre pour la gestion de l'identité —

Partie 3: Mise en œuvre

Reference number
ISO/IEC 24760-3:2025(en)

Horizontal document

© ISO/IEC 2025



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2025

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ... **iv**

Introduction ... **v**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms and definitions ... **1**

4 Abbreviated terms ... **2**

5 Mitigating identity related risk in managing identity information ... **2**
5.1 Overview ... 2
5.2 Risk assessment ... 3
5.3 Assurance in identity information ... 3
5.3.1 General ... 3
5.3.2 Identity proofing ... 3
5.3.3 Credentials ... 3
5.3.4 Identity profile ... 4

6 Identity information and identifiers ... **4**
6.1 Overview ... 4
6.2 Policy on accessing identity information ... 4
6.3 Identifiers ... 5
6.3.1 General ... 5
6.3.2 Categorization of identifier by the type of entity to which the identifier is linked ... 5
6.3.3 Categorization of identifier by the nature of linking ... 5
6.3.4 Categorization of identifier by the grouping of entities ... 6
6.3.5 Management of identifiers ... 6
6.3.6 Categorization of identifier by method of value creation ... 6

7 Auditing identity information usage ... **7**

8 Control objectives and controls ... **7**
8.1 General ... 7
8.2 Contextual components for control ... 8
8.2.1 Establishing an identity management system ... 8
8.2.2 Establishing identity information ... 10
8.2.3 Managing identity information ... 11
8.3 Architectural components for control ... 12
8.3.1 Establishing an identity management system ... 12
8.3.2 Controlling an identity management system ... 13

Annex A (informative) **Practice of managing identity information in a federation of identity management systems** ... **15**

Annex B (informative) **Identity management practice using attribute-based credentials to enhance privacy protection** ... **24**

Bibliography ... **31**

© ISO/IEC 2025 – All rights reserved

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.

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 or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This second edition cancels and replaces the first edition (ISO/IEC 24760-3:2016), which has been technically revised. It also incorporates the Amendment ISO/IEC 24760-3:2016/Amd 1:2023.

The main changes are as follows:

— title has been updated;

— the document has been editorially revised.

A list of all parts in the ISO/IEC 24760 series can be found on the ISO website.

This document has been given the status of a horizontal document in accordance with the ISO/IEC Directives, Part 1.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

© ISO/IEC 2025 – All rights reserved

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 can concern access to applications or other resources.

To address the need to efficiently and effectively implement systems that make identity-based decisions, the ISO/IEC 24760 series 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 for maintaining security within organizational processes. For individuals, correct identity management is important for protecting privacy.

The ISO/IEC 24760 series specifies fundamental concepts and operational structures for identity management and provides a framework on which information systems can meet business, contractual, regulatory, and legal obligations.

This document specifies 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 document is intended to provide a foundation for the practices for identity management in other international standards related to identity information processing including other parts of the ISO/IEC 24760 series, ISO/IEC 29100, ISO/IEC 29101, ISO/IEC 29115, and ISO/IEC 29146.

© ISO/IEC 2025 – All rights reserved

Information security, cybersecurity and privacy protection — A framework for identity management —

Part 3: Practice

1 Scope

This document:

— provides requirements and 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;

— is applicable to any information system where information relating to identity is processed or stored;

— is considered to be a horizontal document for the following reasons:

  — it applies concepts such as distinguishing the term "identity" from the term "identifier" on the implementation of systems for the management of identity information and on the requirements for the implementation and operation of a framework for identity management,

  — it provides an important contribution to assess identity management systems with regard to their privacy-friendliness and their ability to assure the relevant attributes of an identity, and consequently it provides a foundation and a common understanding for any other standard addressing identity, identity information, and identity management.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 24760-1:2025, *Information security, cybersecurity and privacy protection — A framework for identity management — Part 1: Core concepts and terminology*

ISO/IEC 24760-2, *Information security, cybersecurity and privacy protection — A framework for identity management — Part 2: Reference architecture and requirements*

3 Terms and definitions

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

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
identity profile
identity containing attributes specified by an identity template

© ISO/IEC 2025 – All rights reserved

3.2
identity template
definition of a specific set of attributes

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

3.3
identity theft
result of a successful false claim of identity

4 Abbreviated terms

For the purposes of this document, the following abbreviated terms apply.

ICT Information and communication technology

IIP Identity information provider

IIA Identity information authority

PII Personally identifiable information

RP Relying party

5 Mitigating identity related risk in managing identity information

5.1 Overview

This clause presents practices to address identity related risk when operating an identity management system conforming to ISO/IEC 24760-1 and ISO/IEC 24760-2.

Figure 1 shows the operational scope of an identity management system. The arrows in the figure identify processes that affect the recorded identity information. Details of these processes are presented in ISO/IEC 24760-1:2025, Clause 7. These processes are the prime areas of concern in assessing risks in the implementation of an identity management system.

NOTE ISO/IEC 24760-1:2025, Figure 1 shows that when an identity is registered, it can be in different stages: unknown, established, active, suspended or archived. Authentication of an entity typically can only be successful if its identity is active.

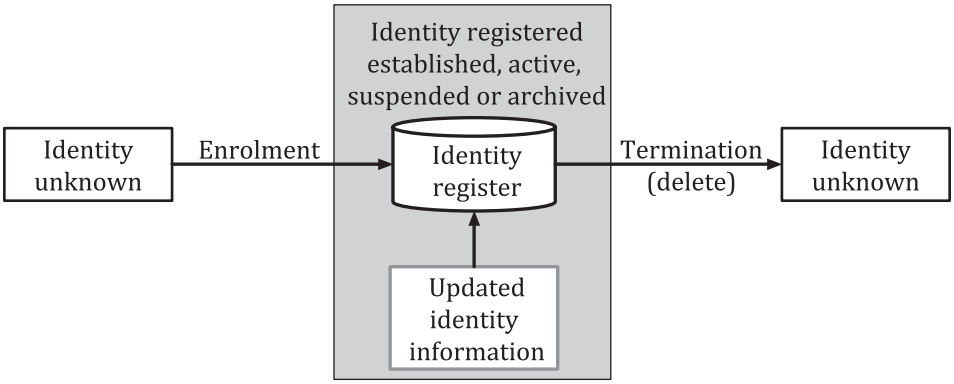


Figure 1 — Operational scope of an identity management system

© ISO/IEC 2025 – All rights reserved