



**International
Standard**

ISO/IEC 24760-2

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

**Part 2:
Reference architecture and
requirements**

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

Partie 2: Architecture de référence et exigences

**Second edition
2025-09**



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	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Symbols and abbreviated terms	3
5 Reference architecture	3
5.1 General	3
5.2 Deployment scenarios	3
5.3 Stakeholders	4
5.3.1 General	4
5.3.2 Principal	5
5.3.3 Identity management authority	5
5.3.4 Identity information authority	6
5.3.5 Relying party	6
5.3.6 Regulatory body	6
5.3.7 Consumer/citizen representative or advocate	6
5.4 Actors	7
5.4.1 General	7
5.4.2 Principal	8
5.4.3 Identity management authority	8
5.4.4 Identity registration authority	9
5.4.5 Relying party	10
5.4.6 Identity information authority	10
5.4.7 Identity information provider	11
5.4.8 Verifier	12
5.4.9 Auditor	13
5.5 Processes and services	13
5.5.1 Documentation	13
5.5.2 Identity information management processes	14
5.5.3 Specific identity information management processes	15
5.5.4 Additional functions	17
5.6 Viewpoints	20
5.6.1 General	20
5.6.2 Context viewpoint	20
5.6.3 Functional viewpoint	20
5.7 Use cases	21
5.7.1 General	21
5.7.2 Principal use cases	22
5.8 Components	23
5.8.1 General	23
5.8.2 Principal	23
5.8.3 Identity register	23
5.9 Compliance and governance	24
5.10 Physical model	24
6 Architecture for managing internal identities, the enterprise model	24
6.1 Context	24
6.2 Stakeholders and concerns	25
6.3 The enterprise deployment scenario	26
6.4 Use cases	26
6.4.1 Employee use cases	26
6.4.2 Employer use cases	27

7	Architecture for managing external identities	27
7.1	Context	27
7.2	Stakeholders and concerns	27
7.3	Deployment scenarios with external identities	29
7.3.1	The federated deployment scenario	29
7.3.2	The service deployment scenario	29
7.3.3	The federated deployment scenario as applied as a service	29
7.4	Use cases	29
7.4.1	Device use cases	29
7.4.2	Sharing use cases	29
8	Requirements for the management of identity information	30
8.1	General	30
8.2	Access policy for identity information	30
8.3	Functional requirements for management of identity information	30
8.3.1	Policy for identity information lifecycle	30
8.3.2	Conditions and procedure to maintain identity information	31
8.3.3	Identity information interface	31
8.3.4	Reference identifier	31
8.3.5	Identity information quality and compliance	33
8.3.6	Archiving information	33
8.3.7	Terminating and deleting identity information	33
8.4	Non-functional requirements	34
	Annex A (informative) Use case	35
	Annex B (informative) Component model	38
	Annex C (informative) Business process model	41
	Bibliography	46

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 24760-2:2015), which has been technically revised.

The main changes are as follows:

- in [Clause 3](#), the definitions of terms from ISO/IEC 24760-1 were removed;
- to address the emerging concept of mobile identity, the term “principal’s private IMS” (PPI) was added in [Clauses 3, 4](#), and described in [5.4.2](#), [5.4.3](#) and [5.4.6](#);
- some of the content of [Clause 5](#) was moved to [Clauses 6](#) and [7](#);
- former [Annex A](#) has been deleted and the existing annexes have been relabelled.

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

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.

Introduction

Data processing systems commonly gather a range of information on its users, which can include people, pieces of equipment, or pieces of software connected to the equipment. Based on the information gathered on user identity, these data processing systems make decisions that can impact how users access to IT resources.

To address the need to efficiently and effectively implement systems that make identity-based decisions, this document specifies a framework for the issuance, administration and use of data. This framework 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 the security of the 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 defines a reference architecture for identity management including interrelationships. These architectural elements are described in respect to identity management deployments scenarios and their models. This document also 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 identity management.

This document is intended to provide a foundation for the implementation of other international standards related to identity information processing such as ISO/IEC 29100, ISO/IEC 29101, ISO/IEC 29115, and ISO/IEC 29146.

This document is not a management system standard (MSS).

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

Part 2: Reference architecture and requirements

1 Scope

This document:

- provides guidelines for the implementation of systems for the management of identity information;
- specifies requirements for the implementation and operation of a framework for identity management;
- 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, *Information security, cybersecurity and privacy protection — A framework for identity management — Part 1: Core concepts and terminology*

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