FINAL DRAFT International Standard

ISO/IEC FDIS 24760-3

IT Security and Privacy — A framework for identity management —

Part 3: Practice

Sécurité IT et confidentialité — Cadre pour la gestion de l'identité —

Partie 3: Mise en oeuvre

ISO/IEC JTC **1**/SC **27**

Secretariat: **DIN**

Voting begins on:
2024-12-27

Voting terminates on:
2025-02-21

Reference number
ISO/IEC FDIS 24760-3:2024(en)

Horizontal document

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

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.

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

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 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.

IT Security and Privacy — 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, *IT Security and Privacy — A framework for identity management — Part 1: Core concepts and terminology*

ISO/IEC 24760-2, *IT Security and Privacy — 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

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:—,[1] 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:—,[1)] 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.

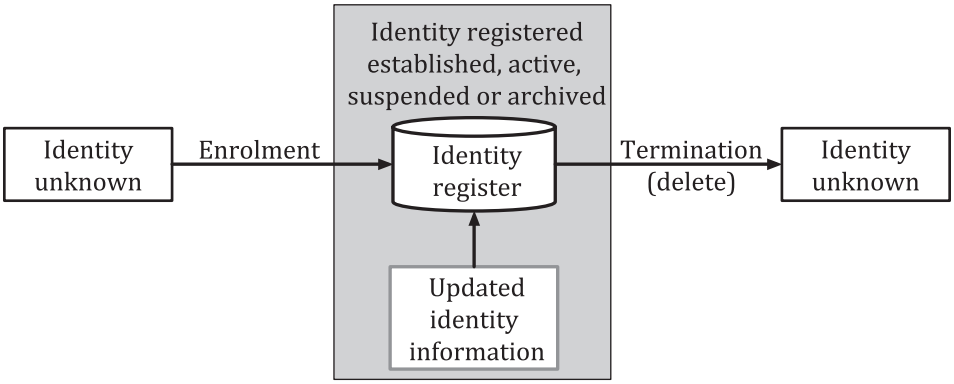

Figure 1 — Operational scope of an identity management system

5.2 Risk assessment

A function of an identity management system is managing identity as data; secure operation of this data management system involves managing the risk of identity errors while protecting the confidentiality, integrity and availability of identity information that is stored, processed and communicated. A risk assessment should be conducted to determine the level of risk of the identity management system. The risk management should take into account the lifecycle of identity and identity information that evolve over time and can impact consumers of this information. The result provides information, which the identity management system can use to determine the necessary risk management criteria and processes. The sort of information the identity management system requires includes the level of assurance of identity required and the requirements for confidentiality, integrity and availability of identity information.

ISO/IEC 24760-2 specifies tools to manage risks as policies, regulation, design and architecture. In some contexts, involving consumers, protecting personally identifiable information and giving principals control over the use of their personally identifiable information is paramount. ISO/IEC 29100, ISO/IEC 29101, ISO/IEC 29134 and ISO/IEC 29151 specify requirements and provide guidance for the protection of privacy.

Identity information managed by an identity management system may also be managed by reference to identity information providers in another domain. For example, identity proofing may be undertaken by a service provider, which operates in a different domain to that of the identity management system.

When identity information is collected and stored, risk management measures shall be implemented by the identity management service. These measures mitigate the risks identified by a risk assessment carried out in the application domain by the relying party. Levels of assurance concerning identity information and access services shall be determined and specified by the relying party according to assessed levels of risk.

5.3 Assurance in identity information

5.3.1 General

Confidence in identity information provided by an identity management system comes from processes that ensure the validity of the information from its collection through its subsequent storage and maintenance by the system. Assurance is typically quantified in terms of assurance levels with higher levels corresponding to greater assurance. The level of assurance achieved depends on the quality of the identity information and the rigour of the identity validation processes. Levels of assurance are described in ISO/IEC 29115.

5.3.2 Identity proofing

Identity proofing, i.e. validating identity information for enrolment of an entity in a domain, shall meet a defined level of assurance. The level of assurance of identity proofing achievable depends on the type and characteristics of information and, in some cases, the scope of this information, e.g. the number of independent identity information providers used as sources of the information.

An increased level of assurance in identity verification may be achieved:

— with verification of additional credentials issued from multiple sources, and

— using a trusted external party that knows the entity to validate claimed identity information.

NOTE 1 ISO/IEC TS 29003 provides requirements for identity proofing.

NOTE 2 ISO/IEC 29115 specifies how to achieve different levels of assurance.

5.3.3 Credentials

An identity management system may issue multiple types of credential, differing in the level of assurance of the identity information represented by the credential.

An identity management system issuing credentials with a high level of assurance supported by a cryptographic mechanism should provide a service for relying parties to actively support the cryptographic validation process.

An issuer of a credential in physical form shall implement an identity management system to process the identity of the credential device in accordance with ISO/IEC 24760-1 and ISO/IEC 24760-2.

5.3.4 Identity profile

An identity management system may use one or more identity profiles for gathering, structuring, or presenting identity information.

NOTE Although a profile can contain identity information, it is not intended for identification. Its purpose is to provide identity information about an entity to system processes that need the information for their processes.

An entity may have multiple identity profiles, each containing a different set of attributes for the entity. For instance, a language preference may be present in a profile for an access interface and not in a profile for book interests.

An identity template may be established as an international or industry standard. The use of a standardized identity template to record identity attributes would facilitate the usage of identity profiles across domains.

An identity profile may be used in access management to determine the required identity attributes for being authorized for a role or privilege in accessing information. An identity profile may be used as a pre-configured subset of identity information to be presented when interacting with a service.

An attribute in an identity profile may be associated with a level of assurance. Using an identity profile with associated levels of assurance to present identity information shall imply that each item of information has been validated at a minimum its associated level of assurance. An identity profile specifying requirements for access to services or resources may be associated with a specific additional entity identifier that may indicate the activities linked to the specific privileges.

6 Identity information and identifiers

6.1 Overview

Organizations should understand the information security concerns for their business and should provide management support to meet the business needs including additional requirements.

In regard to identity management, organizations should understand their liabilities and ensure that adequate controls are implemented to mitigate the risks and consequences of identity information leakage, corruption and loss of availability when collecting, storing, using, transmitting and disposing of identity information. Organizations should specify control objectives and controls to ensure that information security requirements are met.

6.2 Policy on accessing identity information

The identity information pertaining to an entity should be managed to ensure the following:

— identity information remains accurate and up-to-date over time;

— only authorized entities have access to the identity information and are accountable for all uses and changes in identity information, guaranteeing traceability of any processing of identity information by any entity, whether a person, a process or a system;

— the organization fulfils its obligations with respect to regulations and contractual agreements;

— principals are protected against the risk of identity-related theft and other identity related crime.

NOTE Typically, an information security policy highlights the necessity to securely manage identity information. The preservation and protection of any entities identity information is also required when dealing with third parties as typically documented within the operational procedures.

6.3 Identifiers

6.3.1 General

An identifier allows distinguishing unambiguously one entity from another entity in a domain of applicability. An entity may have multiple, different identifiers in the same domain. This can facilitate the representation of the entity in some situations, e.g. hiding the entity's identity when providing the entity's identity information for use in some processes or within some systems. An identifier created in one domain may be reused intentionally in another domain provided the reused identifier continues to provide uniqueness of identity within the other domain.

6.3.2 Categorization of identifier by the type of entity to which the identifier is linked

6.3.2.1 Person identifiers

A person identifier can include a full name, date of birth, place of birth, or various pseudonyms, such as a number assigned by an authority as a reference, e.g. passport number, national identity number or identity-card number.

The use of pseudonyms as identifiers is frequent for person identifiers (see 6.3.3.2).

NOTE A pseudonym can enhance the privacy of persons in an identity-authentication exchange with a relying party, as a pseudonym can reveal less personally identifiable information than if a real name is used as an identifier.

6.3.2.2 Identifier assigned to a non-person entity

Non-person entities, e.g. devices or other information objects, can have their activities identified and recorded as for persons.

Device identifiers allow distinction between devices in the domain in which they operate.

EXAMPLE 1 The International Mobile Equipment Identity (IMEI) is an identifier of the mobile telephone handset in the domain of a mobile telephone services.

EXAMPLE 2 The GSM SIM card number (ICCID) is a unique device identifier in the domain of a mobile telephone service. A SIM card also contains other identifiers including that of the user who registered the SIM card.

It can also be necessary to distinguish information object identifiers in their domains. One of their attributes that compromise a combination of their attributes is usually used as identifier.

EXAMPLE 3 Process name, session name, path name, uniform resource names (URN), uniform resource identifier (URI) are examples of information object identifiers.

EXAMPLE 4 URI is an example of identifier for a location, but the object at that location can change at any time.

6.3.3 Categorization of identifier by the nature of linking

6.3.3.1 Verinymous identifier

A verinymous identifier is an identifier, persistent in its domain of applicability that may be used within and across domains and allows a relying party to obtain further identity information for the entity associated with the identifier. Commonly observed verinimous identifiers includes email address, mobile phone number, passport number, driving license number, social security number and the name-date of birth pair.

A verynimous identifier can allow identity information for entities known in different domains to be correlated. While it is fine to correlate the identities if so desired by the person, unexpected correlation, e.g.