INTERNATIONAL STANDARD

ISO/IEC 24760-3

First edition
2016-08-01

AMENDMENT 1
2023-01

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

Part 3: **Practice**

AMENDMENT 1: Identity Information Lifecycle processes

Reference number
ISO/IEC 24760-3:2016/Amd. 1:2023(E)

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

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).

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) or the IEC list of patent declarations received (see https://patents.iec.ch).

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*.

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

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.

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

Part 3: Practice

AMENDMENT 1: Identity Information Lifecycle processes

Clause 3

Delete 3.1 and 3.6.

5.1

Remove the reference to ISO/IEC 29115 so the text reads as follows:

> Clause 5 presents practices to address identity related risk when operating an identity management system conforming to ISO/IEC 24760-1 and ISO/IEC 24760-2.

Add the following text and figure below the first paragraph:

> 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 24760-1:2019, 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: 2019, Figure 1 shows that when an identity is registered, it can be in different stages: established, active, suspended or archived. Authentication of an entity typically can only be successful if its identity is active.

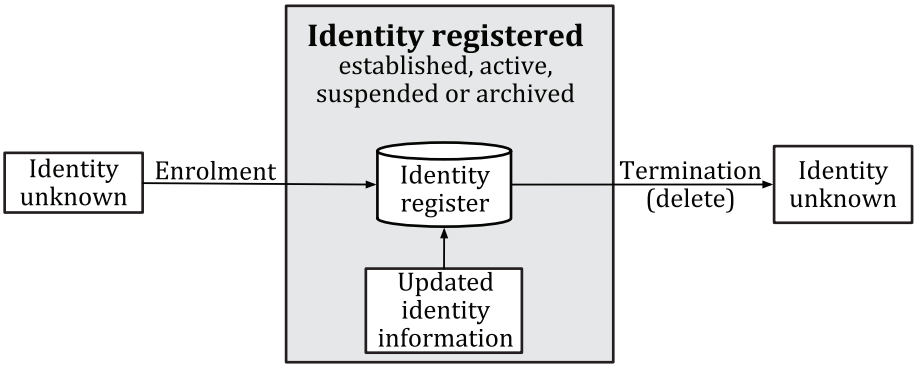

Figure 1 — Operational scope of an identity management system

5.2

Replace the first paragraph with the following:

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 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 may 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.

5.3.3.

Add the following paragraph at the end of the subclause:

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.

6.3

Add the following new subclauses and text:

6.3.6 Categorization of identifier by method of value creation

6.3.6.1 As combination of attributes

A particular combination of attributes may have a unique value over all registered identities. Such a combination of attribute values may serve as an identifier.

NOTE An identifier derived from a combination of attributes can be referred to as a "quasi-identifier"

A combination of attributes of which the combined values are not unique over all registered identities may be defined to function as a shared identifier for a group of entities.

The value of such an identifier intended or expected to be used outside the domain of origin should be transformed into an identifier with a generated unique value by applying a cryptographic hash function to the combined attribute values.

6.3.6.2 Generated with a unique value

An identifier may be generated to have a unique value for all registered identities.

NOTE 1 Typically, at registration one such identifier can be generated to be used as a reference identifier.

NOTE 2 A timestamp with sufficient granularity of time can be used as such an identifier for each subject that simultaneously uses a service in a domain of applications.

6.3.6.3 Assigned from an externally generated unique value

A unique value generated by a third party as associated with a principal may be used as identifier in an identity management system. Guarantees of the uniqueness of the values shall be obtained before deciding to use such an identifier in the registered identities. Such an identifier may be used as reference identifier.

EXAMPLE An externally generated unique value can be the identifier of a state issued identification document, e.g. the document number of a passport or driver licence, the identifier of a credential in physical form, including a hardware token, or a citizen administration number.

NOTE 1 An external unique value can be referred to as an "authoritative identifier", in particular where that identifier can be used to refer to identity information held in the domain of origin of the external identifier value.

To improve privacy protection, the value of such an identifier should be transformed before being registered into an identifier with generated unique value by applying a cryptographic hash function to the externally provided value.

NOTE 2 In case the external identifier is transformed by applying a cryptographic hash function, it can still be used in authentication. In that case, its use as authoritative identifier, e.g. to retrieve additional identity information from the domain of origin of the external identifier, is only possible during authentication after the entity has presented the original value. Typically, in this case, such additional identity information is intended to be included in the authenticated identity, as possibly requested by a relying party.

Clause 7

Replace this clause with the following text:

An identity management system can support the auditing of processes where identity information is accessed. Auditing shall record which information is accessed, the operator initiating the process and any parties outside the system with which information may be shared or from which new information is obtained. In case de-identification is applied when sharing information, auditing shall be performed in a way to assert its correctness.

NOTE 1 Auditing is usually required by law and regulations. Auditing also facilitates business practices when data is being shared between parties as part of their business operations.

NOTE 2 Requirements for auditing can include measures to protect personally identifiable information, to maintaining required time-stamp accuracy and traceability (see the ISO/IEC 18014 series).

Bibliography

Add the following entry:

[8] ISO/IEC TS 29003:2018, *Information technology—Security techniques—Identity proofing*