DRAFT INTERNATIONAL STANDARD

ISO/IEC DIS 24760-3

ISO/IEC JTC **1**/SC **27** Secretariat: **DIN**

Voting begins on:
2015-07-28

Voting terminates on:
2015-10-28

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

Part 3:
Practice

Technologies de l'information — Techniques de sécurité — Cadre pour la gestion de l'identité — Partie 3: Mise en oeuvre

ICS: 35.040

Reference number
ISO/IEC DIS 24760-3:2015(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

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*, Subcommittee SC 27, *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.

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 aspects of assurance in controlling identity information use, aspects of controlling the access to identity information and other resources based on identity information, and control objectives that should be implemented when establishing and maintaining a framework of identity management.

ISO/IEC 24760 consists of the following parts:

— Part 1: Terminology and concepts

— Part 2: Reference architecture and requirements

— Part 3: Practice

ISO/IEC 24760 is intended to provide foundations for other identity management related international standards including:

— ISO/IEC 29100 Privacy framework;

— ISO/IEC 29101 Privacy Reference Architecture;

— ISO/IEC 29115 Entity Authentication Assurance Framework;

— ISO/EC 29146 A framework for access management.

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

Part 3: Practice

1 Scope

This International Standard provides guidance for practice of implementing and managing identity management systems and for ensuring that such systems meet the requirements in ISO/IEC 24760 Part 1, Terminology and Concepts, and in ISO/IEC 24760 Part 2, Reference Architecture and Requirements.

This International Standard 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 may also be addressed in other standards.

2 Normative references

The following referenced documents are indispensable for the application 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 29115:2013, *Information technology — Security techniques — Entity authentication assurance framework*

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

[SOURCE: ISO/IEC 24760-2]

3.2
identity profile
identity containing attributes specified by an identity template

3.3
Identity template
definition of a set of attributes intended for a particular purpose

3.4
identity theft
falsely claiming the benefits in a domain of applicability of an identity known in that domain

3.5
federation operator
actor in a federation responsible for managing the issues arising from the operation of the federation

Note 1 to entry: An existing federation member or an independent third party can carry out the role of federation operator.

3.6
principal
entity to which identity information in an identity management system pertains

[SOURCE: ISO/IEC 24760-2]

4 Symbols and abbreviated terms

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, parts 1 and 2, and ISO/IEC 29115.

5.2 Risk Assessment

One function of an identity management system is to manage the risk of identity errors, and the confidentiality, integrity and availability of identity information that it stores, processes and communicates. To do this it needs to understand the level of risk, which will depend on the application. The owner of the application should conduct a risk assessment to determine the level of risk. The result will provide information, which the identity management system will use to determine the necessary risk management criteria and processes. The sort of information the identity management system will need includes the level of assurance of identity required and the requirements for confidentiality, integrity and availability of identity information.

The tools used are policies, regulation, design and architecture, specified in ISO/IEC 24760-2. In some contexts involving consumers, protecting personally identifiable information and giving principals control over the movement of their personally identifiable information, is paramount. ISO/IEC 29100[3] and ISO/IEC 29101[4] specify requirements for practical protection of privacy.

The information used for the management of identity information of a domain of applicability may also be maintained in an identity management system of another domain. For example, identity proofing and provisioning may be undertaken by a service provider acting in the role of an identity information provider operated by government or by an industry group, as well as at an organization level where the organization is managing identity information pertaining identities in its domain.

When identity information is collected and stored, risk management measures shall be implemented by the identity management service to mitigate the risks identified by a risk assessment carried out in the application domain by the relying party. Levels of assurance in regard to 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

An identity management system provides identity information at specific levels of assurance. Assuring provided identity information requires rigorous application of processes to authenticate identity information and to maintain it. The degree of rigor leads to assurance in the authenticated identity and the identity information provided by the identity management system. Levels of assurance are specified 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 case the scope of this information, e.g. the number of entities holding the information.

An increased level of assurance in identity verification may be achieved

— with verification of additional credentials issued from multiple sources,

— adding controls that are not solely information-based,

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

A higher number of independent sources could also compensate for a lower level of assurance in the information provided by those sources.

NOTE 1 ISO/IEC 29003 provides requirements for Identity proofing.

NOTE 2 ISO/IEC 29115, "Entity authentication assurance", specifies how to achieve different levels of assurance.

5.3.3 Credentials

A credential may be associated with a specific level of assurance for the identity information represented. A credential representing identity information with a high level of assurance should include an authentication code, digital signature or similar mechanisms to establish veracity of the information. A reference to a level specified in ISO/IEC 29115 may be used as explicit indication of the level of assurance conveyed by a credential.

An identity 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.

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 may 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 standardised 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 minimally 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 for compliance with relevant legislation and should provide management support to meet the business needs 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 objectives are met.

6.2 Policy on accessing identity information

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

— 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 is always ensured, guaranteeing traceability of any processing of any piece of identity information by any entity, a human, 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 An information security policy should highlight the necessity to manage and secure identity information. The preservation and protection of any entities identity information is also required when dealing with third parties. This shall be clearly documented within the operational procedures.

6.3 Identifiers

6.3.1 General

An identifier allows to unambiguously distinguish one entity from another entity is a domain of applicability.. Identifiers are used in various circumstances to identify and to record properties and activities of the entity.

An identifier created in one domain may be used in another domain provided the reused identifier guarantees uniqueness. An entity may have multiple, different identifiers in the same domain. This may facilitate representation of the entity in some critical systems if needed, hiding the entity's identity when providing the entity's identity information for use in some processes or within some systems.

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 may be, e.g. a full name, a date of birth, a place of birth, or various pseudonyms such as a number assigned by an authority as a reference, e.g. a passport number, an identity-card number.

The use of multiple identifiers for the same entity is frequent for persons. It enhances privacy of persons in an identity-authentication exchange with a relying party without requiring the relying party to protect general identity information as the identifier does not reveal less personally identifiable information than if a direct identifier is used.

6.3.2.2 Identifier assigned to a non-person entity

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

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

NOTE 1 Example: The International Mobile Equipment Identity (IMEI) is an identifier of the mobile telephone handset in the domain of GSM mobile telephone services.

NOTE 2 Example: 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

Information object identifiers may also need to be distinguished in their domains. One of their attributes of a combination of their attributes is usually used as identifier.

NOTE 1 Example: Process name, session name, path name, uniform resource names (URN), uniform resource identifier (URL) are examples of information-object identifiers.

NOTE 2 Example: An URL is an example of identifier for a location, but the object at that location may 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 may allow identity information for entities known in different domain to be correlated. While it is fine to correlate the identities if this is desired by the person, unexpected correlation, e.g. profiling, has a negative privacy impact. By the nature of the verinymous identifier, if information leakage incident happens, it allows adversaries to perform such correlation and create threats, e.g. of identity theft.

6.3.3.2 Pseudonymous identifier

A pseudonymous identifier is an identifier, persistent in its domain of applicability that is used only within that domain that is bound to an identity, but no identity information is disclosed. Because of this, identities from different domain cannot be correlated using it. Examples of pseudonymous identifier include Pairwise Pseudonymous Identifier found in such protocols like OpenID Connect, where a new identifier is created for the entity in the respective domain.