



BSI Standards Publication

IT Security and Privacy — A framework for identity management

Part 1: Terminology and concepts

National foreword

This British Standard is the UK implementation of ISO/IEC 24760-1:2019.

The UK participation in its preparation was entrusted to Technical Committee IST/33, Information security, cybersecurity and privacy protection.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2022
Published by BSI Standards Limited 2022

ISBN 978 0 539 20384 4

ICS 35.030

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 October 2022.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

English version

IT Security and Privacy - A framework for identity management - Part 1: Terminology and concepts (ISO/IEC 24760-1:2019)

Sécurité IT et confidentialité - Cadre pour la gestion de l'identité - Partie 1: Terminologie et concepts (ISO/IEC 24760-1:2019)

Informationstechnik - Sicherheitsverfahren - Rahmenwerk für Identitätsmanagement - Teil 1: Terminologie und Konzept (ISO/IEC 24760-1:2019)

This European Standard was approved by CEN on 6 June 2022.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.



CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

European foreword

The text of ISO/IEC 24760-1:2019 has been prepared by Technical Committee ISO/IEC JTC 1 "Information technology" of the International Organization for Standardization (ISO) and has been taken over as EN ISO/IEC 24760-1:2022 by Technical Committee CEN-CENELEC/ JTC 13 "Cybersecurity and Data Protection" the secretariat of which is held by DIN.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN-CENELEC shall not be held responsible for identifying any or all such patent rights.

Any feedback and questions on this document should be directed to the users' national standards body. A complete listing of these bodies can be found on the CEN and CENELEC websites.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Endorsement notice

The text of ISO/IEC 24760-1:2019 has been approved by CEN-CENELEC as EN ISO/IEC 24760-1:2022 without any modification.

Contents

Page

Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
3.1 General terms	1
3.2 Identification	3
3.3 Authenticating identity information	3
3.4 Management of identity	5
3.5 Federation	7
3.6 Privacy protection	7
4 Symbols and abbreviated terms	8
5 Identity	8
5.1 General	8
5.2 Identity information	9
5.3 Identifier	10
5.4 Credential	10
5.4.1 General	10
5.4.2 Credential management	11
6 Attributes	11
6.1 General	11
6.2 Types of attribute	12
6.3 Domain of origin	13
7 Managing identity information	13
7.1 General	13
7.2 Identity lifecycle	14
8 Identification	15
8.1 General	15
8.2 Verification	16
8.3 Enrolment	17
8.4 Registration	17
8.5 Identity proofing	17
8.5.1 General	17
8.5.2 Identity evidence	18
9 Authentication	18
10 Maintenance	19
11 Implementation aspects	19
12 Privacy	19
Bibliography	21
Index of terms	23

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).

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 <http://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.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security Techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 24760-1:2011) which has been technically revised. The main changes compared to the previous edition are as follows:

- new terms have been added to Clause 3;
- some definitions have been simplified and corrected;
- some terms have been deleted and some replaced;
- the introductory paragraphs of [Subclause 5.1](#) have been reworded;
- new [subclauses 5.4](#) and [8.5](#) has been created;

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.

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 to maintain security of the organizational processes. For individuals, correct identity management is important to protect privacy.

The ISO/IEC 24760 series 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.

The goal of this document is to specify the terminology and concepts for identity management, in order to promote a common understanding in the field of identity management.

IT Security and Privacy — A framework for identity management —

Part 1: Terminology and concepts

1 Scope

This document defines terms for identity management, and specifies core concepts of identity and identity management and their relationships.

It is applicable to any information system that processes identity information.

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 24760-2:2015, *Information technology — Security techniques — A framework for identity management — Part 2: Reference architecture and requirements*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

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

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <http://www.electropedia.org/>

3.1 General terms

3.1.1 entity

item relevant for the purpose of operation of a *domain* (3.2.3) that has recognizably distinct existence

Note 1 to entry: An entity can have a physical or a logical embodiment.

EXAMPLE A person, an organization, a device, a group of such items, a human subscriber to a telecom service, a SIM card, a passport, a network interface card, a software application, a service or a website.

3.1.2 identity

partial identity
set of *attributes* (3.1.3) related to an *entity* (3.1.1)

Note 1 to entry: An entity can have more than one identity.

Note 2 to entry: Several entities can have the same identity.

Note 3 to entry: ITU-T X1252^[13] specifies the distinguishing use of an *identity*. In this document, the term *identifier* implies this aspect.

3.1.3

attribute

characteristic or property of an *entity* (3.1.1)

EXAMPLE An entity type, address information, telephone number, a privilege, a MAC address, a domain name are possible attributes.

3.1.4

identifier

attribute or set of *attributes* (3.1.3) that uniquely characterizes an *identity* (3.1.2) in a *domain* (3.2.3)

Note 1 to entry: An identifier can be a specifically created attribute with a value assigned to be unique within the domain.

EXAMPLE A name of a club with a club-membership number, a health insurance card number together with a name of the insurance company, an email address, or a Universal Unique Identifier (UUID) can all be used as identifiers. In a voter's register, the combination of attributes *name*, *address* and *date of birth* is sufficient to unambiguously distinguish a voter.

3.1.5

domain of origin

domain (3.2.3) where an *attribute* (3.1.3) value was created or its value has been (re)assigned

Note 1 to entry: The domain of origin can be provided as meta data for an attribute.

Note 2 to entry: The domain of origin typically specifies the meaning and format of the attribute value. Such specification can be based on international standards.

Note 3 to entry: An attribute can contain an explicit value that references the domain of origin, e.g. an ISO country code for a passport number as reference to the issuing country that is the domain of origin of identity information in the passport.

Note 4 to entry: Operationally, a domain of origin can be available as an authoritative source for an attribute (sometimes known as the Attribute Authority). An authoritative source can be operated outside the actual domain of origin. Multiple authoritative sources can exist for the same domain of origin.

EXAMPLE The domain of origin of a club-membership number is the specific club that assigned the number.

3.1.6

reference identifier

RI

identifier (3.1.4) in a *domain* (3.2.3) that is intended to remain the same for the duration an *entity* (3.1.1) is known in the domain and is not associated with another entity for a period specified in a policy after the entity ceases to be known in that domain

Note 1 to entry: A reference identifier persists at least for the existence of the entity in a domain and can exist longer than the entity, e.g. for archival purposes.

Note 2 to entry: A reference identifier for an entity can change during the lifetime of an entity, at which point the old reference identifier is no longer applicable for that entity.

EXAMPLE A driver license number that stays the same for an individual driver's driving life is a persistent identifier, which references additional identity information and that is a reference identifier. An IP address is not a reference identifier as it can be assigned to other entities.

3.1.7

principal

subject

entity (3.1.1) of which identity information is stored and managed by an *identity management system* (3.4.8)

Note 1 to entry: Typically, in a context of privacy protection or where a principal is seen as having agency a principal refers to a person.

[SOURCE: ISO/IEC 24760-2:2015, 3.4, modified —The word "pertains" has been clarified and Note 1 to entry has been reworded.]

3.2 Identification

3.2.1

identification

process of recognizing an *entity* (3.1.1) in a particular *domain* (3.2.3) as distinct from other entities

Note 1 to entry: The process of identification applies verification to claimed or observed attributes.

Note 2 to entry: Identification typically is part of the interactions between an entity and the services in a domain and to access resources. Identification can occur multiple times while the entity is known in the domain.

3.2.2

verification

process of establishing that *identity information* (3.2.4) associated with a particular *entity* (3.1.1) is correct

Note 1 to entry: Verification typically involves determining which attributes are needed to recognize an entity in a domain, checking that these required attributes are present, that they have the correct syntax, and exist within a defined validity period and pertain to the entity.

3.2.3

domain

domain of applicability

context

environment where an *entity* (3.1.1) can use a set of *attributes* (3.1.3) for *identification* (3.2.1) and other purposes

Note 1 to entry: In general, the domain of an identity is well defined in relation to the particular set of attributes.

Note 2 to entry: ITU-T X1252[13] uses the term context; this document prefers the term domain.

EXAMPLE An IT system deployed by an organization that allows users to login is the domain for the user's login name.

3.2.4

identity information

set of values of *attributes* (3.1.3) optionally with any associated metadata in an *identity* (3.1.2)

Note 1 to entry: In an information and communication technology system an identity is present as identity information.

3.3 Authenticating identity information

3.3.1

authentication

formalized process of *verification* (3.2.2) that, if successful, results in an *authenticated identity* (3.3.2) for an *entity* (3.1.1)

Note 1 to entry: The authentication process involves tests by a verifier of one or more identity attributes provided by an entity to determine, with the required level of assurance, their correctness.

Note 2 to entry: Authentication typically involves the use of a policy to specify a required level of assurance for the result of a successful completion.

3.3.2

authenticated identity

identity information (3.2.4) for an *entity* (3.1.1) created to record the result of *authentication* (3.3.1)

Note 1 to entry: An authenticated identity typically contains information obtained in the authentication process, e.g. the level of assurance attained.