TECHNICAL SPECIFICATION

ISO/IEC TS 29003

First edition
2018-03

Information technology — Security techniques — Identity proofing

Technologies de l'information — Techniques de sécurité — Vérification de l'identité

Reference number
ISO/IEC TS 29003:2018(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
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. 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 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 the following URL: www.iso.org/iso/foreword.html.

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

Introduction

An International Standard for identity proofing of natural persons is required, to which other identity management standards can refer.

A large and increasing number of industry and government organizations seek an international identity proofing standard. This document enables interoperability and federated trust for the purposes of digital economies and societies, and support international cyber assurance across supply chains and global commons.

This document relates to: the ISO/IEC 24760 series which specifies a general framework for identity management, including a life cycle for identity information; and ISO/IEC 29115, which specifies levels of assurance for entity authentication. These standards focus primarily on the policy and technical standards for the issuance and operation of identity management and access management systems, which come after the process of enrolment. The use of these standards can benefit from a standard for identity proofing of persons.

This document is intended to be used by any entity that performs identity proofing, such as described in ISO/IEC 29115 and/or the ISO/IEC 24760 series.

Information technology — Security techniques — Identity proofing

1 Scope

This document:

— gives guidelines for the identity proofing of a person;

— specifies levels of identity proofing, and requirements to achieve these levels.

This document is applicable to identity management systems.

2 Normative references

There are no normative references in this document.

3 Terms, definitions and abbreviated terms

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 https://www.electropedia.org/

3.1
application
process whereby information to be used for *identity* (3.9) proofing of a *subject* (3.15) is provided

3.2
authoritative evidence
evidence that holds *identifying attribute*(s) (3.8) that are managed by an *authoritative party* (3.3)

Note 1 to entry: This is one type of evidence of identity.

Note 2 to entry: Authoritative evidence for a particular identifying attribute can be only corroborative evidence for another.

3.3
authoritative party
entity that has the recognized right to create or record, and has responsibility to directly manage, an *identifying attribute* (3.8)

Note 1 to entry: Jurisdiction(s) and/or industry communities sometimes nominate a party as authoritative. It is possible that such a party is subject to legal controls.

3.4
context
environment with defined boundary conditions in which *subjects* (3.15) exist and interact

[SOURCE: ITU-T X.1252 (4/2010), 6.20, modified — entities has been replaced by subjects.]

3.5
corroborative evidence
evidence that holds *identifying attribute*(s) (3.8) that are not managed by an *authoritative party* (3.3)

Note 1 to entry: It is possible that the identifying attributes in corroborative evidence are not as up-to-date or accurate as those in authoritative evidence.

Note 2 to entry: This is one type of evidence of identity.

Note 3 to entry: Corroborative evidence for a particular identifying attribute can be authoritative evidence for another.

3.6
credential
set of data presented as evidence of a claimed or asserted *identity* (3.9) and/or entitlements

[SOURCE: ISO/IEC 29115:2013, 3.8, modified — The Note has been deleted.]

3.7
evidence of identity
EOI
evidence that provides a degree of confidence that a *subject* (3.15) is represented by the *identity* (3.9) being claimed

3.8
identifying attribute
attribute that contributes to uniquely identifying a *subject* (3.15) within a context

3.9
identity
set of attributes related to a *person* (3.12)

[SOURCE: ISO/IEC 24760-1:2011, 3.1.2, modified — "entity" has been replaced by "person" and the Notes have been deleted.]

3.10
identity information
set of values of attributes optionally with any associated metadata in an *identity* (3.9)

[SOURCE: ISO/IEC 24760-1:2011, 3.2.4, modified — The Note has been deleted.]

3.11
level of identity proofing
LoIP
confidence achieved in the identity proofing

3.12
person
human being

3.13
proofing information
information collected for identity proofing

3.14
proofing party
entity that performs identity proofing of a *subject* (3.15)

3.15
subject
person (3.12) whose *identity* (3.9) is being proofed

3.16
supporting attribute
attribute that is used in identity proofing but not as an *identifying attribute* (3.8)

4 Identity proofing concepts

4.1 Identity proofing

Identity proofing is the process to verify identifying attribute(s) to be entered into an identity management system and to establish that the identifying attributes pertain to the subject to be enrolled.

Deploying an identity proofing function should include:

— documenting the policy for identity proofing, the processes conducted and the designated team or person in charge of the process, known as the proofing policy maker;

— determining the context of the identity proofing, the defined boundary and conditions in which the subject and their identity will interact;

— determining the identifying attributes that are needed to be collected and proofed;

— determining the supporting attributes that will be collected in order to carry out identity proofing;

— establishing the LoIP required by the subsequent enrolment process;

— implementing the infrastructure to deliver identity proofing.

Each identity proofing instance includes steps to:

— collect the proofing information;

— determine the veracity of the identifying attributes collected against objectives specified in Clause 5;

— determine that identifying attributes meet the required LoIP to be achieved;

— bind the subject to the claimed identifying attributes.

4.2 Enrolment

Enrolment is the process by which identity information is collected, verified and entered into an identity management system. The design, implementation and operation of an identity proofing system should also consider the ISO/IEC 24760 series and ISO/IEC 29115.

The enrolment process should record information including the outcome of identity proofing.

4.3 Proofing information

The proofing party collects proofing information which can include both identifying and supporting attributes as shown in Table 1. Proofing information can be a subset of the information required for a subject to receive services and/or credentials.

Table 1 — Proofing information and attributes

Types of attribute	Explanation	Examples of attributes
Identifying attributes	One or more attributes that, when combined, uniquely identifies the subject in a context	Pseudonym(s) Name(s) Date of birth Place of birth A parent's name at their birth Biometric characteristic(s) Address(es) Phone number(s) E-mail(s) Time of birth (if known) National identification number(s)
Supporting attributes	Attributes that contribute to identity proofing	Other names Relationships and associations Reference numbers from EOI Relevant information from EOI provided

NOTE Proofing information does not include eligibility or capability attributes. Any assessment of eligibility or capability of a subject is potentially unreliable if the identity has not been proofed to the required LoIP. The nature and accuracy of information collected to determine eligibility or capability (not identity) for a service and/or credential is out of the scope of this document.

4.4 Evidence of identity

4.4.1 General

Evidence of identity is used during identity proofing to provide confidence that a subject has the identity being claimed that is appropriate to a specific LoIP. An application can occur using a number of channels (e.g. in-person, over the phone or online). The subject applies in order to receive services and/or credentials, which determine the necessary LoIP. The LoIP requirements to be met for each of the LoIP objectives are specified in Clause 5.

Evidence of identity can be either authoritative evidence or corroborative evidence. Evidence of identity typically includes one or more of the following:

— proofing information provided by the subject;

— issued evidence containing or linking to subject proofing information;

— databases and registers containing subject proofing information;

— proofing information provided by other known sources.

Any evidence used by a proofing party during identity proofing is to contain proofing information consistent with the application information and with the requirements set forth in Clause 5.

NOTE EOI can be provided in different types. It is possible that the level of identity proofing that can be achieved depends on the type provided.

4.4.2 Authoritative evidence

A subject can use various identifying attributes to create identities in different contexts. For each identifying attribute, there can be authoritative evidence available. That is evidence recognized as the point of truth for the identifying attribute, often characterized as being the very first instance of identity establishment (i.e. the first identity proofing the person is the subject of) and/or controlled by legislation.

Examples of national authoritative evidence are given in A.1.

4.4.3 Corroborative evidence

Where the proofing party does not have access to authoritative evidence for an identifying attribute (or does not need to for the LoIP desired), the residual risk may be mitigated by verifying against corroborative evidence. Where corroborative evidence stores identifying attributes from authoritative evidence, the attributes are not recognized as authoritative.

Examples of national corroborative evidence are given in A.1.

4.5 Actors

4.5.1 General

Checking the evidence of identity involves relationships between subject, proofing party and potentially a verifier. Evidence of identity performs a role in this process.

4.5.2 Subject

The subject or other applicant applies for the subject to undergo identity proofing by the proofing party. An application may be made by either the subject of the application or a person acting on their behalf. Identity proofing is carried out on the subject by the proofing party.

4.5.3 Proofing party

A proofing party establishes the validity of the claimed identifying attributes of the subject in accordance with the LoIP required. Identity information verification is performed against evidence of identity for each identifying attribute.

The proofing party chooses to:

— examine evidence of identity, which contains identifying attributes and, for each attribute, determines whether to accept the attribute; or

— verify the presented identifying attributes with a service provider who has authorized access to the evidence for this purpose. The service provider provides a response to the proofing party.

A proofing party that is carrying out identity proofing relies on the accuracy and integrity of the proofing information in the evidence of identity to which it refers.

4.5.4 Verifier

A verifier is an entity, system, device or software that has the ability to answer a verification request from a proofing party. They can include entities such as authoritative parties or other parties that control evidence. The subject themselves can be a verifier if they can activate evidence to respond.

The response provided by the verifier does not necessarily include a verification judgement but can be proofing information which enables the proofing party to make their judgement on whether successful verification has occurred.