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/IEC 2018

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2018

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

© ISO/IEC 2018 – All rights reserved

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*.

© ISO/IEC 2018 – All rights reserved

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.]

© ISO/IEC 2018 – All rights reserved

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

© ISO/IEC 2018 – All rights reserved

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.

© ISO/IEC 2018 – All rights reserved

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.

4.6 Evidence of identity strength considerations

Unless the identity proofing event is the inaugural establishment of identity for the subject, some evidence (documents, digital identities, etc.) can be the product of an earlier formal identity proofing process. Registration of birth is an example of an inaugural event where there is no previous identity proofing activity for the subject.

The proofing party should evaluate the earlier identity proofing event to determine the extent to which the evidence can be accepted for the current identity proofing event and LoIP, and any further validation that can be necessary.

Not all evidence of identity issued is able to be used in subsequent identity proofing outside the context in which it was issued. It is possible that evidence does not contain any proofing information and/or cannot be linked to proofing information that is externally accessible. Physical documents presented as evidence of identity can include anti-tampering and anti-counterfeit features. Where appropriate and practical, the verification of identity information in physical evidence of identity includes the checking of the anti-tampering and anti-counterfeit features. Electronic forms of evidence of identity can be obtained in a manner that tampering and counterfeiting can be detected.

The strength of the evidence includes these three aspects:

- the original identity proofing undertaken;
- the quality and robustness of the security measures to prevent tampering, counterfeiting and forgery;
- the process used to issue it.

The number of evidence items required depends on the ability of the evidence of identity to meet the identity proofing objectives. Where multiple pieces of evidence are required, additional strength can be achieved by drawing the evidence of identity from the whole life of the subject.

4.7 Levels of identity proofing

The LoIP for an application is based on the extent to which the identity proofing objectives have been met. The target LoIP is determined through an identity-related risk assessment of the subsequent service and/or credential to be provided. This risk assessment is undertaken by the organization providing the service and/or credential, and can contribute to the design and implementation of the identity proofing function by the proofing party.

Table 2 describes each LoIP and the objectives that deliver the strength of each.

Table 2 — Levels of identity proofing

LoIP	Description	Objective
LoIP 1	Low confidence in the claimed or asserted identity	Identity is unique within the context and there is an assumption the identity exists and the subject is assumed to be bound to the identity
LoIP 2	Moderate confidence in the claimed or asserted identity	Identity is unique within the context and moderately establish the identity exists [a] and the subject has some binding to the identity
LoIP 3	High confidence in the claimed or asserted identity	Identity is unique within the context and strongly establish the identity exists [a] and the subject has a strong binding to the identity

[a] The concept requires the values of the identifying attribute to match that of the evidence of identity.

NOTE As LoIP increases, requirements for processes to achieve some objectives become more stringent, as specified in Clause 5.

Individual implementations of identity proofing processes will vary depending on the policy and evidence of identity available to the subject and the proofing party. The reliability and accuracy of the evidence will impact the LoIP that can be achieved. Where the identity-related risk is extreme, a proofing party can achieve one or more objectives in multiple ways.

The LoIP is one element that contributes to the overall level of assurance, of entity authentication. For more information on levels of assurance refer to ISO/IEC 29115.

LoIP requirements are defined by the entity handling the subsequent process, for example, enrolment or credential management. This is in order to ensure that the risks involved are assessed and adequately mitigated to address both the risks involved in making the determination to accept the identity, as well as those inherent in the operation of the service.

4.8 One identity per subject

Depending on the context of the application for which the identity proofing is performed, it can be necessary to ensure that each subject is only registered once, i.e. each subject has only one identity in the context.

Possible controls to achieve this are:

- requiring documents or information from authoritative evidence which are known to be one-per-person;
- comparing the subject’s biometric sample against other biometric samples in the context for detecting and preventing duplication of a person. The biometric information collected should be sufficient and effective for de-duplicating the identity.

4.9 Deceased subjects

The proofing party needs to consider whether the subject is still living or is deceased. This is useful in the detection of attempts to reuse the identities of deceased persons. If necessary, the verification against authoritative evidence can be used to accomplish this task.

Where it is determined that the subject is deceased, and enrolment is still required, the relevant parts of identity proofing should verify the legitimacy of the application and the applicant.

5 Requirements for identity proofing

5.1 Identity proofing policy

The proofing party shall perform identity proofing in accordance with a documented identity proofing policy.

The identity proofing policy shall state, as a minimum:

- the LoIP(s) at which the identity proofing service is offered;
- the jurisdiction in which the identity proofing service operates and in which it is offered, and the applicable legislation;
- the intended context for which identity proofing is being undertaken;
- whether identity proofing is in-person or remote;
- what identifying attributes applicants are required to provide;
- which evidence of identity (authoritative or corroborative) for the identifying attributes shall be used, when verifying proofing information;
- what are the possible outcomes of the identity proofing operations;
- how the results of the proofing process will be communicated to the applicant or appropriate parties;
- what records of the proofing processes will be retained, by whom and for how long, as determined by the policy maker.

A proofing party's identity proofing policy maker should publish its identity proofing policy. If published, an identity proofing policy document shall be dated.

5.2 Determining the level of identity proofing

In order to achieve identity proofing at a specific LoIP, the process shall successfully prove both the existence of identity at that LoIP and identity/subject binding at that target LoIP. Identity proofing requires that each identity is unique in its context, see 5.3.

Table 3 shows how the resulting LoIP is determined.

© ISO/IEC 2018 – All rights reserved

Table 3 — Determining level of identity proofing

	Identity exists at LoIP 1	Identity exists at LoIP 2	Identity exists at LoIP 3
Identity is bound at LoIP 1	LoIP 1	LoIP 1	LoIP 1
Identity is bound at LoIP 2	LoIP 1	LoIP 2	LoIP 2
Identity is bound at LoIP 3	LoIP 1	LoIP 2	LoIP 3

5.3 Identity is unique

The proofing party shall check the identifying attributes provided by the subject to evaluate the duplication of those already managed for other subjects within the context. Any duplication detected is resolved according to the identity proofing policy. Table 4 shows the minimum requirements for identity uniqueness.

NOTE Duplication of identifying attributes can be determined either as full duplication of all attributes or as a duplication of part of the attributes. The identity proofing policy specifies the identifying attributes, e.g. type and number that are expected to be sufficient for uniqueness. If identifying attributes initially provided are found not to be unique either the identity proofing fails or additional attributes can be obtained from the subject or can be generated. The identity proofing policy indicates which additional attributes to obtain or generate, if any.

Table 4 — Minimum requirements by LoIP for Identity is unique

Objective	LoIP 1	LoIP 2	LoIP 3
Identity is unique	Identifying attributes within the context shall be checked for a duplicate identity	Same as LoIP 1	Same as LoIP 1

5.4 Existence of identity in evidence

For LoIP 1, the proofing party shall accept the identifying attributes as provided without carrying out any checking. For LoIP 2, the proofing party shall check that the identifying attributes exist in corroborative evidence; for LoIP 3 the proofing party shall check that identifying attributes exist in authoritative evidence, as determined by the proofing policy.

At LoIP 2 and LoIP 3, if the identifying attributes cannot be confirmed in evidence of identity, the proofing party shall apply a documented exception process as per the proofing policy to attempt to determine the existence of an identity. Such measures, in the exception process, shall be proportional to the LoIP and have regard to the effort required to perform them versus terminating the application. Where such checks are not conclusive, the application should, in any event, be terminated. Table 5 shows the minimum requirements for existence of identity in evidence.

Table 5 — Minimum requirements by LoIP for Existence of identity in evidence

Objective	LoIP 1	LoIP 2	LoIP 3
Existence of identity in evidence	The existence of the identifying attributes in evidence of identity is not checked	Proofing party shall verify that the identifying attributes exist in corroborative evidence	Proofing party shall verify that the identifying attributes exist in authoritative evidence

Where additional supporting attributes are required to carry out identity proofing, the proofing party shall verify them. This process shall yield either valid verified information or non-verified information (which also includes mismatched information).

NOTE Information on the strength of evidence of identity is contained in 4.6. More information on verification processes and detecting fraud is contained in Annex B.

5.5 Identity is bound to a subject

For LoIP 1, the proofing party shall accept the subject is bound to the identity without carrying out any checking. For LoIP 2 and above, the proofing party shall establish that the subject is bound to the identity. The identity being accurate does not mean that the subject is represented by or associated with the identity. For example, the person can be claiming someone else's identity.

For LoIP 2 and above, if the subject is unable to be bound to the identity, the proofing party shall apply a documented exception process, as per the proofing policy. Such measures, in the exception process, shall be proportional to the LoIP. Table 6 shows the minimum requirements for identity binding.

This document refers to the following mechanisms for binding identity information as "factors".

— Something the subject knows: binding is established by a subject performing a mental task using information hidden from public knowledge. This can include verification against evidence of identity other than the evidence provided.

— Something the subject has: binding is established by a subject presenting physical evidence containing identity information to be verified against evidence of identity.

— Something the subject is: binding is established by comparing a biological or behavioural characteristic, observed by the proofing party, with reference biometric information known to correspond to the subject. This can involve automated recognition technology or manual comparison (e.g. face compared manually to a photograph or fingerprint compared manually to a reference fingerprint by a qualified fingerprint examiner.) with evidence of identity.

Table 6 — Minimum requirements by LoIP for Identity is bound to a subject

Objective	LoIP 1	LoIP 2	LoIP 3
Identity is bound to a subject	Binding to the identity is not checked	The proofing party shall check binding to the identity using one factor	The proofing party shall check binding to the identity using two or more factors

NOTE 1 Information on the strength of evidence of identity is contained in 4.6. Examples of binding are given in A.2.

The proofing party shall include in its risk assessment, consideration of masquerading and impersonation attacks, and apply controls to mitigate to an acceptable level the associated risks.

NOTE 2 Identity to subject binding is not explicitly mentioned in ISO/IEC 29115 but is required for persons to reduce the likelihood of identity theft and impersonation.

© ISO/IEC 2018 – All rights reserved

Annex A
(informative)

Evidence of identity and binding examples

A.1 Evidence of identity examples

Table A.1 provides examples of national authoritative and corroborative evidence for commonly used identifying attributes as determined by each jurisdiction. It does not include additional commercial corroborative evidence that exist to support digital economies in many developed countries.

Table A.1 — Examples of evidence of identity

Identifying attribute	Jurisdiction	Authoritative evidence or party examples	Corroborative evidence examples
Name at birth	CN	Birth Certificate, Identity Card, Social Security Card, Driving License, Passport	
	ES	Local/central Civil Register	Passport, driving licence, eID
	GB	HM Passport Office — General Records Office — Retained register of birth certificate(s) and Passport database	ICAO biometric passport, EU EC2252/2004 identity card, UK biometric residency permit
	IR	General Register Office	Public Services Card, Social Services Card, Medical Card, Drug Payment Scheme (DPS) Card, European Health Insurance Card
	IT	National identity register	Passport, driving licence, nautical licence, pension book, firearms licence, national identity card, national eID
	KR	ID database operated by Ministry of Interior and Security, driving license database, passport database	Resident Registration ID Card, Certificate for family relation, KR passport, Driver License
	MY	MyKAD, National Registration Department (NRD)	Passport, Driving License
	NL	Basic Registry of People (BRP)	Birth certificate, passport, NL driving licence, IdentityCard
	NZ	Birth register	NZ Passport, Birth certificate, Driver Licence
	US	Birth Certificate, Social Security Registry, Passport[a], driving license[a], I-90 ("Green Card")	Financial or utility account, credit bureau

[a] Cited in NIST/SP 800-63-2, Table 3, as an example of a "primary government ID"; therefore, implicitly authoritative.

Table A.1 *(continued)*

Identifying attribute	Jurisdiction	Authoritative evidence or party examples	Corroborative evidence examples
Date of birth	CN	Birth Certificate, Identity Card, Social Security Card, Driving License, Passport	
	ES	Local/central Civil Register	Passport, driving licence, eID
	GB	HM Passport Office — General Records Office — Retained register of birth certificate(s) and Passport database	ICAO biometric passport, EU EC2252/2004 identity card, UK biometric residency permit
	IT	National identity register	Passport, driving licence, nautical licence, pension book, firearms licence, national identity card, national eID
	IR	General Register Office	Public Services Card, Social Services Card, Medical Card, Drug Payment Scheme (DPS) Card, European Health Insurance Card
	KR	ID database operated by Ministry of Interior and Security, driving license database, passport database	Resident Registration ID Card, Certificate for family relation, KR passport, Driver License
	MY	MyKAD, National Registration Department (NRD)	Passport, Driving License
	NL	Basic Registry of People (BRP)	Birth certificate, passport, NL driving licence, IdentityCard
	NZ	Birth register, NZ Passport database	NZ Passport, Birth certificate, NZ Electronic Identity Credential, Driver Licence, 18+card
	US	Birth Certificate, Social Security Registry, Passport[a], I-90	Financial or utility account, credit bureaux
Place of birth	CN	Birth Certificate, Social Security Card Database, Identity Card Database	
	ES	Local/central Civil Register	Passport, driving licence, eID
	GB	HM Passport Office — General Records Office — Retained register of birth certificate(s) and Passport database	ICAO biometric passport, EU EC2252/2004 identity card, UK biometric residency permit
	IT	National identity register	Passport, driving licence, nautical licence, pension book, firearms licence, national identity card, national eID
	IR	General Register Office	

[a] Cited in NIST/SP 800-63-2, Table 3, as an example of a “primary government ID”; therefore, implicitly authoritative.

© ISO/IEC 2018 – All rights reserved

Table A.1 *(continued)*

Identifying attribute	Jurisdiction	Authoritative evidence or party examples	Corroborative evidence examples
	KR	ID database operated by Ministry of Interior and Security	Resident Registration ID Card, Certificate for family relation', KR passport, Driver License
	MY	National Registration Department (NRD)	Passport
	NL	Basic Registry of People (BRP)	Birth certificate, passport, NL driving licence, IdentityCard
	NZ	Birth register, NZ Passport database	NZ Passport, Birth certificate, NZ Electronic Identity Credential
	US	Birth Certificate, Social Security Registry, Passport[a], I-90 (Country only)	Financial or utility account, credit bureau
Other official name/s	CN	Birth Certificate, Identity Card, Social Security Card, Driving License, Passport	
	ES	Local/central Civil Register	Passport, driving licence, eID
	IR	General Register Office	
	IT	National identity register	
	MY	National Registration Department (NRD)	Passport
	NL	Basic Registry of People (BRP)	Passport, NL driving licence, IdentityCard
	NZ	Birth register, NZ Passport database	NZ Passport, Birth certificate, NZ Electronic Identity Credential, Driver Licence, 18+card
	US	Social Security Registry, Passport[a], driving license[a], I-90	Financial or utility account, credit bureaux
Address	CN	Identity Card, Driving License	
	IR	General Register Office	Utility bill, Active insurance policy (health/life/house/car), Bank statement, Letter from Department of Social Protection/Revenue
	IT	National identity register	Passport, driving licence, nautical licence, pension book, firearms licence, national identity card, national eID
	KR	ID database operated by Ministry of Interior and Security, driving license database, passport database	Resident Registration ID Card, Certificate for family relation, Driver License
	MY	MyKAD, National Registration Department (NRD)	Utility bills, driving license

[a] Cited in NIST/SP 800-63-2, Table 3, as an example of a "primary government ID"; therefore, implicitly authoritative.

Table A.1 *(continued)*

Identifying attribute	Jurisdiction	Authoritative evidence or party examples	Corroborative evidence examples
	NL	Basic Registry of People (BRP)	
	NZ	None	Driver Licence, Address Verification Service, Bank statement, Utility account
	US	US Postal Service, Social Security Registry, driving license[a]	Financial or utility account, credit bureau
Phone number	CN	Telecommunication provider database	
	KR	Telecommunication provider database	
	MY	Telco providers	
	NZ	Telecommunication provider database	Telco. utility account
	US	Telecommunication provider database	
Email address	US		Financial or utility account, credit bureau
Facial image	CN	Identity Card Database, Social Security Card Database, Driving License Database, Passport Database	
	ES	Passport database, driving licence database, eID database (different images)	Passport, driving licence, eID
	GB	HMPO passport database/passport, UK biometric residence permit, EEA/EU Government issued identity cards that comply with Council Regulation (EC) No 2252/2004	EEA/EU full driving licences that comply with European Directive 2006/126/EC
	IR	General Register Office	Irish Passport, Driving Licence, or Learner Permit, Irish Public Services Card, Irish Certificate of Naturalisation Passport for all non-Irish citizens, EU ID card, UK driving licence
	IT	National identity register	Passport, driving licence, nautical licence, pension book, firearms licence, national identity card, national eID
	KR	ID database operated by Ministry of Interior and Security, driving license database, passport database	Resident Registration ID Card, KR passport, Driver License
	MY	MyKAD, Passport, National Registration Department (NRD)	Driving License

[a] Cited in NIST/SP 800-63-2, Table 3, as an example of a “primary government ID”; therefore, implicitly authoritative.

© ISO/IEC 2018 – All rights reserved

Table A.1 *(continued)*

Identifying attribute	Jurisdiction	Authoritative evidence or party examples	Corroborative evidence examples
	NL	Basic Registry of People (BRP)	Passport, NL driving licence, IdentityCard
	NZ	The person who is the subject of the facial image	NZ Passport, Driver Licence, 18+card
	US	Passport database, driving licence database	
Fingerprint	CN	Identity Card Database, Passport Database	
	KR	ID database operated by Ministry of Interior and Security, passport database	Resident Registration ID Card
	MY	MyKAD, Passport, National Registration Department (NRD)	
	NZ	The person who is the subject of the finger print	
Resident Registration Number (National Identifier)	CN	Identity Card Number	
	KR	ID database operated by Ministry of Interior and Security, driving license database, passport database	Resident Registration ID Card, Certificate for family relation, KR passport, Driver License
	MY	MyKAD, National Registration Department (NRD)	Passport, Driving License
	US	Social Security Registry, I-90 ("Green Card")	

[a] Cited in NIST/SP 800-63-2, Table 3, as an example of a "primary government ID"; therefore, implicitly authoritative.

A.2 Binding examples

Table A.2 provides examples of different mechanisms which can be used to establish binding at the stated LoIP(s) as determined by each jurisdiction.

Table A.2 — Examples of binding processes

Jurisdiction	Mechanism	LoIP
CN	In-person comparison of the face of a person with a photo of Identity Card/ Social Security Card/Passport	2, 3
GB	In-person comparison of the face of a person with a photo identification document held in Authoritative or Corroborative Evidence	3
GB	Online comparison of the face of the person with a digital image in Authoritative or Corroborative Evidence	2
GB	Knowledge based questions that only the person who owns the identity would be expected to know	2
KR	In-person comparison of the face of a person with a photo identification of an official ID (e.g. Resident registration ID, Passport, Driver license)	2
KR	Verification against identity data from prior identity verification processes of e.g. LoIP 3 (e.g. SMS authentication, Internet personal identification number, Licensed public key certificate)	3
KR	Verification against finger print image prior identity verification processes of e.g. LoIP 3 (e.g. Resident Registration ID card)	3

Table A.2 *(continued)*

Jurisdiction	Mechanism	LoIP
MY	Verification against finger print template and identity attributes (e.g. name, photo, date of birth, ID number) in National Registration Identity Card (MyKad) issued by National Registration Department (NRD)	3
MY	Verification against identity attribute in National Registration Identity Card (MyKad) issued by National Registration Department (NRD)	2
NZ	In-person comparison of the face of a person with a photo identification document held in Authoritative or Corroborative Evidence	2
US	In-person comparison of the face of a person with a photo identification document	1, 2, 3
US	CIP requirements of USA PATRIOT Act and other such instruments (in-person)	1, 2, 3

© ISO/IEC 2018 – All rights reserved

Annex B
(informative)

Contra-indications and fraud detection

B.1 Introduction

Evidence for identity proofing can be physical and non-physical.

Sources of contra-indicator can also include law enforcement and sources of known fake or stolen identities (e.g. watch lists), where available.

B.2 Contra-indications of physical evidence of identity

Where physical EOI is used, real and false items can be presented. Table B.1 shows the categories of evidence and how each of the checks undertaken is designed to establish whether the evidence is true or false.

Table B.1 — Evidence of identity checking outcomes

	Evidence of identity			
	Real	**Stolen/Sold**	**Tampered**	**Counterfeit/Fake**
Identity	Real	Real	Real or False[a]	Real or False[b]
Physical evidence checks	Pass	Pass	Fail	Fail
Bound to subject	Pass	Fail	Pass	Pass
Verification with issuing party[c]	Pass	Pass or Fail[d]	Fail	Pass or Fail[b, e]
Corroboration	Pass	Likely to be weak	Likely to be weak	Likely to be weak

[a] Tampered does not mean the identity is incorrect, it can be a genuine identity being inserted on to the evidence.

[b] Counterfeit or fake evidence can contain real or false identity information. Real information can return a pass when verified.

[c] Verification with issuing parties across national borders should be carried out where possible.

[d] Depends on whether the evidence has been reported missing.

[e] If a clone exists, then two versions of the same evidence are in circulation, one real and one fake. Verification with the issuing party shows a Pass until such time as the fake is detected and action is taken. Cryptographically bound evidence can mitigate this risk.

The physical checking of evidence includes:

- checking all information in the application against the evidence for omissions, errors and contradictions;
- checking each item for its physical construction, material quality, print quality, security features, seals and signatures. This can include:
  - any signs of tampering (where a real item has been altered), such as photographs or printed data being altered, or the document being dismantled and reassembled, or pages not aligning (e.g. in a passport);
  - any signs of it being a counterfeit or fake document. Many items have security features that are difficult to fake and require expert skills or special machines to detect fakes. For example,

automated ultraviolet ICAO checks of passports. Checks without such skills or machines are likely to fail to detect a fake item of evidence.

- physical checking should to be carried out by capable people who have the skills, tools and capability to detect counterfeit or tampered evidence.

B.3 Contra-indications of verification

During the verification process the checking of the proofing information can be based on specific supplied evidence or by self-claim. In either case, contra-indicators can include:

- wholly contradicting information, presented in the application or evidence; or
- partially contradictory information presented in the application or evidence. This can be an indicator of keying errors or events such as name changes, which should be ruled out before treating as a potential fraud;
- a verification response that indicates the evidence has been reported as lost or stolen;
- a verification response that indicates the evidence does not have an active status (e.g. suspended, expired, revoked etc.);
- other factors (e.g. geolocation, time etc.).

B.4 Biometric recognition

Biometric data may be acquired and stored to ensure uniqueness of identity for subjects enrolled in a context or for authenticating subjects when conducting transactions in the context. During identity proofing, biometric data in the identity source can be searched to detect an attempt by a subject to claim multiple enrolments under different identities or to claim enrolment under the identity of another subject.

Biometric authentication typically involves a 1:1 (one-to-one) comparison of a biometric sample obtained from a subject against a stored biometric reference for the identity claimed by the subject. Detection of multiple enrolment attempts requires a 1:many (one-to-many) search of the enrolment database comparing the biometric sample obtained from a subject against the biometric references of all previous subject enrolments. One-to-many searches place more stringent requirements on the accuracy of the biometric technology employed and can require the use of multiple biometric samples or modalities.

Where cultural sensitivities make a specific biometric characteristic capture and proofing difficult, alternative biometric or non-biometric options may be considered. However, many have successfully addressed cultural sensitivities when acquiring necessary biometric data. Relying party and legal requirements can be such that it is possible that cultural sensitivities need to be compromised, if trust is to be achieved.

Biometric recognition, as with other recognition and verification technologies, can be subject to error. In the case of biometrics, recognition errors occur in two forms; as false matches (where a subject is falsely recognized as someone else), and false non-matches (where a subject fails to be recognized). The latter course only applies if the subject is enrolled and can therefore be recognized. It can be noted that presentation attacks are possible against the biometric product used in the system.

Biometric recognition cannot be used in isolation or in place of the verification of other identifying attributes. Any contra-indicator caused by a mismatch is investigated by biometric comparison experts before referral for identity fraud investigation.

© ISO/IEC 2018 – All rights reserved

B.5 Interviews

Interviewing is normally carried out in-person, and is carried out for three reasons:

- to deter fraudulent applicants;
- to identify abnormal behaviour;
- to bind the subject to the claimed identity and supporting EOI.

Interviewing procedures heavily depend on the national data protection rules and regulations of the concerned country.

Interviewing techniques need to be sufficient to satisfy these three reasons beyond reasonable doubt. Clause B.5 provides guidance on the typical leading practice techniques. Where an interview is carried out remotely, it is essential that either the subject's actions are independently witnessed and recorded for the purpose of the interview, or the subject is required to carry out live video streaming. Live video streaming involves establishing a video connection between the interviewer and the subject, then the interviewer asks the subject to carry out a series of actions that results in live video that can be compared against known images.

A real-time interaction between the subject and an interviewer representing the identity proofing service can be used as a means of verification and binding of the identity and the subject, where there are suspicions about the validity of the evidence or the application. An interview with the subject can provide an opportunity to explore the binding of the subject to the claimed identity. Questioning the subject on details of the identity claim and about any potential discrepancies between evidence presented and the claim should yield responses that can help to confirm or deny the binding. This can be as a result of additional proofing information provided by the subject or the behaviour of the subject during the interview.

Person to person verification can take place remotely or locally dependent on the suspicion or evidence requiring verification.

The interviewer should:

- be qualified in appropriate interview techniques;
- be qualified in appropriate document checking techniques;
- use appropriate document checking equipment;
- use information not in the public domain and expected to be known only by the genuine subject to establish binding of the subject to the identity;
- carry out the interaction in an appropriate environment and under appropriate conditions.

To identify fraudulent applications, interviewers should:

- use information from the application and other sources (e.g. banks) to support questioning;
- interview the applicant about information held in the supporting documents and, where possible, related information known to the proofing party, which is not in the documents (e.g. information about a bank account associated with a utility bill presented to support the application);
- adjust their technique and ask the same question at different points in the interview and in different ways to ensure unpredictability in the questioning;
- question family relationships, history and movements, and key life events;
- assess their behaviour. In some instances, in-person interviews are very effective in deterring fraud. For record-keeping and integrity of the identity proofing process interviews c be witnessed or videoed in a manner that creates a clear audio and visual record so that the subject is unequivocally identifiable;

- provide more in-depth comparison of the physical appearance of the subject with a photographic image, to establish any discrepancies. It may also include an evaluation of other physical characteristics.

Other aspects of interviewing that can impact the ability, positively or negatively, to detect fraud include:

- the subject being interviewed is not normally accompanied;
- where translation is required (the proofing party can provide the translator to increase integrity);
- where the applicant is unable to communicate for reasons of physical or mental difficulty and attends with a caregiver (the proofing party can also provide a qualified caregiver or medical staff to ensure the interview is carried out correctly and without bias or detriment to the applicant's health). In these circumstances, the interview should be conducted face-to-face and not remotely;
- where cultural sensitivities exist, arrangements can be made for such needs as privacy, same-sex interviews and biometric data capture;
- where a minor is being interviewed, they should be accompanied by representative
- if the interview is done remotely:
- there is sufficient additional monitoring by trusted persons and/or trusted surveillance sensors and video recording to prevent fraud or misrepresentation;
- there can be additional verification checks, prior to the interview, to establish the degree of risk associated with the applicant and the likelihood they can seek to subvert the interview. Where the risk is high, an in-person interview should take place.

If, at the end of the interview, the interviewer is not comfortable that all the requirements have been sufficiently met and/or believes that something is still not right about the application, they should refer the application for further investigation.

© ISO/IEC 2018 – All rights reserved

Bibliography

[1] ISO/IEC 24760 (all parts), *Information technology — Security techniques — A framework for identity management*

[2] ISO/IEC 29115, *Information technology — Security techniques — Entity authentication assurance framework*

[3] Recommendation ITU-TX.1252 (2010), *Baseline identity management terms and definitions* http://www.itu.int/SG-CP/example_docs/ITU-T-REC/ITU-T-REC_E.pdf

[4] Recommendation ITU-TX.1254 (2012), *Entity authentication assurance framework* https://www.itu.int/rec/T-REC-X.1254-201209-I/en

[5] ENISA. Mapping (Interoperable Delivery of European e-government services to public Administrations, Businesses and Citizens) IDABC Authentication Assurance Levels to SAML v2.0

[6] "OECD Recommendation for Electronic Authentication and OECD Guidelines for Electronic Authentication" http://www.oecd.org/dataoecd/32/45/38921342.pdf

[7] British Government Good Practice Guide 45 — Identity Proofing & Verification of an Individual (Issue 2.2) https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/370033/GPG_45_identity_proofing_v2_3_July_2014.pdf

[8] The National e-Authentication Framework http://www.finance.gov.au/policy-guides-procurement/authentication-and-identity-management/national-e-authentication-framework/

[9] Special pub. NIST 800-63-2, Electronic Authentication Guideline, August 2013 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf

[10] OMB M-04-04, *e-Authentication Guidance for Federal Organization* https://georgewbush-whitehouse.archives.gov/omb/memoranda/fy04/m04-04.pdf

[11] PRINCIPLES FOR ELECTRONIC AUTHENTICATION. A Canadian Framework http://publications.gc.ca/Collection/Iu64-16-2004E.pdf

© ISO/IEC 2018 – All rights reserved

ICS 35.030

Price based on 21 pages

© ISO/IEC 2018 – All rights reserved