



ISO/IEC JTC 1/SC 27 **N14162**

ISO/IEC JTC 1/SC 27/WG 5 **N514162**

REPLACES: N13379

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

**DOC TYPE:** Working Draft text

**TITLE:** Text for ISO/IEC 4<sup>th</sup> WD 29003 -- Information technology – Security techniques – Identity proofing

**SOURCE:** Project Editor: Joanne Knight (NZ)  
Project Co-editors: Patrick Curry (UK), Anthony Nadalin (US)

**DATE:** 2014-06-15

**PROJECT:** 29003 (1.27.103)

**STATUS:** In accordance with resolution 2 (contained in SC 27 N14199) of the 17th SC 27/WG 5 Plenary meeting held in Hong Kong, Special Administrative Region of China, 7-11 April 2014 this document is circulated for study and comment.

National Bodies, experts and liaison organisations of SC 27/WG 5 are requested to send their comments / contributions on the above-mentioned document by 2014-09-24.

PLEASE submit your comments / contributions on the hereby attached document via the SC 27 e-balloting/commenting website at:  
<http://isotc.iso.org/livelink/livelink/open/jtc1sc27>

**PLEASE NOTE:** For comments please use the SC 27 TEMPLATE separately attached to this document.

**ACTION:** COMM

**DUE DATE:** 2014-09-24

**DISTRIBUTION:** P, O- and L-Members  
W. Fumy, SC 27 Chairman  
M. De Soete, SC 27 Vice-chair  
E. J. Humphreys, T. Chikazawa, M. Bañón, J. Amsenga, K. Rannenberg, WG-Conveners

**MEDIUM:** Livelink-server: <http://isotc.iso.org/livelink/livelink/open/jtc1sc27>

**NO. OF PAGES:** 1 + 35

**ISO**

International Organisation  
for Standardisation



**IEC**

International Electrotechnical  
Commission



## **International Standard ISO/IEC WD4 29003**

### **Information technology — Security techniques — Identity Proofing**

***[Editorial Note:***

***This version of the standard is limited to Person entities. The remaining entities –Device, Software & Organisation – will be addressed in later versions.***

***Text on these three entities is contained in the Working Draft 3 document and will be carried into this standard in due course.]***

## CONTENTS

*Page*

Forward .....	iii
Introduction .....	iv
Relevant Documents to be Considered .....	iv
Liaison Organisations .....	iv
Other Organisations .....	iv
1 Scope .....	1
1.1 Statement of scope .....	1
1.2 Original statement of scope .....	1
2 Normative references .....	3
2.1 Identical International Standards .....	3
2.2 Paired International Standards .....	3
2.3 Additional references .....	3
3 Terms and definitions .....	3
3.1 Terms used as defined in ISO/IEC 29115:2013 .....	3
3.2 Other terms .....	4
4 Abbreviations .....	6
5 Conventions .....	7
6 Identity Proofing Context .....	7
6.1 ISO/IEC 29115:2013 .....	7
6.2 Identity information .....	7
6.3 Identity information sources .....	8
6.4 Evidence of identity .....	8
6.5 Actors .....	9
7 Concepts .....	10
7.1 Entity and Identity Life cycles .....	10
7.2 Enrolment phase overview .....	11
7.3 Levels of assurance .....	12
7.4 Leveraging previous IPV processes .....	13
8 Requirements for Identity Proofing and Verification .....	15
8.1 Establishment of the IPV process .....	15
8.2 Conducting an IPV process .....	17
9 Person IPV .....	20
9.1 Person identity attributes .....	20
9.2 Person IPV minimum requirements .....	21
9.3 Person IPV additional guidance .....	22
Annex A .....	24
Annex B .....	27
Annex C .....	29
Bibliography .....	30

## Forward

ISO (the International Organisation for Standardisation) and IEC (the International Electrotechnical Commission) form the specialised system for worldwide standardisation. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organisation to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organisations, 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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 29003 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

## Introduction

An International Standard (IS) for identity proofing and verification (IPV) is required to which other identity management standards can refer, based on the four Levels of Assurance described in ISO/IEC 29115:2013 or other similar standards.

Existing and emerging IS for identity management focus primarily on the policy and technical standards for the operation of identity management and access management systems. They describe the use of credentials and make reference to processes for the issuance of identity credentials. These issuance processes are dependent upon entity IPV processes for which no reference standards exist. Further, an increasing number of governments seek a set of IPV standards upon which they can enhance their national IPV processes in a way that is more aligned internationally, to meet a wide range of pressing immigration, societal, security and business needs.

This IS is intended to be used principally by registration authorities (RA) in support of credential service providers (CSPs) and by others having an interest in their services (e.g., relying parties and auditors of those IPV services) described in ISO/IEC 29115:2013 - Entity Authentication Assurance Framework (EAAF).

## Relevant Documents to be Considered

### National Documents to be Considered— Current Versions of:

Canada, British Columbia Evidence of Identity Standard

Malaysia – National Registration Act 1959

New Zealand Evidence of Identity Standard 2009

UK Good Practice Guides 45 and 46 – Identity Verification & Validation

The Financial Action Task Force - The Forty Recommendations -  
[www.oecd.org/newsroom/2789371.pdf](http://www.oecd.org/newsroom/2789371.pdf).

### Liaison Organisations

As part of this work, harmonisation with other organisations which are pursuing identity proofing work will occur to include non-standards development bodies such as: FIDIS, ITU-T JCA Cloud, ITU-T SG17, ITU-T SG13, Kantara Initiative and ITU-T JCA IDM.

### Other Organisations

National equivalents of a Ministry of Justice, a Ministry of Internal Affairs and Communications, and a National Police Agency and other national organisations with responsibilities relevant to ISO/IEC 29003.

## INTERNATIONAL STANDARD &lt;29003&gt;

**Information technology — Security techniques — Identity proofing****1 Scope****1.1 Statement of scope**

This International Standard (IS) provides best practices and guidance on required processes for the establishment of an entity's identity for parties using or expecting to use ISO/IEC 29115. This standard is used to establish an entity's identity to an understood Level of Assurance in accordance with ISO/IEC 29115, and prior to delivery of a service to that entity.

In scope:

- a) The identity proofing and verification requirements to be used as a national body standard in support of enrolment of entities. Definitions of identity proofing and verification (IPV) principles, risk assessment, and controls sufficient to meet the requirements of ISO standards for entity authentication, including ISO/IEC 29115. These controls shall take account of threats, counter-fraud requirements and best practices described by law enforcement organizations.
- b) An entity is understood in this standard to be something that has separate and distinct existence and that can be identified. This should include:
  - 1) Persons
  - 2) Devices
  - 3) Software applications
  - 4) Organisations
- c) A resulting standard that is sufficient for:
  - 1) Nations and industry to have confidence in using them
  - 2) Nations and industry to have confidence in the results of each others' national IPV systems and the credentials
  - 3) Certification bodies to develop assessment and audit criteria against which certified auditors can successfully conduct Trusted Third Party (TTP) audit and assurance of IPV

Out of scope:

- a) The system requirements for the identity media infrastructure, the establishment of "identity authorities", the physical requirements for identity media, requirements for relying parties, Personal Identity Information exchange requirements.
- b) Audit and compliance requirements.

*[Editors note: Reference to In and Out of Scope to be removed before final publication]*

**1.2 Original statement of scope**

*[Editors' note: The following is the previous statement of scope included temporarily to allow comparison with the scope agreed at Hong Kong]*

This International Standard (IS) provides best practices and guidance on required processes for the initial establishment and subsequent confirmation of an entity's identity for parties using, or expecting to use, ITU-T X.1254, ISO/IEC 29115:2013 or other similar standards. The material is

used to establish and/or confirm identity and thus should give greater confidence in an entity's identity prior to the issuance of identity credentials or delivery of a service to that entity, by or for that entity.

In scope:

- a) The development of identity proofing and verification (IPV) processes to be used as a national body standard in support of the enrolment of entities. Definitions and controls are provided for IPV principles and risk assessments that are sufficient to meet the requirements of ISO identity management standards for entities, notably ITU-T X.1254 / ISO/IEC 29115:2013. These controls take account of threats, counter-fraud requirements and best practice guidance described by national policy specifications from government organisations.
- b) Entities that require identity proofing and verification in accordance with this and associated ISO standards are:
  - 1) Persons;
  - 2) Devices or Security Modules, particularly (but not limited to) for computer and telecommunication use cases, including e.g. Trusted Platform Module (TPM), Mobile Trusted Module (MTM) and similar approved standards. This includes products with parts or identifiable components whose integrity and authenticity is being asserted;
  - 3) Software. Services, which may include network and application protocols such as SSL/TLS and VPN, which employ trust-based models using certificates, etc. Software, which may include firmware, operating system code, application code or executable scripts;
  - 4) Organisations, non-person entities that exist to carry out business in all kinds of organisations, including government, industry and voluntary.

NB: For the purposes of trust, all persons, devices and software have a relationship with one or more organisations for reasons of employment, ownership, issuance and management.

- c) A resulting International Standard that is sufficient for:
  - 1) Nations and industry to have confidence in using identities proven according to requirements of that standard;
  - 2) Nations and industry to have confidence in the results of each others' national IPV systems and the credentials;
  - 3) Certification bodies to develop assessment and audit criteria against which certified auditors can successfully conduct audit and assurance of IPV service providers;
  - 4) Establishing a foundation for mutual recognition of identity proofing arrangements between nations and industries.

Out of Scope:

- Vetting is outside the scope of this International Standard.

## 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.

- ITU-T X.1254: Information technology — Security techniques — Entity Authentication Framework;
- ISO/IEC 29115:2013: Information technology — Security techniques — Entity Authentication Framework.

### 2.1 Identical International Standards

None.

### 2.2 Paired International Standards

None.

### 2.3 Additional references

## 3 Terms and definitions

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

### 3.1 Terms used as defined in ISO/IEC 29115:2013

authentication

authoritative source

claim

context

credential

credential service provider

entity

entity authentication assurance

identity

identity information verification

identity proofing

registration authority

relying party

time stamp

transaction

trust framework



## 3.2 Other terms

### 3.2.1

#### **applicant**

person making an application, who is either the subject of the application or is acting on behalf of the entity and is already registered at the same LoA

### 3.2.2

#### **application**

process where data is collected from an applicant for enrolment

NOTE Application is usually is the first step in the enrolment process.

### 3.2.3

#### **assertion**

statement made by an authoritative source to a relying party containing authoritative identity information

### 3.2.4

#### **assured identity**

identity that has been determined as genuine after a successful application of IPV to a given Level of Assurance

### 3.2.5

#### **certification body**

third party that assesses and certifies a client organisation with respect to published standards, and any supplementary documentation required under the certification system

### 3.2.6

#### **contra-indicators**

pieces of information that either contradict statements from the applicant or raise some doubt over whether the application is legitimate

### 3.2.7

#### **corroborative source**

source, register or database of entities' identity attributes and supporting information against which identity information verification can occur

NOTE A corroborative source may not be as up-to-date or accurate as the authoritative source

### 3.2.8

#### **enrolment**

process of inauguration of an entity into a context

### 3.2.9

#### **evidence of identity**

combination of evidence types that provide confidence that an entity possesses the attributes being claimed

### 3.2.10

#### **identity entity binding**

process of checking by a verifier that the identity is bound to the entity at a desired LoA

### 3.2.11

**identity referee**

trusted referee

entity who provides a reference in relation to knowledge of an entity and their link to a claimed identity

NOTE Identity referees will often be more specifically defined by a registration authority setting criteria such as being an adult, knowing the entity for a period of time and not being related etc.

**3.2.12**

**registration**

process whereby, having successfully completed the IPV process, the entity's identity data is recorded in a register

**3.2.13**

**relying party**

entity that relies on the verification of identity information for a particular entity

NOTE A relying party is exposed to risk caused by incorrect identity information. Typically it has a trust relationship with one or more identity information authorities.

[SOURCE: ISO/IEC 24760-1, 3.3.7]

**3.2.14**

**subject**

entity contained in the application, whose identity is being proofed and verified

**3.2.15**

**verification**

process to determine that presented identity information associated with a particular entity is applicable for the entity to be recognised in a particular context

NOTE Verification can involve checking that the required attributes are present, have the correct syntax, and exist within a defined validity period

[SOURCE: ISO/IEC 24760-1:2011, 3.2.2, modified – the word 'context' replaces 'domain' and the words 'at some point' have been deleted.]

**3.2.16**

**verifier**

entity that performs verification

NOTE A verifier may be the same as, or act on behalf of, the entity that controls identification of entities for a particular context.

[SOURCE: ISO/IEC: 24760-1:2011, 3.3.6, modified – in the Note the word 'context' replaces 'domain'.]

## 4 Abbreviations

For the purposes of this International Standard, the following abbreviations apply:

CSP	Credential Service Provider
e-ID	Electronic Identity Document
EAAF	Entity Authentication Assurance Framework
ICT	Information and Communications Technology
ID	Identity Document
IEC	International Electrotechnical Commission
IPV	Identity Proofing and Verification
IS	International Standard
ISO	International Standards Organisation
ITU-T	Telecommunication Standardisation Sector for the International Telecommunications Union
LoA	Level of Assurance
NPE	Non-Person Entity
PII	Personally Identifiable Information
RA	Registration Authority
RP	Relying Party
SAML	Security Assertion Markup Language
SSL	Secure Sockets Layer
TFP	Trusted Framework Provider
TLS	Transport Layer Security

## 5 Conventions

This International Standard follows the ISO Directive, Part 2, Annex H regarding verbal forms for the expression of provisions.

- a) “Shall” indicates a requirement;
- b) “Should” indicates a recommendation;
- c) “May” indicates a permission; and
- d) “Can” indicates a possibility and capability.

## 6 Identity Proofing Context

This standard complements aspects of ISO/IEC 29115:2013 Information technology -- Security techniques -- Entity authentication assurance framework, specifically the enrolment phase, addressed therein.

This chapter outlines the relationship between this standard and ISO/IEC 29115:2013. It also provides the context for where identity proofing processes fit within the wider Entity Authentication Assurance Framework (EAAF).

### 6.1 ISO/IEC 29115:2013

The Entity Authentication Assurance Framework (EAAF), which is the subject of ISO/IEC 29115:2013, outlines three phases in its model –

- Enrolment phase – consists of four processes: application and initiation; identity proofing and identity information verification; record-keeping/recording; and registration;
- Credential management phase – consists of all processes relevant to the life cycle management of a credential and may involve some or all of: creation; issuance; binding; activation; storage; revocation; renewal and/or replacement; and record-keeping;
- Entity authentication phase – consists of the entity’s use of its credential to attest to its identity to a relying party.

This IS expands on the Enrolment phase outlined in clause 8.1 of ISO/IEC 29115:2013 with specific focus on the identity proofing and identity information verification of an entity. As outlined in the introduction to this clause, other phases and processes within the EAAF will have an impact.

In developing the detail of this IS, and providing the ability to operationalise the IPV process, there has been a need to evolve the content of ISO/IEC 29115:2013. This includes but is not limited to adding additional requirements and further refining some terms used in ISO/IEC 29115:2013.

### 6.2 Identity information

Identity information is a subset of all the information that will be required to establish and maintain a relationship with an entity. In this IS, identity information shall include both the attributes that represent the identity and the information required to be collected and recorded in order to carry out the identity proofing and verification process.

During the enrolment process, other information may be collected to enable assessment of eligibility for services and/or capability for roles. Information may also be collected and assigned to

facilitate authorisation to information and services. While this information may also be subject to checking and verification, this is outside the scope of this document.

Any assessment of eligibility or capability of an entity shall be considered unreliable if the identity has not been proofed to the required LoA.

### 6.3 Identity information sources

For each identity attribute there should be an authoritative source available that can confirm the attribute and the binding of the attribute to the claimed identity. Most important attributes may often be captured in the first IPV process and identity registration for an entity; these attributes show evidence of history. The latest versions of some of these, and other, attributes are also important where up-to-date evidence is required.

Over the life of an entity they may have a number of identities registered in different contexts. Unless a permanent link is retained between an identity register and the authoritative source of an attribute and any changes occur in both registers simultaneously, the second register is likely to become out of date. This lack of a persistent link, and/or the absence of a link, means registers resulting from these IPV processes are considered corroborative sources.

Where an identity attribute does not have an authoritative source (other than the entity itself e.g. address), there is a residual risk that the verification result could be wrong. Reliance on the verification result should reflect the assessment the RA has made of the reliability of the source and the impact of any inaccuracy on the service to be provided.

A single credential verified against its issuing authority may contain attributes from both source types. The issuing authority may be an authoritative source for some attributes but only a corroborative source for others.

### 6.4 Evidence of identity

The enrolment process may occur using a number of channels (e.g. in-person, over the phone or online) and as such the evidence provided to support the application could be in a number of forms. It is the LoA being met that determines the stringency of the IPV process and the channel merely impacts the ability to meet certain requirements.

Evidence could include:

- Information provided by the entity, including biometric characteristics;
- Credentials including documents, devices or electronic identity credentials;
- Machine-based attestation;
- Information provided by referees.

It is possible for a single credential to meet all the evidential requirements for an IPV process<sup>1</sup>. Refer to clause 7.4 Leveraging previous IPV processes.

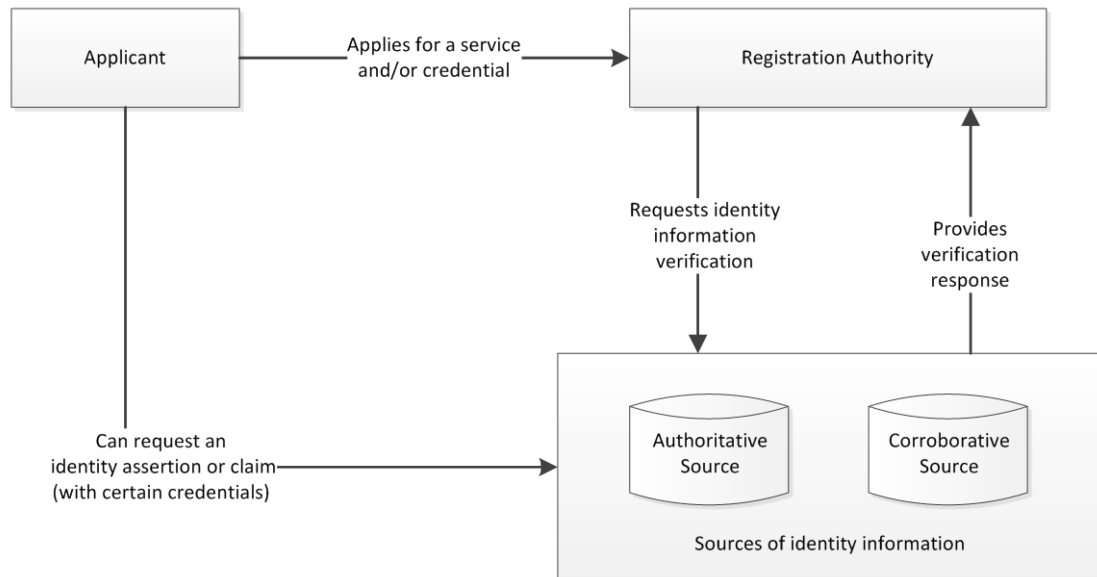
---

<sup>1</sup> A Standing Document [SD-NN] is being proposed in support of this International Standard for nations to list their IPV evidence and policy documents, including documents that are currently approved for electronic verification and non-electronic identity purposes. Nations would supply and regularly update their list of identity documents for proving/verifying identity within their own nation.

## 6.5 Actors

The actors involved in the IPV process include entities who are applicants, the registration authority (RA) and sources of identity information.

The following figure and sub clauses describe in more detail the actors in the IPV process.



**Figure 1 – Primary actor relationships**

### 6.5.1 Applicant

An application may be made by either the subject of the application or a person acting on their behalf. The identity proofing and verification process will be carried out on the subject.

### 6.5.2 Registration Authority

A registration authority (RA) establishes the identity of the applicant in order to supply the applicant with a service and/or credential. As such it operates a register of identities. An RA may carry out identity proofing and verification processes itself or contract portions to another party to do it on their behalf.

An RA who is carrying out identity proofing or identity information verification becomes a relying party (RP). They are relying on the accuracy and integrity of responses they receive.

### 6.5.3 Sources of identity information

As each source of identity information is the result of an IPV process carried out previously then any RA that has a register of identities may in turn make it available to future IPV process. The RA could have a register that is an authoritative source or corroborative source. The RA could also be an issuing authority of evidence which may contain information attributes that are authoritative and corroborative.

## 7 Concepts

This clause provides information on general concepts that, in addition to the clause on Identity Proofing Context, are important to enable different contexts to map their environments to this IS. This includes relevant text from ISO/IEC 29115:2013 and expands on it where required.

### 7.1 Entity and Identity Life cycles

Both entities and identities have life cycles. An entity can have multiple identities, each one relating to a different context. An entity may never have an identity in a particular context. Identity information that at some time related to an entity may continue to exist long (if not indefinitely) after the entity itself has ceased to exist. The following tables describe the general life cycle states.

State	Description	Examples
Pre-existence	Before the entity fully exists.	An unborn person, a programme being written but not yet released as an application, a device in the process of being manufactured.
Existence	The entity exists and is functioning or able to function. During existence many events may occur.	A living person, an organisation (whether it is actively trading or not), a physical device (whether it works or not).
Post-existence	The entity no longer exists.	A deceased person, an organisation that has been closed permanently from trading, a device that has permanently malfunctioned or been destroyed.

**Table 1 - Entity life cycles**

More detail on Entity life cycles may be found in Annex A

State	Description	Explanation
Established	Identity is known but is not ready for use.	An identity has been claimed as part of an application but has not yet been proofed and/or verified. Could also apply to an identity for an entity in pre-existence.
Active	Is current and usable.	Is complete for the context and has undergone an IPV process applicable to that context.
Suspended	Activity on an identity has been temporarily halted.	Some aspect of the identity is in question. E.g. activity is suspended to prevent damage while an investigation occurs. Identities may require to be re-verified at various intervals and will be suspended while this activity takes place.
Archived	The entity associated with the identity no longer exists.	The entity is deceased or has been destroyed. This status does not prevent posthumous activity from occurring where relevant.
'unknown' <i>An absence of any record</i>	Identity is not yet known to the context.  Identity has been deleted, purged or expunged.	Identity exists in other contexts but is not required by this context.  Where the indefinite retention of identities is not required an identity may be deleted in which case it would be as if it had never existed within the context. No status is required.

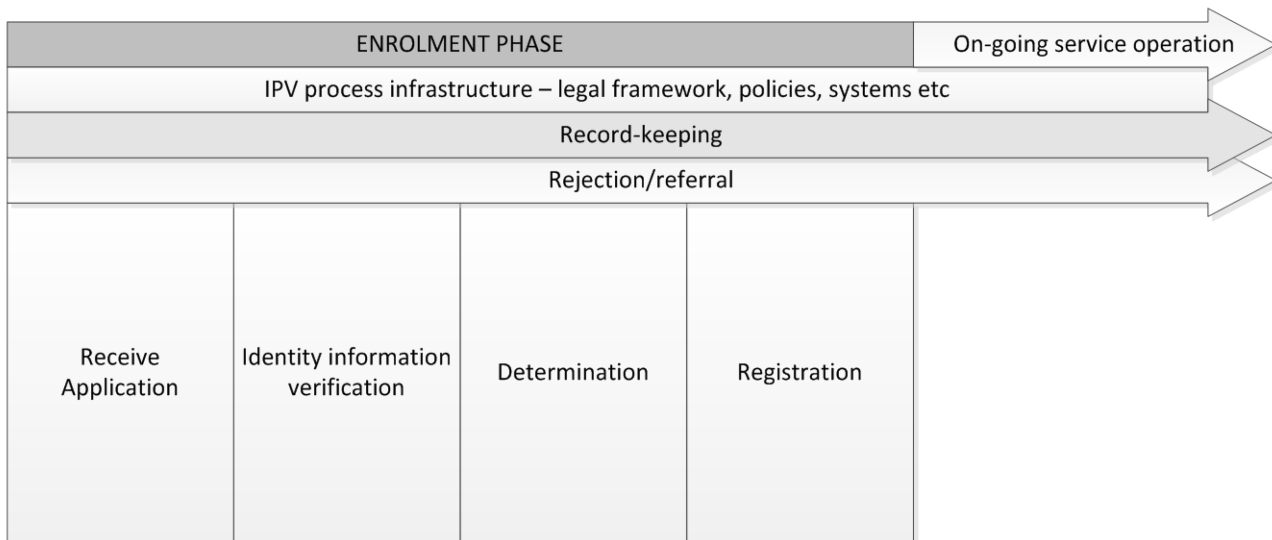
**Table 2 - Identity life cycles**

## 7.2 Enrolment phase overview

Enrolment is the first phase in the Entity Authentication Assurance Framework (EAAF), outlined in ISO/IEC 29115:2013, prior to the Credential Management Phase.

The enrolment phase can be initiated by the applicant or someone acting on their behalf. Either will usually be making an application to an RA in order to access a service or perform a transaction. It will usually result in the issuance of a credential to facilitate future contact. The application could also be for an identity credential only to facilitate other enrolment events.

The following figure outlines the enrolment phase as it relates to IPV.



**Figure 2 – IPV enrolment Process**

The processes shown above are not strictly sequential but overlap each other. Aspects within each process may be carried out at different times depending on operational requirements.

Aspects of the process will differ according to the rigour required to achieve the applicable LoA. In the case of an entity enrolling under LoA1, these processes are minimal or may not occur. In other cases, enrolment processes may be extensive.

### 7.2.1 Receive application

The applicant shall provide information and evidence during the application process. Also, record keeping begins when the application is received.

The detail of the application will be dependent upon:

- the requirements of this Standard;
- the applicable Level of Assurance;
- additional specific requirements of the applicable jurisdiction(s);
- additional specific requirements of the RA;
- the purpose for which the identity is to be used.

Initial checks shall be carried out on the application and the entity (if present) to ensure the application is valid before proceeding to the next stage. These checks involve direct interaction with the applicant (remotely or in person) and their application. The amount of checking will be determined by the LoA to be achieved. During the initial checking process the following activities generally occur:

- application will be checked for completeness;



- physical checking of presented identity credentials to detect possible fraud, tampering or counterfeiting – either manually or using technology;
- entity is bound to their identity;
- the identity is checked for uniqueness.

If the application is being made remotely it will not be possible to carry out physical checks on identity credentials and binding the entity to the identity will be more difficult. Instead, the process may involve the collecting of information, rather than credentials, for later verification and/or getting applicants to activate electronic credentials. The degree to which identity entity binding can occur will impact the acceptance of remote processes and the LoA that may be achieved.

### 7.2.2 Identity information verification

Identity information verification is the process of checking identity information and/or credentials against issuers, data sources, or other resources with respect to authenticity, validity, correctness, and binding to the entity. This process does not involve the applicant and uses pre-established relationships with various sources of authority and has the following outcomes:

- Verified information - where the information was checked and result was successful;
- Un-matched information – where the check was unsuccessful.

### 7.2.3 Determination and registration

Once all the checking processes have been completed a determination is made on whether to accept or reject the identity. The judgement about whether an identity is acceptable or not for a particular LoA is independent of any judgement about eligibility for a service or credential.

If the identity is accepted, and the non-IPV aspects of the enrolment allow, the identity will be registered, i.e. added to the register for that context.

Should the identity be rejected it will not be added to the register, however information about the process and decision will still be recorded. The application may also be referred for further examination or other follow up.

### 7.2.4 Record-keeping

Record-keeping is done throughout enrolment, on-going service operation and potentially indefinitely. Record-keeping begins with the receipt of the application, including the information and documentation that was collected (and may be retained). It continues through the identity proofing and information verification processes, recording the results of these steps, and other pertinent data. It records the decision to accept, reject, or refer the application. Where it is important for historic purposes, records of an identity and IPV process, or portions of them, may be kept long after the entity has gone and the identity has been closed.

Comprehensive and accurate records are important to provide evidence of integrity of the identity proofing processes and the proofing results.

## 7.3 Levels of assurance

ISO/IEC 29115:2013 defines objectives to be met by identity proofing processes for each of the four LoAs in the Entity Authentication Assurance Framework (EAAF).

Identity proofing processes at a higher LoA include the processes of the lower LoAs. For example, LoA3 identity proofing assumes that LoA1 and LoA2 identity proofing controls have been satisfied. Table 8.1 from ISO/IEC 29115:2013 is provided here in Table 3.

LoA	Description	Objective	Controls	Method of processing
<b>LoA1 - low</b>	Little or no confidence in the claimed or asserted identity	Identity is unique within a context	Self-claimed or self-asserted	Local or remote
<b>LoA2 - medium</b>	Some confidence in the claimed or asserted identity	Identity is unique within context and the entity to which the identity pertains exists objectively	Proof of identity through use of identity information from an authoritative source	Local or remote
<b>LoA3 - high</b>	High confidence in the claimed or asserted identity	Identity is unique within context, entity to which the identity pertains exists objectively, identity is verified, and identity is used in other contexts	Proof of identity through use of identity information from an authoritative source + identity information verification	Local or remote
<b>LoA4 – very high</b>	Very high confidence in the claimed or asserted identity	Identity is unique within context, entity to which the identity pertains exists objectively, identity is verified, and identity is used in other contexts	Proof of identity through use of identity information from multiple authoritative sources + identity information verification + entity witnessed in-person	Local only

**Table 3 - Applying Identity Proofing Objectives to the LoAs**

The appropriate LoA to be met by an identity proofing and verification process will be driven by an identity-related risk assessment of the subsequent service provided or credential issued. ISO/IEC 29115:2013, clause 6.5 provides more information on selecting the appropriate Level of Assurance.

Any implementation of an IPV process relies on the identity information and sources that are available to the applicant and RA. The reliability and accuracy of credentials, identity information, and sources determine the actual assurance provided by the enrolment phase.

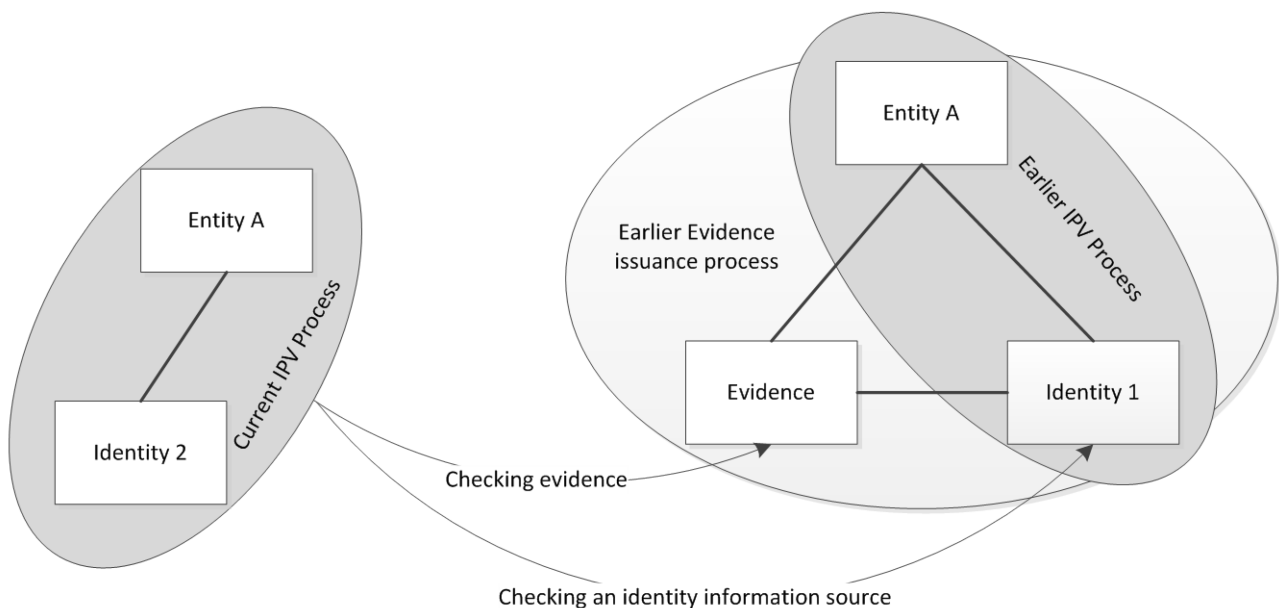
For more information on Levels of Assurance refer to ISO/IEC 29115:2013.

#### **7.4 Leveraging previous IPV processes**

Any IPV process that uses evidence (documents, credentials etc) is leveraging previous IPV processes. The RA needs to evaluate the earlier processes to establish the extent to which it will be able to contribute its own IPV process.

The overall LoA of any evidence is gained by the combined strength of three aspects; the IPV process, the credential (which could be a document) and the credential issuance process. The overall LoA will be determined by the aspect that has achieved the lowest LoA.

The figure below shows how the current process leverages the processes carried out in earlier IPV and credential issuance processes. It also shows how, during the identity information verification step, a source of identity information can also be checked.



**Figure 3 – Leveraging previous IPV processes**

Not all credentials issued during the credential management phase of the EAAF are able to be used in a subsequent IPV process outside the context in which they were issued. Credentials might not contain any identity attributes and/or might not be linked to a source of identity information that is externally accessible.

The degree to which the credential has been bound to the entity and identity is also important. The IPV process covers the binding of the entity and the identity. The credential issuance process covers the binding of the credential, the identity and the entity. A credential that has not been sufficiently bound will reduce the number of IPV objectives it can meet. This will necessitate additional evidence to be used.

Where organisations using this standard intend to issue a credential for use by other IPV processes, a trust framework may be appropriate. A recommended approach to the creation and operation of a trust framework has been included in Annex B.

## 8 Requirements for Identity Proofing and Verification

This clause is divided into two parts. The first part covers requirements relating to the establishment of the IPV process and the second part to the conducting of the IPV process.

### 8.1 Establishment of the IPV process

Establishing an IPV process involves the setting up of an infrastructure to enable the IPV process to operate successfully. Establishment is done prior to the start of the IPV operations. The conduct of the operations should be reviewed periodically and changes made to the IPV process in accordance with the outcome of the reviews.

#### 8.1.1 Establish IPV context

The RA shall specify the context for which the IPV process will operate and the identities that will be proofed. This is needed in order to assess accurately identity-related risk, to assess the availability of identity evidence relevant to the context and to determine the identity evidence required for the IPV process. The purpose for which IPV is being performed should determine the information attributes (including identity information) that are to be provided by applicants.

The RA shall carry out an identity-related risk assessment and determine the LoA to be met by the IPV process. This assessment should be reviewed if there are any changes in the context or purpose for which IPV is being carried out. See ISO/IEC 29115:2013, clause 6.5 for more information on selecting the level of assurance.

#### 8.1.2 Governance

Where IPV processes are being implemented in a single organisation or enterprise, for use only within that organisation, there shall be a governance regime that ensures the identification and mitigation of the risks, the protection of identity information and the operation of the organisation's identity management regime.

Where the IPV process involves many organisations, for use across the community of organisations, there shall be a collaborative governance regime that ensures the identification and mitigation of the shared risks, the protection of identity information and the operation of the community's identity management regime.

Any federated model shall require a collaborative governance approach and agreed common policy.

IPV systems and services should be certified by a scheme approved by industry or government within the domain of operation.

#### 8.1.3 Legal framework

All actors in the IPV process shall understand and comply with any legal requirements incumbent on them in connection with operation and delivery of the service. This has implications including, but not limited to, the types of information that may be sought, how identity proofing is conducted, and what information may be retained. Handling of PII is a particular legal concern (see Annex B). Account should be taken of all jurisdictions within which actors operate. At LoA2 and higher, specific policy and contractual requirements should also be identified.

RAs shall set forth the terms under which enrolment is provided and under which the services associated with that enrolment shall be used. The terms of service associated with the enrolment may be established pursuant to a trust framework. Where appropriate, liability disclaimers or other legal provisions shall be accepted by, or on behalf of, the entity prior to continuation of the enrolment processes.

#### 8.1.4 IPV process design

The RA shall determine and/or approve the design of the IPV process. The IPV process shall include:

- Evidential requirements – the evidence that is to be provided in order to meet each objective at the required LoA. This should include an assessment of the LoA of sources and credentials to be accepted;
- Exception handling processes – processes that are to be followed in circumstances which normal procedures are unable to handle. This could include an inability to meet standard evidential requirements, apparent inconsistency between evidence and applicant and cultural or disability issues. Exception handling processes will usually entail interaction with the applicant in an attempt to resolve the problem. Resolution may involve the provision of alternative or additional evidence and processes. Failure to resolve problems may ultimately lead to the rejection of the application;
- Source availability – the selection of data sources against which identity credentials and/or information can be verified and the establishment of the legal framework under which they will operate;
- Service provider arrangements – the establishment of legal frameworks, training and other assurances covering service providers undertaking any part of the IPV process e.g., data source owners;
- Anti-collusion processes – processes (such as segregation of duties) and measures to prevent collusion by employees that results in the deliberate registration of false identity information;
- System requirements – the system components that will support the processes, including those listed above, to an adequate LoA.

A summary of identity-related threats and the requirements that cover the controls for each, is provided in Annex C.

#### 8.1.5 IPV policies

The RA shall ensure that policies exist to set explicit criteria for receiving, processing and recording applications. These policies should include (but are not limited to):

- The publication of a document which provides an overview of the identity information, sources, and/or issuers that are relied upon in support of the enrolment phase;
- Explicit guidelines for handling variations to the published documents;
- Privacy and protection of personally identifiable information. Additional information is provided in Annex B and ISO/IEC 29100 and 29101;
- Individual biometric characteristics (if captured) to be done in accordance with relevant standards such as ICAO 9303 and ISO/IEC 19794-X series standards and used for end-to-end authentication in accordance with ISO/IEC 24761 – ACBIO;
- Service level agreements with other RAs who are the sources of identity information being verified. These will include timeliness, quality etc.;
- Data storage, security and dissemination;
- Record-keeping.

These policies shall be published and should be made publicly available where relevant.

### 8.1.6 Information security management

At LoA2 and higher, IPV processes and actors shall have in place documented information security management practices, policies, approaches to risk management, and other appropriate measures, so as to provide assurance that effective practices are in place. For LoA3 and above, a formal information security management system shall be used for risk management and critical cyber controls implemented.

Depending on the agreements for legal, contractual, and technical compliance, actors should ensure that parties are abiding by commitments and may provide an avenue for redress in the event they are not. At LoA2, for PII, anti-collusion, cybersecurity, liability and other compliance reasons, this assurance should be supported by security audits, both internal and external, and the secure retention of records of significant events, including those audits.

An audit can be used by relying parties to check that parties' practices are in line with what has been agreed. The RA should establish a public policy for dispute resolution.

### 8.1.7 Continual monitoring and improvement of process

The RA shall employ effective measures to detect, respond and report instances of fraud, abuse or misuse. The continued monitoring of the IPV process ensures it remains fit for purpose, trusted and of high quality. The higher the LoA, and the degree to which the identity is being used by other Relying Parties, the greater the frequency shall be on which this monitoring will occur. Aspects to be monitored should include (but are not limited to):

- Fit for purpose. The identity attributes and the LoA achieved, continue to meet the requirements of the RA;
- Effectiveness. The IPV process is not resulting in fraudulent identities being registered;
- Timely. The IPV process is able to be completed within a timely manner (not impacting effectiveness), there are no bottlenecks in the process and the exception process is being used only as often as anticipated.

## 8.2 Conducting an IPV process

This clause applies to the performance of an IPV process on an individual application. Unless otherwise stated these requirements apply to all LoAs. However the rigour with which they are carried out will depend on the LoA to be met.

### 8.2.1 Receive the application

The RA shall begin the record-keeping on receipt of an application. A time stamp should be attached to the receipt of application for audit purposes and to enable service level agreements to be monitored.

The RA should check all received applications for completeness. Continuing the IPV process if information is incomplete or missing will cause delays, inefficiencies and potentially incorrect assessments. In remote applications this should be in the form of system edits on the field being completed.

Where physical evidence is supplied, the RA shall check the item for; connection to the applicant, validity, security features and evidence of tampering. For this purpose it shall only be acceptable for original evidence to be used. Expired documents do not necessarily mean the identity is no longer valid. Acceptance of expired documents shall require consultation with the issuing authority to determine the constraints that may apply.

Where an application involves the supplying of information rather than physical evidence the RA shall ensure that this information is able to be verified. For LoA 2 and above information shall be verified in the absence of physical evidence checks.

In a remote application the applicant should use an electronic credential to authenticate to an identity information source. This credential, its issuance process and the associated IPV process shall have met a LoA equal or higher than that of the current application. Refer to Leveraging previous IPV processes in clause 7.4.

### **8.2.2 Check the identity is unique**

The RA shall establish that the identity attributes to be registered will not result in a duplicate identity, within the context, by matching the attributes against those already registered. Multiple applicants claiming the same identity attributes shall require investigation and resolution before an application can proceed further.

Where a legitimate duplication occurs the RA shall assign an attribute, such as a unique identifier, to separate the identities. Where duplicates are occurring regularly the RA should consider increasing the number of identity attributes collected until uniqueness is achieved without reliance on an assigned attribute.

In addition, at LoA 3 and LoA 4, the RA should have processes to ensure an entity can claim one and only one identity in a given context.

### **8.2.3 Check the identity's existence and status**

For LoAs 2 and above, if the identity has never existed in an Authoritative source, the RA shall refuse the application.

As in most cases there will also be a requirement for an identity to relate to a living or active entity, this should be checked. In some contexts there are valid reasons for registering an entity after it no longer exists, for example a tax liability.

### **8.2.4 Perform identity entity binding**

For LoA 2 and above, the RA shall establish that the entity is bound to the identity. The verified existence of an identity does not mean that the applicant has ownership of the identity. I.e. the identity may have been stolen. This aspect is not explicitly mentioned in ISO/IEC 29115:2013 but is a required elaboration for Person entities to reduce the likelihood of stolen identities and impersonation.

### **8.2.5 Identity is used in other contexts**

For LoA 3 and above the RA should check that the entity has used their identity consistently and normally in other contexts. An entity typically has multiple identities established and used in different contexts. An identity that is not used in other contexts presents a higher likelihood it could be fraudulent.

### **8.2.6 Perform identity information verification**

Verification of the integrity of identity information collected:

- Need not occur at LoA 1;
- Should occur at LoA 2 and LoA 3; and
- Shall occur at LoA 4.

Identity information shall be verified against authoritative and/or collaborative sources according to the LoA being met. The RA shall make arrangement with authoritative and corroborative sources to ensure that responses to verification requests shall be timely and compliant with the agreed service level agreements and policies.

Care should be taken that even though it may appear to have integrity, some information may have expired thus, depending on the desired LoA, verification may also be required. In some situations, additional identity attributes may be required to improve the Level of Assurance. Such attributes shall also be verified.

### **8.2.7 Determination and registration**

The IPV process shall take as long as necessary to achieve the LoA required. Any short-cutting will weaken the identity and could result in a lower LoA. In this case the registration should not occur or, if the context allows, only be registered at the LoA that has been achieved. This will mean subsequent access to services and/or the issuance of a credential may not occur until further IPV can be undertaken to achieve the necessary LoA or the service may be granted with limitations applied.

### **8.2.8 Record-keeping**

The RA shall record all relevant information that supports the IPV process and the determination, to enable independent auditing of the IPV system operations and results by internal and external bodies, as required by relevant policies and legislation.

Secure record-keeping and recording are required to support the whole enrolment process. Enrolment requires the same standard of time stamping and record-keeping as the Credential Management Phase, described in ISO/IEC 29115:2013.



## 9 Person IPV

This clause provides specific requirements and additional guidance for IPV processes on Person entity types. It expands on the minimum requirements in clause 9.2 as they relate to Person entities.

### 9.1 Person identity attributes

Identity attributes are a subset of the personal information that the RA collects in order to provide services and/or credentials to entities. Attributes that are part of the IPV process are generally divided into three types as shown in Table 4.

Type	Explanation	Examples of Attributes
<b>Core</b>	Attributes that form a stable combined key to the identity in a context	Name or pseudonym (e.g. screen handle) Date of Birth Place of Birth
<b>Additional</b>	Additional attributes used to create or ascertain uniqueness of identity when core attributes are not unique within a context.	Gender A parent's name at their birth Biometric characteristic(s) Address(es) Phone number(s)
<b>IPV process</b>	Other attributes that are not required for providing uniqueness of identity but are often collected to support the IPV process.	Other names email address(es) Relevant information from evidence provided Attributes required to carry out verification with other sources

**Table 4 – Person identity attributes**

## 9.2 Person IPV minimum requirements

The following two tables outline the minimum requirements, by LoA, for meeting specific IPV controls. The IPV requirements get more stringent, the higher the LoA. The first table is focussed on a local IPV process, while the second covers remote.

Controls	Requirements by LoA for local IPV			
	LoA 1	LoA 2	LoA 3	LoA 4
<b>Identity is unique</b>	RA records shall be checked for duplicate	RA records shall be checked for duplicate	RA records shall be checked for duplicate <b>And</b> Entity should be matched against all other identities in the register using biometric recognition or equivalent	RA records shall be checked for duplicate <b>And</b> Entity should be matched against all other identities in the register using biometric recognition or equivalent
<b>Identity's existence</b>	No specific control	RA shall check the identity information from 1-2 pieces of evidence, that reflect an authoritative source	RA shall check the identity information from 1-2 pieces of evidence, that reflect an authoritative source <b>And</b> Identity information should be verified against an authoritative source e.g. birth register	RA shall check the identity information from 1-2 pieces of evidence, that reflect an authoritative source <b>And</b> Identity information shall be verified against an authoritative source e.g. birth register
<b>Identity's status</b>	No specific control	Business process for establishing Identity Entity binding	Business process for establishing Identity Entity binding <b>Or</b> Identity information should be verified against the Death Register	Business process for establishing Identity Entity binding <b>And</b> Identity information shall be verified against the Death Register
<b>Identity Entity binding</b>	No specific control	RA shall carry out in-person verification against a credential that contains a photographic image and matching identity attributes <b>Or</b> Verification by an identity referee	RA shall carry out in-person verification against a credential that contains a photographic image and matching identity attributes <b>Or</b> Biometric recognition where authorised access is available to an authoritative source containing the entity's biometric information <b>Or</b> Verification by an identity referee	RA shall carry out in-person verification against a credential that contains a photographic image and matching identity attributes <b>And</b> Biometric recognition where authorised access is available to an authoritative source containing the entity's biometric information

Controls	LoA 1	LoA 2	LoA 3	LoA 4
<b>Identity is used in other contexts</b>	No specific control	No specific control	RA shall check the identity information from at least 1 piece of evidence, that reflects a corroborative source <b>And</b> Identity information should be verified against corroborative sources <b>And</b> Contact information listed in evidence should be verified by using it to contact the entity	RA shall check the identity information from 1-2 pieces of evidence, that reflect a corroborative source <b>And</b> Identity information shall be verified against corroborative sources <b>And</b> Contact information listed in evidence shall be verified by using it to contact the entity

Table 5 – Requirements for local IPV

Remote identity proofing requires the use of a credential that has a combined strength of three aspects – the IPV process, the credential and the issuance process (as outlined in clause 7.4 Leveraging previous IPV processes); that is equal to or higher than the LoA required to be met.

	Requirements by LoA for remote IPV			
Controls	LoA 1	LoA 2	LoA 3	LoA 4
<b>Remote IPV</b>	Check against RA records for duplicate	Entity shall activate an assertion of an e-ID issued at LOA 3 or above <b>And</b> Check against RA records for duplicate	Entity shall activate an assertion of an e-ID issued at LOA 3 or above <b>And</b> Check against RA records for duplicate <b>And</b> Identity information should be verified against the Death Register	Entity shall activate an assertion of an e-ID issued at LOA 4 <b>And</b> Check against RA records for duplicate <b>And</b> Identity information shall be verified against the Death Register

Table 6 – Requirements for remote IPV

### 9.3 Person IPV additional guidance

This clause provides additional information which will aid in the design and operation of IPV processes for persons but should not be regarded as requirements.

#### 9.3.1 Evidence strength

There will be evidence (which includes national ID cards or e-IDs) issued at sufficient strength to allow them to fulfil the evidential requirements on their own. Only evidence meeting LoA 3 or above will meet this criteria or be suitable for remote use. As per the clause 7.4 Leveraging previous IPV processes, the strength will come from the three aspects of the credential. The original IPV process undertaken, the strength of the credential and the process used to issue it shall all be at the same LoA or higher.

While efforts should be made to use the highest quality of evidence for IPV processes, the number of evidence items required will depend on their ability to meet the controls – specifically Identity's existence, Identity Entity binding and Identity is used in other contexts.

Where multiple documents are required, additional strength can be achieved by drawing from the breadth and depth of the whole life of the individual.

### **9.3.2 Binding entities to identities**

Identity entity binding has to be performed for LoA 2 and above, for which there are many techniques.

Credentials containing biometric information (such as a facial image) may be compared with the entity in an in-person event. Where sufficient technology is available this can occur using such things as video linking.

If a source of identity information includes biometric information as an attribute, then it may be possible to collect the same type of biometric characteristic from the entity and compare it with the identity information source to establish binding. Implementation of biometric solutions should be done in conjunction with the relevant International Standards.

Where there are no attributes available for entity binding, alternative processes can be utilised, e.g. testimony by an identity referee who has known the subject for a specified period of time. Identity referees should come from groups (e.g. Registered Medical Practitioners, Police) recognised by the RA and with whom the RA is able to make independent contact.

## Annex A

(informative)

### Contra-indications and fraud detection

#### A.1 Physical evidence

Where physical evidence is used there will be Real and False items presented. Table A shows the categories of evidence and how each of the checks undertaken is designed to detect its use.

	Evidence			
	Real	Stolen/Sold	Tampered	Counterfeit/Fake
<b>Identity</b>	Real	Real	False	Real or False**
<b>Physical evidence checks</b>	Pass	Pass	Fail	Fail
<b>Bound to entity</b>	Pass	Fail	Pass	Pass
<b>Verification against issuing source</b>	Pass	Pass or Fail*	Fail	Pass or Fail** #
<b>Corroboration</b>	Pass	Likely to be weak	Likely to be weak	Likely to be weak

**Table A – Evidence checking outcomes**

\* Depends on whether the evidence has been reported missing

\*\* Counterfeit or fake evidence can contain real or false identity information. Real information could return a pass when verified.

# If a clone exists, then two versions of the same evidence are in circulation, one Real and one Fake. Verification against the issuing source will show a Pass until such time as the Fake is detected and action is taken. Cryptographically bound credentials can mitigate this risk.

The physical checking of evidence can include:

- 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, pretending to be a real document. Many items have security features that are almost impossible to fake but require expert skills or special machines to use. For example, automated ultraviolet ICAO checks of passports. Checks without such skills or machines are much more likely to fail to identify a fake item of evidence.

#### A.2 Verification

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

- Directly and completely contradicting key information, presented in the application or evidence; or
- Partially contradicting information presented in the application or evidence. This may be an indicator of keying errors or events such as name changes, which should be ruled out before treating as a potential fraud. The higher the LoA, the greater the risk and the requirement to halt the application, pending investigation
- 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.

### A.3 Biometric recognition

.Biometric characteristics can be matched 1:1 against a known source for Identity Entity binding, or in a 1:many (one-to-many) against all records in the register, to prevent multiple identities for a single entity.

Where cultural sensitivities make biometric capture and proofing difficult, alternative biometric or non-biometric options may be considered. However this is highly unusual. Most nations have successfully made arrangements to address cultural sensitivities and also captured necessary biometrics. Relying party and legal requirements can be such that cultural sensitivities may have to be compromised, if trust is to be achieved.

The important thing to note about the use of biometric recognition is that it does not provide as precise a response as other identity information verification processes. It is based on the probability of a match and therefore can result in false positives and negatives.

Biometric recognition cannot be used in isolation or in place of the verification of other identity information attributes. Any contra-indicator caused by a mismatch will be investigated by those experienced in biometric matching before referral for identity fraud investigation.

### A.4 Interviews

Interviewing is an important tool for fraud detection where evidence is in short supply or there are suspicions about the validity of the application.

To identify fraudulent applications, interviewers can:

- 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 RA, which is not in the documents e.g. previous address to the one currently listed in the passport, 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. E.g. the applicant provides a date of birth correctly (7 June 1990), later in the interview, discussing employment, the interviewer asks if the 9<sup>th</sup> is correct;
- 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 IPV process interviews may be witnessed or video recorded with clearly audible sound, using High Definition video format;
- 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 such as accents, disabilities etc.

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

- The person being interviewed may not normally be accompanied;
- Where translation is required (the RA 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 proxy or caregiver (the RA 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 this situation, the interview should be carried out in-person;
- Where cultural sensitivities exist, arrangements can be made for such needs as privacy, same-sex interviews and biometric capture;
- Where a minor (age 15 or less) is being interviewed, they may be accompanied by a parent or legal guardian;
- If the interview is done remotely:
  - There will be 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 could seek to subvert the interview. Where the risk is high, an in-person interview can 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 can refer the application for further investigation.

## Annex B

(informative)

### Trust Frameworks

This annex establishes recommendations for the creation and operation of Trust Frameworks and the provision of criteria against which RAs can be assessed. The development of Trust Frameworks offers the opportunity for widespread and consistent adoption of this IS (and others which define requirements for other aspects of Credential Management Services) in a way which can lead to mutual recognition between different frameworks adhering to the same reference standards. At the time of publication of this IS it is not considered appropriate to try to set explicit requirements in this area.

#### B.1 Trusted Framework Providers (TFPs)

Participating RAs should observe the following best practices as the basis on which their own operations can be recognised as providing value and assurance to the target communities, as well as a basis for comparison and ultimately mutual recognition between Trust Frameworks.

RAs should observe and apply the following best practices:

- a) establish and maintain policies governing and suited to the context and scope of operations;
- b) establish and maintain processes and procedures which support its policies and objectives;
- c) establish and maintain agreements which determine the obligations upon all parties participating under the framework<sup>2</sup>;
- d) publish their policies, processes, criteria, terms and conditions for participation and other key descriptive documents to, at least, the defined community of interest, and preferably in the public domain;
- e) take account of the interests of and seek representation and input from all interested parties, e.g. service providers, RPs, credential holders, organisational sponsors of credentialed entities, legislators and other national and local government offices;
- f) encourage adherence to the provisions of this and other related standards;
- g) operate and publish the results of an assurance scheme by which RAs and their services can be assessed for their conformity to the requirements of (at least) this IS (see B.2);
- h) manage a programme of internal governance and periodic review of administrative and technical functions of the framework, including technical and policy working groups;
- i) provide for oversight of framework members and their adherence to agreements and principles of the framework, with processes in place to handle any breach of same;
- j) be aware of and fit within the jurisdictional framework in which they operate (which may be multiple jurisdictions, which the framework should have some means of accommodating);
- k) align with any special interests of the community which it serves (e.g. a sector-specific focuses);
- l) publish a list of members of the framework, indicating their role and/or status. For RAs, indicate the nature and extent of their services and the Level(s) of Assurance at which they are provided;

---

<sup>2</sup> Such agreements should focus on how parties interact within the context of the Trust Framework but should not usurp their independent contractual relationships.



- m) manage an outreach and mutual recognition programme with other TFPs, both nationally and internationally, and through that strive to attain as much commonality of policy and practice as they can reasonably achieve, across all of the foregoing recommendations;
- n) where investment fees are expected for various forms of participation, these are clearly and unambiguously published.

## **B.2 Service Assurance Criteria**

In order to ensure that RAs providing services under the auspices of a Trust Framework are operating to equivalent or comparable practices and standards, the TFP should publish criteria against which RAs may be judged as to their conformance to best practice and the requirements expressed in this IS (see B.3). Such criteria, called Service Assurance Criteria, should:

- a) address the technical requirements stated in this IS, ensuring that the criteria can be associated with discrete functions which might be operated as separate services;
- b) address business and other administrative and operational criteria to ensure that a Credential Service is being operated on sound practices;
- c) in fulfilling a) and b) above, define clear and measurable minimum (baseline) criteria for each LoA, such that, for any given LoA and service scope, any service would have to fulfil the same minima;
- d) not restrict RAs from being able to tailor their services to accommodate specific jurisdictions and technologies;
- e) be suitable for use as reference criteria against which an assessment to determine a service's conformity could be conducted.

## **B.3 Determining Conformity**

One strength of a Trust Framework is its ability to set criteria against which services can be assessed and to then define and operate an assessment regime which delivers assurance as to the conformity of a service. I.e. that, for its defined scope and LoA, a service meets or exceeds the applicable criteria. To accomplish this, TFPs should establish an assessment programme which:

- a) defines the requirements for those organisations and individuals wishing to perform assessments (against the criteria);
- b) determines the conformance of applicant assessors against those criteria and awards accreditation to those which meet them;
- c) establishes rules and conditions under which assessments of services shall be performed;
- d) formalises and publishes the determination of both assessor accreditation and service approval.

To assist with RAs finding suitable assessors, and RPs and others in finding approved services (and observing B.1 k), the TFP should publish a status list indicating which services, providers and assessors have achieved a formalised status within the Trust Framework.

**Annex C**

(informative)

**Summary of Threats**

The following table outlines the high level threats to IPV processes and the controls for each. The controls are expressed as one or more of the requirements specified in this Standard. Requirements include the general requirements (clause 8) and entity specific requirements for each LOA (clause 9).

<b>Threat</b>	<b>Requirement providing control</b>
IPV process not trusted	Governance Legal framework IPV policies
Identity information is not protected	Legal framework IPV policies Information security management
IPV process is not consistent	IPV Policies IPV process design Check for completeness
Identity is not fit for purpose	Establish IPV context LoA determination Continual monitoring and improvement of process
Identity information is of poor quality	LoA determination IPV process design Determination and registration Continual monitoring and improvement of process
Identity is false	Check the identity's existence and status Check the entity uses the identity in other contexts Perform identity information verification
Identity is stolen	Perform identity entity binding Perform identity information verification
Identity is duplicated	Check for completeness Check the identity is unique
Collusion	IPV policies Continual monitoring and improvement of process Information security management

**Table C.1 – Threats and requirements**

## Bibliography

This bibliography provides a listing of non-normative references used in the development of this International Standard.

- [1] The National e-Authentication Framework  
<http://www.finance.gov.au/policy-guides-procurement/authentication-and-identity-management/national-e-authentication-framework/>
- [2] Australian Government Gatekeeper Public Key Infrastructure  
<http://www.gatekeeper.gov.au/>
- [3] New Zealand Standard: *Evidence of Identity (EOI)* December 2009  
[http://www.dia.govt.nz/diawebsite.nsf/wpg\\_URL/Resource-material-Evidence-of-Identity-Standard-Index?OpenDocument](http://www.dia.govt.nz/diawebsite.nsf/wpg_URL/Resource-material-Evidence-of-Identity-Standard-Index?OpenDocument)
- [4] OMB M-04-04, *e-Authentication Guidance for Federal Organization*  
<http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>
- [5] 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/271266/GPG\\_45\\_Identity\\_proofing\\_and\\_verification\\_of\\_an\\_individual\\_-\\_issue\\_2.2\\_December\\_2013.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/271266/GPG_45_Identity_proofing_and_verification_of_an_individual_-_issue_2.2_December_2013.pdf)
- [6] ITU-T Focus Group on Identity Management Report 5 Report on Requirements for Global Interoperable Identity Management  
<http://www.itu.int/ITU-T/studygroups/com17/fgidm/>
- [7] ITU-T Focus Group: Report on Identity Management Report 6 Framework for Global Interoperability  
<http://www.itu.int/ITU-T/studygroups/com17/fgidm/>
- [8] ITU-T Report on the Definition of the Term “Identity”, April, 2008  
<http://www.itu.int/ITU-T/jca/idm/>
- [9] Kantara Initiative Identity Assurance Framework v3.0  
<https://kantarainitiative.org/confluence/display/GI/Identity+Assurance+Framework>
- [10] NIST Special Pub 800-36 Guide to Selecting Information Technology Security Products, October 2003,  
<http://csrc.nist.gov/publications/nistpubs/800-36/NIST-SP800-36.pdf>
- [11] NIST Special Pub 800-63 Electronic Authentication Guideline Version 1.0.2, April 2006  
[http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1\\_0\\_2.pdf](http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf)
- [12] “OECD Recommendation for Electronic Authentication and OECD Guidelines for Electronic Authentication”  
<http://www.oecd.org/dataoecd/32/45/38921342.pdf>
- [13] Principles for Electronic Authentication: A Canadian Framework  
[http://strategis.ic.gc.ca/epic/site/ecic-ceac.nsf/en/h\\_gv00240e.html](http://strategis.ic.gc.ca/epic/site/ecic-ceac.nsf/en/h_gv00240e.html)
- [14] B. VAN ALSENOY and D. DE COCK, ‘Due processing of personal data in eGovernment? A Case Study of the Belgian electronic identity card’, *Datenschutz und Datensicherheit*, March 2008, p. 180.
- [15] ENISA, Mapping (Interoperable Delivery of European e-government services to public Administrations, Businesses and Citizens) IDABC Authentication Assurance Levels to SAML v2.0.
- [16] ITU-T Recommendation X.1252 (2010) Baseline identity management terms and definitions.
- [17] ITU-T Recommendation Y.2720 (2010), Next generation network identity management framework.
- [18] ITU-T Recommendation Y.2721 (2010) NGN identity management requirements and use cases.
- [19] ITU-T Recommendation Y.2722 (2010) NGN identity management mechanisms.
- [20] ISO/IEC 9798:2010, Information technology – Security techniques – Entity authentication.
- [21] ISO/IEC 19792:2009, Information technology – Security techniques – Security evaluation of biometrics.

[22] ISO/IEC 24760-1:2011, Information technology -- Security techniques -- A framework for identity management -- Part 1: Terminology and concepts

[23] ISO/IEC 27001:2005, Information technology -- Security techniques -- Information security management system.

[24] ISO/IEC 29100:2011, Information technology -- Security techniques -- Privacy framework.

[25] ISO/IEC 29101, Information technology -- Security techniques -- Privacy architecture framework.

[26] ISO/IEC 29115:2013 - , Information technology -- Security techniques -- Entity Authentication Assurance Framework (EAAF).