ISO/IEC JTC 1/SC 27 N12538

ISO/IEC JTC 1/SC 27/WG 5 N512538

REPLACES: N11746

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE: Working Draft text

TITLE: **Text for ISO/IEC 2nd WD 29003 -- Information technology – Security techniques – Identity proofing**

SOURCE: Project Co-editors: Patrick Curry (UK), Anthony Nadalin (US)

DATE: 2013-07-15

PROJECT: **29003 (1.27.103)**

STATUS: **In accordance with resolution 2 (contained in SC 27 N12555) of the 15th SC 27/WG 5 Plenary meeting held in Sophia Antipolis, France, 22nd – 26th April 2013 this document is circulated for study and comment.**

National Bodies, experts and liaison organizations of SC 27/WG 5 are requested to send their comments / contributions on the above-mentioned document by 2013-09-15.

PLEASE submit your comments / contributions on the herby 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: **2013-09-15**

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 + 58

Secretariat ISO/IEC JTC 1/SC 27 - DIN Deutsches Institut für Normung e. V., Burggrafenstr. 6, 10772 Berlin, Germany, Telephone: + 49 30 2601-2652; Facsimile:+ 49 30 2601-1723; e-mail: krystna.passia@din.de
HTTP://www.jtc1sc27.din.de/en

ISO

International Organization for Standardization

IEC

International Electrotechnical Commission

International Standard ISO/IEC WD2 29003

Information technology — Security techniques — Identity Proofing

[Editorial Note: the title is misleading and does not reflect the definitions in this document. A title change to "Identity Proofing & Verification of Persons, Organisations, Devices and Software" is being proposed]

CONTENTS

Forward

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.

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

Existing and emerging ISO standards 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 Identity Proofing and Verification (IPV) processes for which no reference standards exist. An ISO standard for IPV is required to which other identity management standards can refer, based on the four Levels of Assurance described in ISO/IEC 29115 or other similar standards. 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, which are being made worse by the proliferation of untrusted mobile devices, Internet of Things, Internet Protocol Version 6 and the additional trust requirements of cloud services.

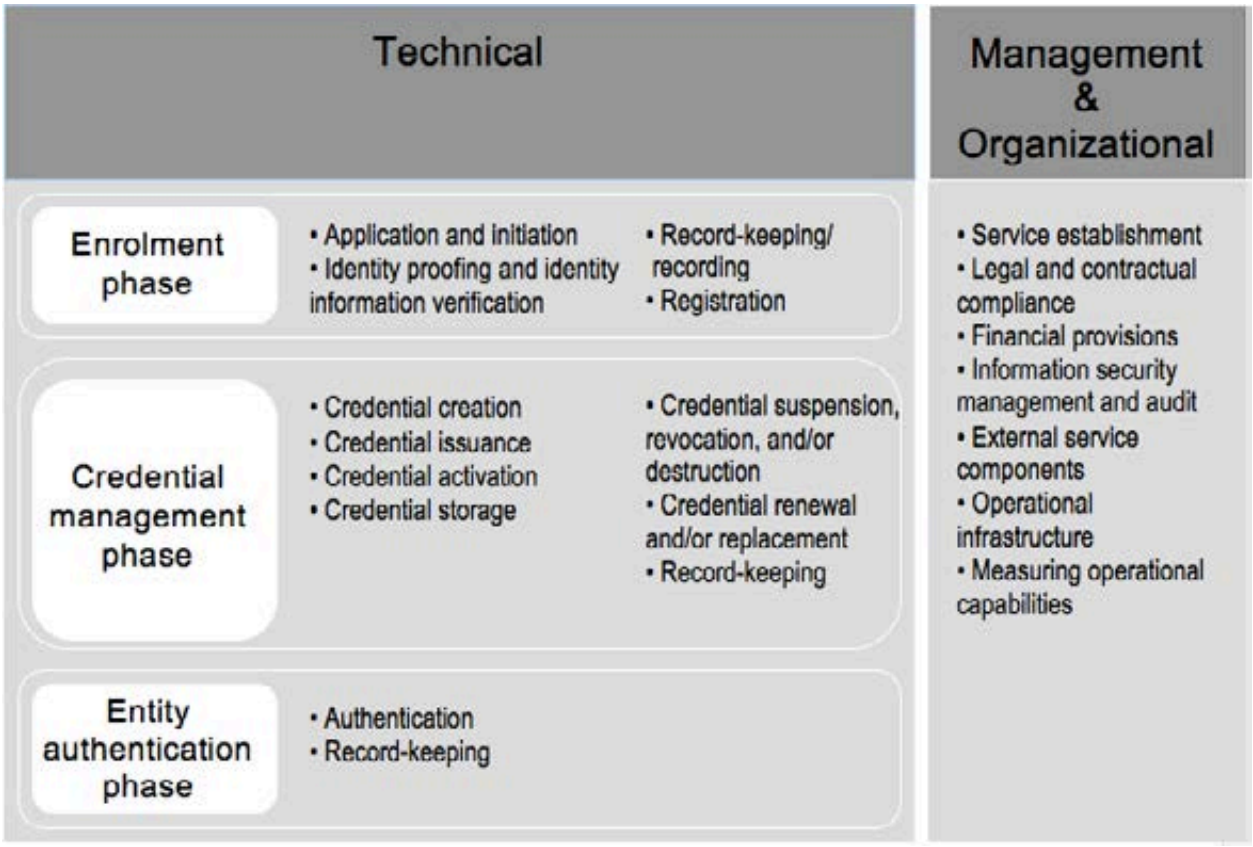

Figure 1 - Overview of the Entity Authentication Assurance Framework

This International Standard is intended to be used principally by Identity Proofing and Verification Service Providers (IPVSP) 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 the Entity Authentication Assurance Framework (EAAF) described in ISO/IEC 29115 and outlined in Figure 1.

Relevant Documents to be Considered

ISO/IEC 29115, Entity Authentication Assurance Framework.

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

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

US ANSI Identity Verification Standard

The Financial Action Task Force - The Forty Recommendations - www.oecd.org/newsroom/2789371.pdf.

Liaison Organisations

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

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 <29003>

Information technology — Security techniques — Identity proofing

1 Scope

This International Standard (IS) provides best practices and guidance on required processes for initial establishment and subsequent confirmation of an entity's identity for parties using or expecting to use ITU-T X.1254, ISO/IEC IS 29115 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 delivery of a service to that entity, by or for that entity.

In scope:

- The development of identity proofing and verification (IPV) processes to be used as a national body standard in support of enrolment of entities. Definitions are provided for IPV principles, risk assessment, and controls sufficient to meet the requirements of ISO identity management standards for entities, notably ITU-T X.1254 l ISO/IEC IS 29115. These controls shall take account of threats, counter-fraud requirements and best practice guidance described by national policy specifications from government organisations.
- Entities that require to be authenticated in accordance with ISO standards, for which they need to be enroled:
    - Persons, particularly citizens, consumers, government employees and industry employees.
    - 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.
    - Software applications. May also include network and application protocols such as SSL/TLS and VPN, which employ trust-based models using certificates, etc.
    - Organisations. For the purposes of trust, all persons, devices and software have a relationship with one or more organisations for reasons of ownership, issuance and management. Each organisation must be trustworthy to the same Level of Assurance as any credentials being issued or asserted, or higher.
- A resulting International Standard that is sufficient for:
    - Nations and industry to have confidence in using them
    - Nations and industry to have confidence in the results of each others' national IPV systems and the credentials
    - Certification bodies to develop assessment and audit criteria against which certified auditors can successfully conduct Trusted Third Party (TTP) audit and assurance of IPV service providers.

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 IS 29115: Information technology — Security techniques — Entity Authentication Framework

2.1 Identical International Standards

None.

2.2 Paired International Standards

None.

2.3 Additional references

3 Definitions

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

3.1

Accountable Person

The single person who is accountable for the provision and maintenance of information associated with an organisation to any authority.

NOTE 1 – All organisations shall have an accountable person.

NOTE 2 – The Accountable Person shall have a credential compliant with this International Standard and ISO/IEC 29115. That credential shall be at the same LoA, or higher, as the organisation's LoA.

3.2

Application

A process where an entity applies to be identity proofed

NOTE 1 It usually is the first step in the enrolment process.

NOTE 2 It usually is based on the documents provided to support the application.

3.3

Applicant

The person making the application, who is either:

- the subject of the application or
- is acting on behalf of the subject and is already registered at the same LoA.

NOTE - If the person who is not the entity is an employee acting on behalf of an organisation, then both the person and the organisation shall be trustworthy to the same LoA or higher LoA.

3.4

Assertion

Statement made by an entity without accompanying evidence of its validity.

[ITU-T X.1252]

NOTE - The meaning of the terms claim and assertion are generally agreed to be somewhat similar but with slightly different meanings. For the purposes of this International Standard, an assertion is considered to be a stronger statement than a claim.

3.5

Authentication

A process used to achieve sufficient confidence in the binding between the entity and the presented identity.

[ITU-T X.1252]

3.6

Authentication Factor

Piece of information and/or process used to authenticate or verify the identity of an entity.

[ISO/IEC 19790]

NOTE - Authentication factors are divided into four categories:

- something an entity has (e.g., device signature, passport, hardware device containing a credential, private key);
- something an entity knows (e.g., password, PIN);
- something an entity is (e.g., biometric characteristic); or
- something an entity typically does (e.g., behaviour pattern).

3.7

Authentication Protocol

Defined sequence of messages between an entity and a verifier that enables the verifier to perform authentication of an entity.

3.8

Authoritative Source

Repository which is recognized as being an accurate and up-to-date source of information.

3.9

Biographical footprint

The trail of information recorded in information systems as a result of normal social, living and employment activities during a person's lifetime. This trail of information can be used to evidence a person's link to a claimed identity.

3.10

Certification Bodies

Organisations approved by government or pan-industry authorities to assess the capabilities and competencies of an auditing company and their auditors, and to certify the company to audit the compliance of a trust service provider.

3.11

Claim

Statement that something is the case, without being able to give proof.

[ITU-T X.1252]

NOTE - The meaning of the terms claim and assertion are generally agreed to be somewhat similar but with slightly different meanings. For the purposes of this International Standard, an assertion is considered to be a stronger statement than a claim.

3.12

Confidence Score

A percentage score of the confidence about the subject's identity, which is generated by the IPV SP during the IPV process.

NOTE 1 – The higher the score, the higher the confidence.

NOTE 2 – Successful registration at a specific LoA depends on achieving an adequate confidence score.

NOTE 3 – Some IPV SPs use the term 'risk score', but not always consistently.

3.13

Context

Environment with defined boundary conditions in which entities exist and interact.

[ITU-T X.1252]

3.14

Contra-indicators

Results of IPV processes that contradict each other to the extent that one or more of the results are incorrect and further investigation is required to establish the truth.

3.15

Credential

Set of data presented as evidence of a claimed or asserted identity and/or entitlements.

NOTE – See Annex XX for additional characteristics of a credential.

3.16

Credential Service Provider

Trusted actor that issues and/or manages credentials.

3.17

Data Service Providers

A registered provider of analysed data and information services, based on identity-specific, pseudonymised or anonymised data, for specific business purposes through to bulk data for statistical purposes and trend analysis.

3.18

Enrolment

The process from initial application for a credential through several identity proofing and identity verification checks that, if successful, result in entry into an identity Register for the purpose of issuing a credential that is bound to the entity and its identity.

3.19

Entity

Something that has separate and distinct existence and that can be identified in a context.

[ITU-T X.1252]

NOTE – For the purposes of this International Standard, entity is also used in the specific case for something that is claiming an identity.

3.20

Entity Authentication Assurance

Degree of confidence reached in the authentication process that the entity is what it is, or is expected to be.

[ITU-T X.1252]

3.21

Evidence of Identity

The types of evidence that, when combined, provide confidence that an individual is who they say they are.

3.22

Identifier

One or more attributes that uniquely characterize an entity in a specific context.

[ISO/IEC 29115]

3.23

Identity

A representation of an entity in the form of one or more attributes that allow the entity or entities to be sufficiently distinguished within a context.

NOTE – For identity management (IdM) purposes, the term identity is understood as contextual identity (subset of attributes), i.e., the variety of attributes is limited by a framework with defined boundary conditions (the context) in which the entity exists and interacts.

[ITU-T X.1252]

3.24

Identity Entity Binding

Process of checking by a verifier that the identity is bound to the entity to a desired degree of confidence

3.25

Identity Information Verification

Part of the Enrolment Process. Process of checking the authenticity, validity, integrity, correctness and binding of the identity by using data from many sources, including the biographical, sociological and biometric footprints, to corroborate the application and statements made by the applicant or their proxy, thus to identify a fraudulent application or to establish a confidence score.

NOTE 1 - It does not involve interaction with the applicant;

NOTE 2 - Identity Proofing will have already begun or been completed;

NOTE 3 - The confidence score determines the resulting Level of Assurance.

3.26

Identity Proofing

Part of the Enrolment Process. Identity proofing is the process of capturing and verifying sufficient information to identify an entity in the application to a specified or understood LoA, and that the result is fit for purpose.

NOTE – It involves:

- interaction with the applicant, the subject (remotely or in person) and their application;

- physically checking the application and supporting evidence and documents, to detect possible fraud, tampering or counterfeiting

- validating each document or evidence with the issuing authority, or systemically authenticating a credential with the issuing authority (i.e. where the credential interacts cryptographically with issuing authority), where possible;

- checking that the information in the documents and the application with the subject, either remotely or in person according to the Level of Assurance, to be confident that the entity has the claimed identity.

3.27

Identity Proofing and Verification Service Provider (IPVSP)

A service provider who carries out identity proofing and/or identity information verification.

NOTE 1 - The Registration Authority normally relies upon the IPVSP for these services.

NOTE 2 – The IPVSP is not normally the Registration Authority and does not normally hold or maintain the register.

3.28

Identity Provider

A service provider who stores identity profiles for use by the identity owner to provide assertions for authentication based on a security token, to relying parties.

3.29

Legal Entity Identifier

A global legal entity identifier for parties to financial transactions in financial markets, endorsed by the G20.

Man-in-the-middle Attack

Attack in which an attacker is able to read, insert, and modify messages between two parties without their knowledge.

3.30

Mobile Trusted Module

A Mobile Trusted Module (also known as Trusted Platform Module Mobile) is conceptually a Trusted Platform Module (Version 1.2 or higher) as defined by the Trusted Computing Group, optimised for use in a mobile environment.

3.31

Multifactor Authentication

Authentication with at least two independent authentication factors.

[ISO/IEC 19790]

3.32

Multitype Authentication

Authentication with at least two different types of authentication factor, including:

- Something you are

- Something you have
- Something you know
- Something about your behaviour

3.33

Mutual Authentication

Authentication of identities of entities which provides both entities with assurance of each other's identity.

3.34

Non-repudiation

Ability to protect against denial by one of the entities involved in an action of having participated in all or part of the action [X.1252].

3.35

Registration

Process whereby, having successfully completed the IPV process, the entity's identity data is recorded in an authoritative register, also known as a Source of Authority or Authoritative Source.

3.36

Registration Authority

Trusted actor that establishes and/or vouches for the identity of an entity to a CSP.

3.37

Relying Party

Actor that relies on an identity assertion or claim.

3.38

Repudiation

Denial in having participated in all or part of an action by one of the entities involved [X.1252].

3.39

Responsible Person

The persons who are required by law or regulation to exercise responsibility and oversight for management and oversight of an organisation, and who are responsible for the governance to ensure regulatory compliance.

NOTE 1 – All organisations shall have a one or more responsible persons.

NOTE 2 – All responsible persons shall have a credential compliant with this International Standard and ISO/IEC 29115. That credential shall be at the same LoA, or higher, as the organisation's LoA.

3.40

Salt

Non-secret, often random, value that is used in a hashing process.

NOTE - It is also referred to as sand.

3.41

Secure Content Automation Protocol

A suite of specifications that standardise the format and nomenclature by which security software products communicate software flaw and security configuration information.

[NIST SP800-126]

3.42

Shared Secret

Secret used in authentication that is known only to the entity and the verifier.

3.43

Source of Authority

An Authoritative Source, register or database of entities' identity attributes that have been subject to certification to a specified Level of Assurance, sufficient for other parties to rely upon the registered data for an entity and establish a trust relationship with that entity.

3.44

Subject

The entity contained in the application, whose identity is being examined and, if successful, registered.

3.45

Time Stamp

Reliable time variant parameter which denotes a point in time with respect to a common reference.

3.46

Transaction

Discrete event between an entity and service provider that supports a business or programmatic purpose.

3.47

Trust Framework

Set of requirements and enforcement mechanisms for parties exchanging identity information.

3.48

Trust Functions

Functions that establish and enhance trust in an information-centric, electronic relationship between two or more parties. For example, authentication, digital signatures, identity-linked encryption, secure email and logical and physical access control.

3.49

Trusted Platform Module

A secure cryptographic module fixed to a motherboard that stores keys, passwords and digital certificates, and can carry out secure functions of measurement, device authentication, signing and key generation.

NOTE 1 – TPM is a leading architectural and technological standard, published by the Trusted Computing Group, that is becoming the practical standard for device authentication.

3.50

Trusted Third Party

Authority or its agent, trusted by other actors with respect to specified activities (e.g. security-related activities).

NOTE - A trusted third party is trusted by an entity and/or a verifier for the purposes of authentication.

3.51

Trustworthy

The ability for an entity to be trusted at a given Level of Assurance (LoA) having been enrolled and successfully registered by Source of Authority, and then for the entity to use a credential to authenticate at that LoA.

3.52

Unique Property Reference Number

Nationally unique identifier for a building or part of a building that has an address or requires to be identified for legal, government and business purposes, including the provision of utilities and for elections.

3.53

Validation

The checking of a document, credential or attribute with the issuer or Source of Authority to ensure it is valid, based on the most current information available.

NOTE 1 - Validation can occur during **Identity Proofing, Identity Information Verification** and **Verification.**

NOTE 2 – Online, systemic validation of a credential (e.g. smartcard, token, mobile phone, biometric) provides for higher assurance than offline validation (e.g. phone call, black list lookup)

3.54

Validity Period

Time period during which an identity or credential may be used in one or more transactions.

3.55

Verification

Process of checking information by comparing the provided information with previously corroborated information.

3.56

Verifier

Actor that corroborates identity information.

NOTE – The verifier can participate in multiple phases of the EAAF and can perform credential verification and/or identity information verification.

3.57

Vetting

The separate process of verifying additional attributes to be associated with a registered entity's identity for the purposes of determining the suitability of an entity for a role or employment, and then allocating permissions or access rights.

NOTE 1 – Vetting is outside the scope of this International Standard, but defined for clarity.

NOTE 2 – Vetting is to enable authorisation. IPV is to enable authentication.

4 Abbreviations

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

AAS	Archive Attribute Set
ACA	Attestation Certificate Authority
AIK	Attestation Identity Key
AML	Anti-Money Laundering Legislation
CA	Certificate Authority
CAA	Certified Attribute Authority
CAS	Current Attribute Set
CSP	Credential Service Provider
DSP	Data Service Provider
EAA	Entity Authentication Assurance
EAAF	Entity Authentication Assurance Framework
EoI	Evidence of Identity
EK	Endorsement Key
IAS	Initial Attribute Set
IdM	Identity Management
ICT	Information and Communications Technology
IDP	Identity Provider
IEC	International Electrotechnical Commission
IMEI	International Mobile Equipment Identity
IP	Internet Protocol
IPV	Identity Proofing and Verification
IPVSP	Identity Proofing and Verification Service Provider
IS	International Standard
ISO	International Standards Organisation
ITU-T	Telecommunication Standardization Sector for the International Telecommunications Union
KYC	Know Your Customer
LoA	Level of Assurance
LEI	Legal Entity Identifier
MAC	Media Access Control
MTM	Mobile Trusted Module
NFIQ	NIST Fingerprint Image Quality
NPE	Non-Person Entity
PCI DSS	Payment Card Industry Data Security Standard
PII	Personally Identifiable Information
PIN	Personal Identification Number
RA	Registration Authority
RP	Relying Party
SAML	Security Assertion Markup Language
SCAP	Security Content Automation Protocol
SSL	Secure Sockets Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
TCG	Trusted Computing Group
TPM	Trusted Platform Module
TTP	Trusted Third Party

UPRN	Unique Property Reference Number
URL	Uniform Resource Locator
VAT	Value Added Tax

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 and Verification Context

To implement IPV requires an understanding of its functions, and how they relate to usage and trust. This context for IPV includes:

- The IPV Model
- The Entity and Credential Lifecycles
- The Four Contexts of Identity
- Levels of Assurance (LoA)
- LoA Requirements for IPV
- Actors
- Requirements for IPV Systems and Services

6.1 Identity Proofing and Verification Model

The IPVSP shall follow the following steps for IPV to attain the desired Level of Assurance:

1. Policy acceptance
2. Check for sufficient information quality in the application
3. Check that the entity exists and is living
4. Check that the identity is fit for purpose
5. Perform Identity verification
6. Perform Identity entity binding
7. Check that the entity uses or used their identity in the community
8. Perform risk analysis to produce a Confidence Score
9. Register
10. Perform continuous monitoring

Figure 2 – IPV Model, shows the components in the Identity Proofing Verification model as part of the Enrolment Process.

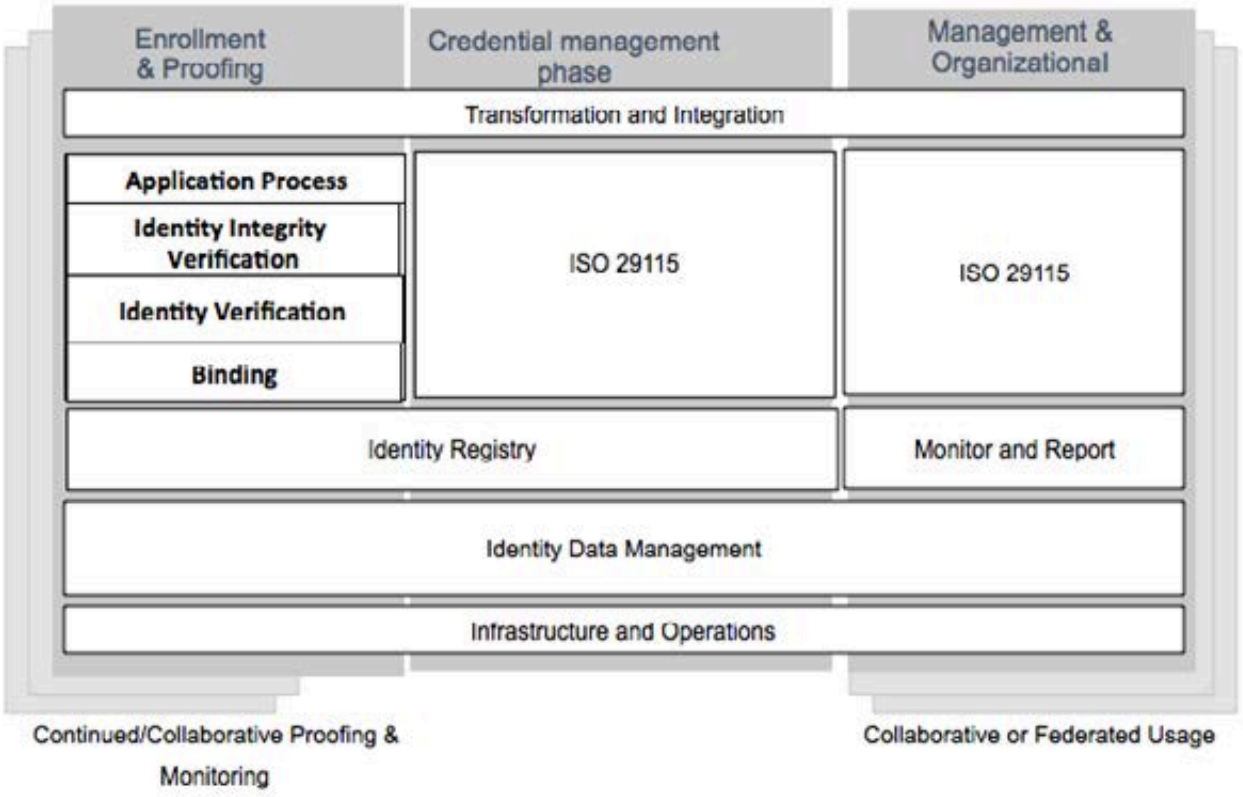

Figure 2 - IPV Model

6.1.1 Policy Acceptance

One or more policies must exist that set explicit criteria, according to this International Standard, for receiving and processing applications for entities. These policies should include explicit guidelines for handling variations within Evidence of Identity, which arise from national circumstances. These policies must be published and available.

6.1.2 Application Quality Check

Determine the required LoA.

Checks are made on the application and supporting Evidence of Identity (EoI) to ensure it is has sufficient information quality to be processed at the required LoA.

6.1.3 Check the entity exists and is living

The entity exists or has existed at a point of time for the Enrolment Process to be valid. IPV of a non-existent entity is out of scope of this document. Existence must include checking against:

- A birth register or manufacturer's production record using serial number, etc to ensure that the entity does exist or has existed.
- A death register or the destruction register for a non-person entity (NPE), to determine whether the entity is still alive.

If the entity does not exist or has not existed, the application is refused. There may be a requirement to register posthumous entities - the entity did exist but was never registered.

6.1.4 Check the identity is fit for purpose

IPV is done for a specific purpose, such as providing an electronic credential to an employee, opening a bank account, etc. For each purpose, the attributes in the identity which is being proofed could be different. For example, to provide an electronic credential to an employee, having the combination of name and date of

birth as the identity to be proofed is not sufficient. It also needs to have the attribute attesting that the entity is an employee of the corporation.

These additional attributes, necessary to ensure the IPV result is fit for purpose, shall also included in the application's supporting EoI.

6.1.5 Perform identity information verification

The verifier shall verify the integrity of the EoI collected. Even though it may appear to have integrity, some information may have expired. In some situations, additional identity attributes may require verification to improve the Confidence Score. Where the subject is a person and the applicant is unable to produce sufficient documentary EoI (e.g. refugees), it may be necessary to interview people from the subject's community and life history to gather sufficient references to achieve the Level of Assurance. In such situations, the risks associated with different verification processes and additional checks in some countries, shall be taken into account.

Note that it may not always be possible to perform the identity verification, as the source of the identity may not provide enough quality information, or it is inaccessible in a timely manner.

6.1.6 Perform identity entity binding

The fact that identity is accurate does not mean it is bound to the subject. The identity shall be bound to the subject.

Identity entity binding has to be performed, for which there are many techniques. For example, if the identity includes biometric data as an attribute, then the subject's biometric data and that of the identity should be corroborated to establish the binding. On the other hand, if there are no attributes available for entity binding, an external source may have to be utilized, e.g. testimony by a trusted referee who knew the subject for a specified period of time.

It is important to check that the subject is the sole claimant of the identity. Multiple claimants constitute a contra-indicator, which would require investigation and resolution before an application could proceed further.

6.1.7 Check that the entity uses or used the identity in the community

An entity typically has multiple identities in different contexts. The applicant may use them for fraudulent purposes. An identity that is not used in the community presents a high risk. The verifier should check that the subject's identity is used consistently and normally by the subject in the community.

6.1.8 Perform risk analysis

Each of the sources for the document and pieces of information for the EoI are subject to risks of error, negligence, collusion and more. A risk analysis of the sources and of the IPV processes of the IPVSP shall be undertaken. The IPVSP shall establish appropriate procedures for risk management and mitigation, and their effective implementation. They should include proper management oversight, systems and controls, segregation of duties, training and other assurance. Responsibility should be explicitly allocated for ensuring that policies and procedures are implemented effectively.

6.1.9 Registration Decision

If there are no unresolved contra-indicators, the previous steps may result in a Confidence Score sufficient for the application to be approved at the required LoA and the subject's identity will be recorded in the Authoritative Source's register.

6.1.10 Perform continuous monitoring

On-going monitoring is an essential element of effective IPV procedures. The IPV status of the identity will continue to be monitored after registration to identify any changes that could impact the IPV associated with the identity and the binding to the entity for the assigned LoA. Such changes include:

- Attributes. Changes in key attributes at registration should be updated in the e.g. name, date of birth, place of birth, gender, address and date of marriage. Similarly for NPEs.

- Biometrics. Biometrics should be updated whenever their accuracy is questionable and 1:1 matching for authentication becomes difficult. This should normally be done at least once every 10 years.
- Behaviour. Any changes in the normal and regular pattern of activity of the entity and the use of their credential for authentication may indicate a significant change in behaviour and the introduction of new risks. They may also help to identifying fraudulent transactions, particularly if the identity or the credential has been stolen or subverted.
- Contra-indicators. New contra-indicators may emerge that could require immediate revocation of credentials and investigation of the entity and its identity.

6.2 Entity and Credential Lifecycles

This clause is to clarify that the characteristics of entity and credential lifecycles. Every entity has an identity and an entity lifecycle. During an entity's lifecycle, it can have one or more credentials to assert its identity. Each credential has a credential lifecycle.

6.2.1 Entity Lifecycle

Person and Non-Person Entity (NPE) lifecycles:

- Differ in two major ways; person entity lifecycles are more complicated and they are the subject of much more legislation and regulation.
- Cannot be suspended. An entity's identity is created at birth, is used during its life and ceases to be used for IPV purposes after death or revocation.

In most societies, a person's entity lifecycle comprises eight major events or time periods, which contribute to the person's biographical footprint:

- Pre-Birth. A period when medical organisations may assign a temporary identity to a foetus for medical purposes.
- Birth. The event when a baby is born and exits the mother's body.
- Registration. An event where the birth is registered by a trusted authority with the date, location, authority, child's name(s) and names of the parents. A validated birth certificate is an authoritative document for IPV.
- Pre-education. A period during which a child is with, and dependent upon, its parent(s) or guardian(s), prior to education. The parents or guardians usually act as a proxy for the child for the purposes of trust, and the biographic footprint is linked to the parent.
- Education. A period when a person's primary interaction is with educational authorities. A person's educational activities contributes to their biographic footprint. This period can occur more than once.
- Employment. A period when a person's primary interactions are with and on behalf of an employer. The biographic footprint results from employment activities. During periods of unemployment, this footprint largely disappears to leave only evidence of government (or other) benefit payments. Employment is the period of greatest financial and consumer activity, contributing to the biographic footprint. This is also the period when the greatest number of credentials are bound to a person's identity. Employment documents can be an authoritative document for IPV. This period can occur more than once.
- Marriage. An event and a period of time when two persons' identities are formally linked and whose biographic footprints normally have a high degree of commonality, which gives greater confidence for IPV to authorities and relying parties. A validated marriage certificate is an authoritative document for IPV. Marriage can occur more than once.

- Retirement. The period between employment and death. The biographical footprint tends to be similar to unemployed persons, except that a retired person normally has more financial activity and possessions, which also inform their biographical footprint. Retirement can occur more than once.
- Death. An event that is recorded by an authority with the date, location, authority, person's name(s) and cause of death, which is usually witnessed by an authorised person e.g. doctor. A validated death certificate is an authoritative document for IPV. There is no change to the biographical footprint after death. No IPV events occur after death.
- Post death. Executors of the deceased's estate act as a proxy for the deceased. The requirement to protect Personally Identifiable Information (PII) and privacy data persists after death to prevent misuse of a deceased's identity for fraud and also violence against living relatives (e.g. witness protection or police informer's family).

An organisation's lifecycle has four events or time periods:

- Creation. An organisation is created when it is registered by an authority with the date, location, authority, directors' names and details. Under UNCITRAL rules, all nations operate registers for companies conducting commercial business, however this International Standard extends to include all kinds and sizes of organisations requiring to be trusted at a LoA for the purposes of conducting business electronically. This includes commercial organisations (for-profit and not-for-profit), voluntary or charitable organisations and government organisations. The creation certificate is an authoritative document for IPV. No IPV events occur before creation.
- Operation. A period when the organisation functions normally and is able to authenticate and carry out other trust functions.
- Administration. An event and a temporary period when organisation goes into Administration when it can no longer function normally and requires some form of administrative action to address the needs of relying parties. For example, a company may be sold, broken up or put into receivership prior to being dissolved; a government organisation may be reorganised, merged or disbanded.
- Dissolved. When an organisation ceases to be and its identity has been revoked.

A device's lifecycle has five events or time periods.

- Creation. An event when the device comes into being. No IPV events occur before creation.
- Registration. An event where a trusted manufacturer or authority registers the device with the date of creation, date of registration, location, authority and device details. This record of creation is the equivalent of a birth certificate and is an authoritative document for IPV. The record is cryptographically signed and registered. In the case of Trusted Platform Module (TPM), it results in the creation of a TPM private key in the TPM device, which never leaves the device.
    - NOTE. Other similar technologies to TPM include Mobile Trusted Module (MTM). For the purposes of this International Standard, where reference is made to TPM, MTM is included where MTM supports that function.
- Operation. A period when the device functions normally and is able to authenticate and carry out other trust functions.
- Revocation. When the device ceases to be trusted device and its identity has been revoked
- Destruction. When the device is no longer required. The device should be destroyed securely.

A software application's lifecycle has four events or time periods.

- Creation. An event when the device comes into being. No IPV events occur before creation.
- Registration. An event where a trusted manufacturer or authority registers the software with the date of creation, date of registration, location, authority and software details. This record of creation is

the equivalent of a birth certificate and is an authoritative document for IPV. The record is cryptographically signed and registered.

- Operation. A period when the software functions normally and its signature is valid. The status of the signature is regularly checked using Secure Content Automation Protocol (SCAP). When the signature is updated, the change is either pushed or notified to registered software users. Alternatively, the software signature can time expire and alert the management software. SCAP also communicates other security information that may result in the requirement to revoke the existing software, even if an update is not available.
- Revocation. When the software's signature is no longer valid and the software is required to be updated and revoked.

6.2.2 Credential Lifecycle

The credential lifecycle is described in ISO/IEC 29115 and includes: credential creation; credential pre-processing; credential initialisation; credential binding; credential issuance; credential activation; credential storage; credential suspension, revocation and/or destruction; credential renewal and/or replacement. Credential use is described under entity authentication.

The credential lifecycle is relevant to this standard where a credential is used as part of a document set in support of an application for a different credential. E.g. a citizen e-ID is used to authenticate in an application for an employee credential, or a passport is used to validate an application for an employee credential. In both cases, there is a chain of trust and the Relying Party in the first part of the chain is the Registration Authority for the second part, in which case it:

- Shall establish the Level of Assurance of the first credential;
- Should establish a mechanism for any change in the trust status (revocation, suspension or renewal) of the first credential to be reflected in the trust status of the second credential;
- Shall confirm liability arrangements between CSPs of both first and second credentials.

There may be a reciprocal process in a chain of trust. If so, the Registration Authority in the second part of the chain should inform the Registration Authority in the first part of the chain about any changes in the trust status of the second credential or its associated entity that could affect the status of the credential in the first part of the chain.

6.3 The Four Identity Contexts

A person has up to four identity contexts, each of which has a different legal situation, risk model and user experience:

- Person as a citizen, interacting with their government
- Person as a consumer, interacting with merchants and financial organisations
- Person as a government employee, whose employment relationship is governed by legislation
- Person as a company employee, whose employment relationship is governed by contract

A person applying for an employee or consumer credential is normally required to prove their citizenship or produce a government identity document. Globally, nations have one of two approaches to issuing citizen identity documents:

- Approach One. To register their citizens at birth and build up a profile or footprint of each citizen so that, at an appropriate age, the citizen will be issued a citizen electronic identity (e-ID) credential at LoA 3 or 4. The e-ID can authenticate to a national authoritative register at LoA3 or LoA4.
- Approach Two. To require citizens to apply for a citizen identity document or credential by submitting evidence of their identity in support of their application. The application and evidence of identity is then subject to IPV.

6.4 Levels of assurance

ISO/IEC 29115 defines four LoAs for entity authentication in the Entity Authentication Assurance Framework (EAAF). Each LoA describes the degree of confidence in the processes leading up to and including the authentication process itself, thus providing assurance that the entity that uses a particular identity is in fact the entity to which that identity was assigned.

For the purposes of this International Standard (IS), LoA is a function of the processes, management activities, and technical controls that have been implemented by all actors in the enrolment phase. The overall LoA achieved by an implementation using the EEAF will be the level of the phase with the lowest LoA. This International Standard provides further details for the enrolment phase.

The business selection of the LoA to meet an identity and access management requirement will be driven by the risk assessment and the LoA for the authentication method, which is described, with guidance, in ISO/IEC 29115. This will determine the LoA required for IPV.

Special arrangements (e.g. additional interviews) may be required for exceptional cases, particularly where a person is obviously trusted within their community but is unable to provide the necessary documents or evidence of identity for a normal application.

The LoAs are defined as shown in Table 1.

Level	Description
1 – Low	Little or no confidence in the claimed or asserted identity
2 – Medium	Some confidence in the claimed or asserted identity
3 – High	High confidence in the claimed or asserted identity
4 – Very high	Very high confidence in the claimed or asserted identity

Table 1

6.4.1 Level of assurance 1 (LoA1)

At LoA1, the only objective is to ensure the identity is unique within the intended context. The identity should not be associated with two different entities. LoA1 permits pseudonymity but not anonymity.

At LoA1, there is minimal confidence in the claimed or asserted identity of the entity, but some confidence that the entity is the same over consecutive authentication events.

In practice, the prime use of LoA1 is for social networking.

6.4.2 Level of assurance 2 (LoA2)

At LoA2, there are two objectives. First, the identity shall be unique in the context. Second, the entity to which the identity pertains shall exist objectively, which means the identity is not fictitious or fabricated for fraudulent purposes. At LoA2, there is some confidence in the claimed or asserted identity of the entity. This LoA is used when moderate risk is associated with erroneous authentication.

In practice, the prime use of LoA2 is for online financial transactions and other consumer-centric activities. Anti-money laundering (AML) and Know Your Customer (KYC) legislation obliges the organisations involved to require the applicant to register and provide some form of government-issued identity documentation, in addition to address and bank account information that can be validated or verified.

Where payment credentials are involved, such as credit or debit cards, relying parties can be confident that the issuing bank has carried out a credit check, which is a form of verification. Although this is for creditworthiness (i.e. ability to pay), it also provides some confidence of trustworthiness.

For example, human identity proofing at LoA2 should include checking birth, marriage and death registers to ensure some provenance and confidence about the identity and that it is living, but it does not prove that the entity in possession of a birth certificate is the entity to which the birth certificate relates. Similarly, identity proofing at LoA2 for NPEs should include:

- verification of a serial number, chip number or IMEI with the manufacturer

- proof of ownership or control by the responsible individual(s), who should hold personal identity credentials at the same or higher LoA in their own right.

6.4.3 Level of assurance 3 (LoA3)

LoA3 has an additional objective - to verify the identity information through one or more authoritative sources, such as an external database, which is protected to the same or higher LoA; and validation is communicated via secure means. Identity information verification shows that the identity is in use and links to the entity; and is in the possession of the real or rightful owner claiming or asserting the identity.

At LoA3, there is high confidence in the claimed or asserted identity of the entity. This LoA is used where substantial risk is associated with erroneous authentication. This LoA employs multitype authentication, using at least two different types of factor (usually 'something you have' and 'something you know') for which the relevant biographic and biometric factors should be captured during enrolment.

In practice, the prime use of LoA3 is for employee authentication within and across government and industry organisations conducting normal business, where the employee acts on behalf of the organisation and must comply with the organisation's policies. Data protection, privacy, export control and other regulations, as well as the requirement to protect intellectual property, commercial transactions and other sensitive information oblige the organisations involved to require the applicant or employee to register and provide government identity documents and additional documentation, in addition to address and bank account information that can be validated or verified.

For example, a transaction in which a company submits certain confidential information electronically to a government agency may require a LoA3 authentication transaction or digital signature. Other LoA3 transaction examples include online access to accounts that allow the entity to perform certain financial transactions, or use by a third party contractor of a remote system to access potentially sensitive client personal information.

Another example is a laptop that is connecting to a secure network and has to authenticate to the network and to access a Demilitarised Zone in a cloud environment. It does this using device authentication, which also binds the LoA3 employee to the laptop, and provides a TPM assertion to the relying party organisation's network via the employee's authoritative register.

6.4.4 Level of assurance 4 (LoA4)

LoA4 adds one additional objective to LoA3 by requiring entities to be witnessed in-person (for humans) to help protect against impersonation.

At LoA4, there is very high confidence in the claimed or asserted identity of the entity. LoA4 provides the highest level of entity authentication assurance defined by ISO/IEC 29115. LoA4 is similar to LoA3, but it adds the requirements of in-person identity proofing for human entities and the use of tamper-resistant, tamper-evident and tamper-responsive hardware devices for the storage of all secret or private cryptographic keys. Additionally, all PII and other sensitive data included in authentication protocols shall be cryptographically protected in transit and at rest.

In practice, the prime use of LoA4 is for danger to life, major financial loss, emotional damage, societal damage and national security situations, where the risks involved fully justify the extra costs of LoA4 enrolment and multitype authentication infrastructures. Increasingly, LoA4 is used for federated logical access control, across organisational boundaries and national borders, and also for federated physical access control to buildings and controlled sites. These additional requirements present extra risks, whose mitigation should require stronger IPV.

At LoA4, digital certificates (e.g., X.509, Trusted Platform Module) may be used to authenticate NPEs, such as mobile devices and devices connected to a network. Also, in order to prevent unauthorized access to the power grid, digital certificates may be used in the deployment of smart meter technologies.

6.5 LoA Requirements for IPV

The stringency of identity proofing requirements is based on the objectives that must be met for each LoA, which are cumulative i.e. each LoA builds on lower LoAs.

- LoA1 has one objective - to ensure the identity is unique within the intended context. The identity should not be associated with two different entities.
- LoA2 has an additional objective - the entity to which the identity pertains shall exist objectively, which means the identity is not fictitious or intentionally fabricated for fraudulent purposes. For example, human identity proofing at LoA2 may include checking, by the IPVSP, of birth and death registers to ensure some provenance (although it does not prove that the entity in possession of a birth certificate is the entity to which the birth certificate relates). Similarly, identity proofing at LoA2 for NPEs may include checking, by the IPVSP, a serial number with the manufacturer.
- LoA3 has an additional objective - to verify the identity information through one or more authoritative sources, such as an external database. Identity information verification shows that the identity is in use and links to the entity. However, there is no assurance that identity information is in the possession of the real or rightful owner of the identity.
- For persons, LoA4 adds one additional objective to LoA3 by requiring entities to be witnessed in-person to help protect against impersonation.

IPV processes at a higher LoA shall include the processes of the lower LoAs. For example, LoA3 identity proofing assumes that LoA1 and LoA2 identity proofing controls have been satisfied. A summary is in Table 2.

LoA	Description	Objective	Controls	Method of processing
LoA1 - low	Little or no confidence in the claimed or asserted identity	Identity is unique within a context	Self-claimed or self-asserted	Local or remote
LoA2 - medium	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
LoA3 - high	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
LoA4 – very high	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 2 - Applying Identity Proofing Objectives to the LoAs

Any implementation of the EAAF relies on (a subset of) the identity information and sources that are available to prospective entities and/or to the RA.

The reliability and accuracy of these credentials, identity information, and sources determine the actual assurance provided by the enrolment phase. Consequently, implementers of the EAAF shall carefully consider the assurance provided by the identity (management) infrastructures that are used by the different sources and issuers when deciding which credentials, identity information, and/or sources to rely on for identity proofing and identity verification purposes. Any implementation of the EAAF shall involve 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.

6.6 Actors

The actors involved in the EEAF (ISO/IEC 29115) include entities, CSPs, RAs, RPs, verifiers, and TTPs. These actors may belong to a single organization or separate organizations. There may be a variety of relationships and capabilities provided by a number of organizations including shared or interacting components, systems, and services.

For IPV, the list of actors is expanded to enable different organisations to carry out each function:

6.6.1 Registration authority

A Registration Authority (RA) operates the register of identities, and establishes and/or verifies and vouches for the identity of an entity to a CSP. The RA shall be trusted by the CSP to execute the processes related to the enrolment phase and register entities in a way that allows later assignment of credentials by the CSP.

Each RA shall ensure that the appropriate identity proofing and identity verification for the LoA is carried out. It would be normal to contract to a certified identity proofing service provider and/or a certified identity verification service provider. In order to differentiate the entity from other entities, an entity is typically assigned one or more identifiers, which will allow the entity to later be recognized in the applicable context.

6.6.2 Identity Proofing Service Provider

The Identity Proofing Service Provider is an actor that carries out identity proofing. They have the expert skills and equipment to use the security features of identity documents and to check foreign identity documents. They also have knowledge and experience of fraud vectors and may have access to government and commercial lists of lost, stolen and fraudulent documents and fraudsters.

6.6.3 Identity Verification Service Provider

The Identity Verification Service Provider is normally either a government agency that conducts biographic and biometric footprint checks of citizens, foreign workers and employees for identity verification, or a company licensed to collect and analysed data for the purpose of creditworthiness checks and identity verification of individuals and companies (e.g. credit reference agencies). In agreed circumstances, companies can check some government-held information and vice-versa.

6.6.4 Relying party

An RP is an actor that relies on an identity claim or assertion. The relying party may require an authenticated identity for a variety of purposes, such as account management, access control, authorization decisions, etc. The relying party may itself perform the operations necessary to authenticate the entity, or it may entrust these operations to a third party.

6.6.5 Record-keeping/recording

This is the process of concluding the enrolment of an entity that, if successful, results in registration. This record shall include the information and documentation that was collected (and may be retained), information about the identity information verification process, the results of these steps, and other pertinent data. A decision is then rendered and recorded to accept, deny, or refer the enrolment for further examination or other follow up.

Records shall be kept for every (applicable) process involved in the credential management phase. Where credentials are issued to human entities, the keeping of records is likely to involve the processing of PII.

6.7 Requirements for Identity Proofing and Verification Systems and Services

This clause shall apply for LoA2 and above, and may apply for LoA1 where there is a legal obligation for an pseudonymous entity to be identified for reasons of liability or criminal investigation.

It should be possible to make users and suppliers of IPV systems accountable for any failure in the results of the IPV process, or in their actions to detect fraud and conduct protective monitoring of systems and the employees that operate the system.

IPV systems and services shall:

- Be assured by a scheme approved by industry or government within the jurisdiction of operation.
- Support the detection, response and reporting of fraud, abuse or misuse.
- Include within their processes, measures to prevent collusion by employees that results in the deliberate registration of false identity information leading to the issuance of a valid credential with a false identity or the provision of false information from the register to a relying party.
- Record accounting information to enable independent auditing of the IPV system operations and results by internal and external bodies as required by relevant business practices and legislation.

Any Register of Organisations (ROO) shall be assured by a scheme approved by industry or government within the jurisdiction of operation.

7 Enrolment

Enrolment is the first phase in the Entity Authentication Assurance Framework (EAAF), prior to the Credential Management Phase. Enrolment comprises four primary processes:

- Application and initiation.
- Identity proofing and verification (IPV). IPV uses the application details and supporting evidence for the entity, referring to trusted third parties as necessary, in order to verify the information provided and its binding to the identity of the entity..
- Record keeping/recording. 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.
- Registration. Entry in an authoritative register of a successful enrolment, which is then available to Trusted Third Party (TTP) organisations including:
    - Credential Service Providers (CSPs) for the production and issuance of credentials;
    - Identity Providers (IDPs) who support the creation of an account in a directory service, to which a credential can be bound for the purposes of logical and physical access control.
    - Data Service Providers (DSPs) who provide data and information services, ranging from analysed information for specific business purposes through to bulk data for statistical purposes and trend analysis.

The required processes differ according to the rigour required by the applicable LoA. In the case of an entity enrolling under LoA1, these processes are minimal (e.g., an individual may click a “new user” button on a webpage and create a username and password). In other cases, enrolment processes may be extensive. For example, enrolment at LoA4 requires an in-person meeting between the entity and the RA, as well as extensive identity proofing.

8 Application and Initiation

The detail of the application and initiation process will be dependent on national, organisational and credential specific requirements. The application together with supporting information is made to a service provider who initiates the identity proofing and verification process.

The enrolment process can be initiated by the subject or a third party on behalf of the subject, or by the CSP itself (e.g., government-issued identification card, employee badge). For example, at higher LoAs, applications may be accepted only where the entity has been sponsored by a third party.

The application process will involve the provision and recording of information to characterise and support the application. The information should ensure that the entity is identified uniquely within a context as required by the relevant LoA (e.g., in the case of a human entity this might include recording the full name, date and place of birth).

For NPEs, such as for a mobile device, enrolment at a given LoA may require initialisation during manufacture or through the deployment of credentials to the device, which enables the device to be identified uniquely and to receive tailored device settings via an encrypted configuration profile.

9 Identity Proofing and Verification - General

IPV is the process of capturing and verifying sufficient information to identify an entity to a specified or understood LoA. If successful, the result is recorded in an authoritative register. In reality, identity proofing and identity verification processes are not sequential but overlap each other, but recognising that proofing involves interacting with the applicant and verification does not.

Validation of a credential with a Source of Authority can occur during proofing and/or verification. Validation normally involves either:

- An IPVSP interaction with the Source of Authority, independently from the subject, or
- The subject using their electronic credential to authenticate to the Source of Authority, witnessed by the IPVSP. (this should be the subject at LoA1 and 2, and shall be the subject at LoA3 and 4).

Depending on the context, a variety of identity information (e.g., government identity cards, driver's licenses, biometric information, machine-based attestation, birth certificates) from authoritative sources may fulfil identity proofing requirements. The actual identity information presented to fulfil identity proofing requirements varies with the LoA and over time.

A Standing Document [SD-NN] is being proposed in support of this International Standard for nations to list their IPV policy documents:

- Identity proofing and verification documents that are currently approved for electronic authentication and non-electronic identity purposes. Nations would supply and regularly update their list of identity documents for proving/verifying identity within their own nation.
- A list of the types of organisations that exist
- A list of attributes required for each type of organisation, the policy for their enrolment and the organisations approved to be a CAA.

10 Person IPV

The first requirement is for Relying Parties to be able to validate a person's identity and/or their attributes with a timeliness compliant within an agreed Common Policy. The norms for timeliness are as follows:

- Less than 6 hours for LoA 4 – Very High Assurance.
- Less than 24 hours for LoA 3 – High Assurance.
- Less than 48 hours for LoA 2 – Medium Assurance, although some international industry communities allow for longer.
- Not specified for LoA 1 – Low Assurance.

The second requirement is for attributes (bound to PersonID). Each should be issued by a Certified Attribute Authority (CAA) at a specified LoA.

Threats	Controls	Required controls			
		LoA1	LoA2	LoA3	LoA4
Impersonation	IPV:Attributes	#1	#2	#3	#4

Table 3 - Enrolment phase controls for each LoA

The following controls against enrolment phase threats correspond to #1 - #6 listed in Table 3.

IPV:Attributes

#1 – There is no requirement

#2 – All shall apply.

- First name
- Middle name
- Last name
- Date of Birth
- Place of Birth
- Gender
- Home address
- Home UPRN (if UPRN exists)
- Home telephone number
- Nationality or nationalities
    - If a national citizen, the National ID Number or similar
    - If foreign or a dual national, the National ID Number of each citizenship

#3 – All attributes at #2 shall apply plus:

- Passport issuing authority
- Passport number, expiry date and remaining Machine Readable Zone data.
- Home email address
- Work address
- Work UPRN (if UPRN exists)
- Work telephone number
- Work email address
- Bank account details
- Known aliases
- Parents' names and address(es)
- Referees' names and addresses
- ICAO-compliant facial image
- Additional biometric and biographic attributes required by an authority

#4 – All attributes at #3 plus:

- Additional biographic and biometric attributes required by an authority

Three Attribute Sets shall be maintained.

- Initial Attribute Set (IAS). All attributes recorded during initial enrolment are saved in perpetuity, together with their LoA, source, date and (if appropriate) the digital signatures and public encryption keys of the appropriate CAA.
- Current Attribute Set (CAS). The most up-to-date set of attributes bound to the OrgID, which will be provided in response to a request by an authorised relying party.
- Archive Attribute Set (AAS). All superseded attributes are archived for reasons of forensics, resilience and data integrity.

10.1 IPV Approaches

Citizenship and government-issued identity documents underpin IPV for persons.

Globally, nations have one of two approaches for issuing identity documents to their citizens:

- Approach One. To register their citizens at birth and build up a profile or footprint of each citizen so that, at an appropriate age, the citizen will be issued a citizen electronic identity (e-ID) credential at LoA 3 or 4. The e-ID can authenticate to a national authoritative register at LoA3 or LoA4.
- Approach Two. To require citizens to apply for a citizen identity document or credential by submitting evidence of their identity in support of their application. The application and evidence of identity is then subject to IPV.

Nations have one of three approaches for the identification of foreign nationals, working or resident:

- To accept and use the identity documents issued by the foreign nationals government, either by agreement or by enabling cross-border validation or authentication to a Source of Authority.
- To issue a foreign national electronic credential (either the same as or similar to the citizen's e-ID), having validated or authenticated the foreign citizen identity credential. This is based on Approach One.
- To issue a foreign national electronic credential without the ability to carry out cross-border validation or authentication, and instead carrying out Approach Two.

The rest of this Section concerns Approach Two only.

10.2 Identity Proofing - Person

Identity proofing is the process of capturing and verifying sufficient EoI to identify an entity to a specified or understood LoA. It involves interaction with the applicant (remotely or in person) and their application. It is the process of the physical checking of presented identity documents to detect possible fraud, tampering or counterfeiting, and also taking steps to bind the entity to the claimed identity. The identity proofing requirements shall be more stringent, the higher the LoA – See Table 4. Also, the identity proofing process shall be more stringent for entities asserting or claiming an identity remotely (e.g., via an online channel) than locally (e.g., in-person with the RA).

LoA	Controls	Method of processing	Biometric
LoA1 - low	Self-claimed or self-asserted	Local or remote	No biometric
LoA2 - medium	Proof of identity through use of identity information from an authoritative source	Local or remote	May include face
LoA3 - high	Proof of identity through use of identity information from an authoritative source + identity information verification	Local or remote	Will include face. May include second biometric for matching
LoA4 – very high	Proof of identity through use of identity information from multiple authoritative sources + identity information verification + entity witnessed in-person	Local only	Will include face. May include second biometric for matching and third for authentication

Table 4 - Proofing Overview

10.2.1 Documentary Evidence of Identity

Documentary evidence to prove an identity is provided with the application for a given LoA.

The evidence should reflect the breadth and depth of the whole life of the individual across all three categories:

- Citizen. Evidence that demonstrates the person's life as a citizen and any support or services they are provided by their government or the government where they live;
- Money. Evidence that demonstrates the person's financial and working life;
- Living. Evidence that demonstrates where they live and what they consume.

The evidence within these categories will have differing LoA for many reasons, such as their purpose, issuing process, inherent security features and the ability of the document to be validated or authenticated.

Primary evidence. The issuing source has very strong issuance procedures that include robust checking processes sufficient to meet the required LoA, anti-collusion and counter-fraud throughout. It shall be possible to establish an unambiguous link between the identity evidence presented, the claimed identity and the living person in the application. The IPVSP shall be able:

  - to validate the identity evidence with the Source of Authority within the same jurisdiction and, where possible, in another jurisdiction. Where validation in another jurisdiction (i.e. across borders) is not directly possible, indirect means shall be available to validate the documents through a TTP located in the second jurisdiction, where the Source of Authority is also located.
  - to test the security features of each identity document using appropriate technology where the security feature requires it, and expert skills otherwise.
  - to provide supervised facilities for a person who possesses a citizen e-ID to authenticate to their national Source of Authority.
  - to carry out biometric authentication of any identity evidence containing biometrics.

- Secondary evidence. Issued using strong issuance procedures. The evidence contains some security features to assist in the checking and validation of the evidence, but not sufficient to qualify as primary evidence. It should be possible to establish an unambiguous link between the identity evidence, the claimed identity and the living person.
- Tertiary evidence. Issued using weak issuance procedures. The evidence contains weak or no security features and/or cannot be validated with the issuing authority. The evidence may have been issued following a remote application process and is easily forged or altered.

RAs should gather evidence from all three identity categories to demonstrate breadth and depth of evidence in accordance with the minimum numbers shown in Table 5. The same piece of evidence cannot be used to cover more than one identity category. Each piece of evidence should be assessed and classified as Primary, Secondary or Tertiary.

Table 5 shows the minimum number of documents required to support EoI.

LoA	Primary	Secondary	Tertiary
4	Two	Two	Two
3	Two	One	One
2	One	One	One
1	-	-	-

Table 5 -Minimum Items of Evidence by LoA

Identity evidence is shown at Annex B.

10.2.2 Primary Threats and Controls

Table 6 identifies the required controls for the enrolment phase according to LoA.

Threats	Controls	Required controls			
		LoA1	LoA2	LoA3	LoA4
Impersonation	IdentityProofing: PolicyAdherence	#1	#1	#1	#1
	IdentityProofing: In Person				#2
	IdentityProofing: AuthoritativeInformation	#3	#4	#5	#6

Table 6 - Enrolment phase controls for each LoA

Note – In the above table, the identifiers #1 - #6 correspond to the specific controls required to provide protection at each LoA. Each of these controls is described in detail below. Identity proofing in person is not mandatory for LoA1-3, but it is recommended for LoA3.

The following controls against enrolment phase threats correspond to #1 - #6 listed in Table 4.

IdentityProofing: PolicyAdherence

#1. Publish the identity proofing policy, and perform all identity proofing in accordance with the published identity proofing policy.

IdentityProofing: In Person

#2. In-person identity proofing shall be used for humans.

IdentityProofing: AuthoritativeInformation

#3. Identity information may be self-claimed or self-asserted.

#4. The following controls apply:

- All controls from #3

In addition:

- The entity shall provide identity information from at least one authoritative source of identity information.

a) For humans:

i. In-person:

- Ensure that the entity is in possession of a Primary identification document from at least one authoritative source that bears a photographic image of the holder that matches the appearance of the entity; and
- Ensure that the entity is in possession of at least one Secondary and one Tertiary supporting identification document; and
- Ensure that the presented identification documents appears to be a genuine document, properly issued and valid at the time of application.

ii. Not-in-person:

- Ensure that the entity is in possession of a Primary identification document from at least one authoritative source that bears a photographic image of the holder that matches the appearance of the entity; and
- Ensure that the entity is in possession of at least one Secondary and one Tertiary supporting identification document; and
- The existence and validity of the evidence provided shall be confirmed in accordance with policy requirements.

#5. The following controls apply:

- All controls from #4.

In addition:

a) For humans:

i. In-person:

- The entity shall provide identity Primary information from at least one additional policy-compliant authoritative source.
- Verify the accuracy of contact information listed in the identification document by using it to contact the entity;
- Verify both Primary identification documents (e.g., document attesting to birth, marriage, or immigration) against registers of the relevant authoritative source;

- Corroborate personal information against applicable authoritative information sources and (where possible) sources from other contexts, sufficient to ensure a unique identity; and
- Verify information previously provided by, or likely to be known only by, the entity.

ii. Not-in-person:

- Ensure check by a trusted third party (who is at the same LoA or higher) of the entity's assertion/claim to the current possession of a LoA3 (or higher) credential from an authoritative source; and/or
- Verify information previously provided by, or likely to be known only by, the entity.

#6. The following controls apply:

- All controls from #5.

In addition:

a) For humans:

- The entity shall provide identity Primary or Secondary information from at least one additional policy-compliant authoritative source.
- The entity shall provide identity Tertiary information from at least one additional policy-compliant authoritative source.

10.2.3 Counter-Fraud Measures

Table 7 shows the possible counter-fraud threats that document checking during identity proofing

If a clone exists then two versions of the document are in circulation, one Real and one Fake, but the Source of Authority will only show the Real document until such time as the Fake is detected and action is taken. Cryptographically bound credentials can mitigate this risk.

Identity	Document	Threat	Validation
Real	Real	OK	Pass
Real	Stolen	ID fraud	Lost and Stolen
Real	Tampered	ID fraud	Source of Authority
Real	Fake	ID fraud	Fail
Real	Clone	ID fraud	Fail
Fake	Real	ID fraud	Source of Authority
Fake	Stolen	ID fraud	Lost and Stolen
Fake	Tampered	ID fraud	Source of Authority
Fake	Fake	ID fraud	Fail
Sold	Real	Impersonation	Source of Authority
Sold	Stolen	Impersonation	Lost and Stolen
Sold	Tampered	Impersonation	Source of Authority
Sold	Fake	Impersonation	Fail
Stolen	Real	ID theft	Source of Authority
Stolen	Stolen	ID theft	Lost and Stolen

Stolen	Tampered	ID theft	Source of Authority
Stolen	Fake	ID theft	Fail

Table 7 - Document Proofing Outcomes

Depending on the LoA, identity proofing controls for remote and in-person proofing shall include:

- Checking all information in the application for omissions, errors and contradictions.
- Checking each document for its physical construction, material quality, print quality, security features, seals and signatures. This should include:
    - Any signs of tampering (where a real document has been altered), such as photographs or printed data being altered, or the document being dismantled and reassembled, or pages not aligning in a passport.
    - Any signs of it being a counterfeit or fake document, pretending to be a real document. Many documents 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. Document checks without such skills or machines are much more likely to fail to identify a fake document.
- Checking each document for consistency and accuracy of the information in each document and between documents. This shall include
    - Checking whether a document has been reported as lost or stolen.
    - Validating documents with the Source of Authority, wherever possible.
    - Authenticating credentials systemically to their Source of Authority, wherever possible.
    - Validating the active status or expiration of documents that have a defined lifetime.
- Capturing biometric characteristics where appropriate for the LoA (e.g. face, fingerprints (individuals or tenprint sets), iris, palm, vein, voice etc.). Information and image quality is essential. Individual biometrics shall be captured in accordance with ICAO 9303 and ISO/IEC 19794-X series standards and used for end-to-end authentication in accordance with ISO/IEC 24761 - ACBIO.
    - Where biometric proofing is required in enrolment for LoA3 and above, the biometrics shall be matched 1:many (one-to-many) against all records in the biometric store to prevent duplicate identities. Additional appropriate biometrics (e.g. fingerprint, voice) should also be captured for subsequent authentication using 1:1 matching.
    - Interviewers shall compare the physical appearance of the subject during the interview with the biometric and other relevant information, to establish any discrepancies e.g. of physical characteristics, appearance and accents, which may require further investigation.
    - 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.
- Questioning the applicant about information in the supporting documents and, where possible, related information known to the authorities, 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. To identify fraudulent applications:
    - Interviewers shall use information from the application and other sources (e.g. banks) to support questioning.
    - Interviewers shall 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 9th is correct.

- Interviewers shall question family relationships, history and movements, and key life events.

- Questioning the applicant by interview to assess their behaviour. Experience shows that in-person interviews are very effective in deterring fraud. For LoA 4, all interviews shall be witnessed or video recorded with clearly audible sound, using High Definition video format. Where interviews are required for LoA 3, they should be witnessed or recorded in the same way. The video record is to be stored and protected as a legal record and privacy data.
  - The person being interviewed shall not normally be accompanied.
  - Where translation is required, the RA shall provide the translator.
  - Where the applicant is unable to communicate for reasons of physical or mental difficulty and attends with a proxy or caregiver, the RA shall 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 hamper normal identity proofing, alternative arrangements should be made for such needs as privacy, same-sex interviews and biometric capture, so as to ensure that identity proofing is carried out correctly
  - Where a minor (age 15 or less) is being interviewed, they will be accompanied by a parent or legal guardian, who shall be authenticated using their own identity document of the same LoA or higher to that being requested for the minor.
  - If the interview is done remotely:
    - There shall be sufficient additional monitoring by trusted persons and/or trusted surveillance sensors and video recording to prevent fraud or misrepresentation for a given LoA.
    - There shall be additional verification checks prior to the interview to establish the degree of risk associated with the applicant and the likelihood they will seek to subvert the interview. Where the risk is high, an in-person interview shall take place.
  - However, other nations may be unable or unwilling for various reasons to mandate the requirement for in-person interviews except for high risk situations, e.g. when the applicant has a history of criminal or anti-social behaviour, or when the application contains significant contra-indicators. Such applicants shall be interviewed in person.

10.3 Identity Information Verification

Identity information verification is the process of checking identity information and credentials against issuers, data sources, or other internal or external resources with respect to authenticity, validity, correctness, and binding to the entity. It does not involve interaction with the applicant. It involves using data from many sources, including the biographical and biometric footprints, to corroborate the application and statements made by the subject or the applicant.

Identity information verification seeks to:

- Corroborate the information provided in the application as evidence of identity, using data sources for the biographic footprint, resulting in a confidence score that determines which LoA to assign.
- Detect contra-indicators in the biographic footprint that either:
  - Directly and completely contradict key information presented in the application, to the extent that application shall proceed no further until the case has been investigated or an immediate decision is taken to refuse the application. This may result in an additional fraud investigation. In these situations, IPVSPs shall take all reasonable steps to ensure that the

corroborating data is factually correct and does not result in a legitimate applicant being falsely rejected.

- Partially contradicts information presented in the application and presents a level of risk that could be a cause for halting the application or reducing the confidence score. The higher the LoA, the greater the risk and the requirement to halt the application, pending investigation.

Corroboration should check for:

- The existence of the claimed identity and that the person is living.
- The validation of identity documents not yet validated or the assessment of sufficient corroborating information to give sufficient confidence that the documents could be validated at the chosen LoA.
- Evidence that the person is the owner of the claimed identity
- Evidence of use of the claimed identity in the three categories – Citizen, Money and Living.
- All verification activity should give due account to the timeliness, accuracy and relevance of corroborating information.
  - Time shall include the recent activity, The more recent the activity, the greater its value.
  - Time shall include history. New information isn't always the best. Due weight should be given to there being a rich set of corroborating data over time, particular where it links to other known identities, locations and events. Old community, family and background information is valuable and should be augmented by recent transactional activity information. The longer the period, the greater its value.
- IPVSPs should have a confidence rating for each information attribute, which feeds into the overall Confidence Score.

11 Organisation IPV

11.1 Introduction

Organisations, their employees, partners, customers, consumers, devices, data and cryptographic signatures need to be trusted. All these entities are, or should, be bound to a unique Organisational Identifier or OrgID so that it, and any associated attributes, can be validated in real time by any relying party (person, organisation, device or application) to a given LoA.

The underlying issues are international and transnational. UNCITRAL is responsible for the commercial law requiring all nations to have registers for commercial organisations, however national implementations vary in scope, governance and trustworthiness, and most are not suitable for the Internet Age. They need to be improved to meet this International Standard.

11.2 The Problem

Where identity credentials are issued based on best practice and international standards (ISO 29115, ITU-T X.1254 etc), most consumers are issued LoA 2+ credentials and most employees are issued LoA 3+. Conformance with such standards enables federated trust across organisations and secure collaboration. i.e. an organisation can trust identity credentials and associated attributes belonging to another organisation, where they are issued and used in accordance with agreed Common Policy overseen by Collaborative Governance in a federation model.

It is policy that any organisation in the enrolment or issuance process for a trusted credential is itself operating at the same LoA as the credential, or higher. Thus a company issuing LoA 3 credentials to its employees must itself be a LoA 3 or 4 organisation. The same applies to compliant Credential Service Providers (CSPs) and Identity Providers (IDPs).

In addition, the timeliness and accuracy of the information underpinning any credential or associated attribute are fundamental to their trustworthiness. This can be done by a positive check (is it valid, yes or no?) or a negative check (has it been revoked? If not, I will assume it is valid), to within a specified timeliness. The de facto revocation time for a LoA 3 credential is normally 24 hours, i.e. if a policy issue occurs, the credential will be revoked or attribute status changed, and the new status published, all within 24 hours. Similarly, the revocation time for a company or organisation (OrgID) at LoA 3 and any attributes bound to the OrgID should be the same.

This requires nations and/or industry sectors to establish suitable and compliant registers as Authoritative Sources for their OrgIDs – Registers of Organisations (ROO).

11.3 Types of Organisations

There are many types of organisations – an example list for one country is at Annex C. However, most of these can grouped under three headings:

- Publicly owned organisations, including for-profit, not-for-profit and voluntary organisations.
- Privately owned organisations, including for-profit, not-for-profit and voluntary organisations.
- Government owned organisations.

11.3.1 Publicly Owned Organisations

A Publicly Owned Organisation shall be a legally recognised entity whose formation or incorporation included the filing of required forms with the registration authority in its jurisdiction, the issuance or approval by such registration authority of a charter, certificate or licence, and whose existence can be verified with that registration authority. Also, a Publicly Owned Organisation shall:

- Have a verifiable physical existence, a registered office and business presence;
- Have an Accountable Person who is accountable for the provision and maintenance of information associated with the organisation to any authority. The Accountable Person shall be a Responsible Person;
- Have at least one additional Responsible Person associated with the Publicly Owned Organisation must be identified and validated;
- Together with the Accountable Person, not be located or residing in any country where the verifier is prohibited from doing business or issuing a certificate by the laws of the verifier's jurisdiction;
- Together with the Accountable Person, not be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the verifier's jurisdiction.

11.3.2 Privately Owned Organisations

A Privately Owned Organisation shall be a legally recognised entity whose formation or incorporation included the filing of required forms with the registration authority in its jurisdiction, the issuance or approval by such registration authority of a charter, certificate or licence, and whose existence can be verified with that registration authority. Also, a Privately Owned Organisation shall:

- Have a verifiable physical existence, a registered office and business presence;
- Have an Accountable Person who is accountable for the provision and maintenance of information associated with the organisation to any authority. The Accountable Person shall be a Responsible Person;
- Have at least one additional Responsible Person associated with the Privately Owned Organisation must be identified and validated;
- Together with the Accountable Person, not be located or residing in any country where the verifier is prohibited from doing business or issuing a certificate by the laws of the verifier's jurisdiction;

- Together with the Accountable Person, not be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the verifier's jurisdiction;
- Not be designated on the records of the incorporating or registration authority by labels such as "inactive," "invalid," "not current," or the equivalent;
- Have a Jurisdiction of Incorporation, Registration, Charter, or License, and/or its Place of Business that shall not be in any country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction;
- Not be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.

11.3.3 Government Owned Organisations

The legal existence of the Government Owned Organisation must be established by a parent Government organisation that is itself established by statute or legislation and is accountable, ultimately, to the Head of State or national legislative assembly. The operation of the Government Owned Organisation shall be similarly accountable. Also, the Government Owned Organisation shall:

- Have a verifiable physical existence, a registered office and business presence;
- Have an Accountable Person who is accountable for the provision and maintenance of information associated with the organisation to any authority.
- Not be in any country where the verifier is prohibited from doing business or issuing a certificate by the laws of the verifier's jurisdiction;
- Not be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the verifier's jurisdiction.

11.4 Business Requirements

The first business requirement is for Relying Parties, (e.g. CSPs, customers, regulators, partner organisations and allies) to be able to validate an OrgID and/or its attributes with a timeliness compliant within an agreed Common Policy. The norms for timeliness are as follows:

- Less than 6 hours for LoA 4 – Very High Assurance.
- Less than 24 hours for LoA 3 – High Assurance.
- Less than 48 hours for LoA 2 – Medium Assurance, although some international industry communities allow for longer.
- Not relevant for LoA 1 – Low Assurance.

The second business requirement is for attributes (bound to OrgID) that cover the following categories. Each should be issued by a Certified Attribute Authority (CAA) at a specified LoA. ROO validates against each CAA as required by policy. For example (see below), UPRNs are centrally issued at LoA4 but LEIs are self-asserted with some supporting evidence at LoA 2:

- Category 1 - Authentication. OrgID and all attributes required to support the enrolment and management of an OrgID at a given LoA. This should include the Unique Property Reference Number (UPRN) for the registered address and each address for a primary company function, and the Legal Entity Identifier (LEI), where it has been assigned, in accordance with G20 Rules. It also includes the details of: the Accountable Person; the Responsible Persons for the organisation (e.g. Directors and Trustees); and Primary Beneficiaries (e.g. Any Beneficiary with a shareholding of 10% or more). The Accountable Person is always one of the people responsible for the organisation. (Mandatory)
- Category 2 – Authority to Act. Other trust functions, including certifications and certification dates, required by legislation and regulation for both the organisation and also the persons authorised to act

on behalf of the organisation. This includes licences to operate in accordance with regulations. (Mandatory)

- Category 3. Sector-specific qualification or certification attributes required by regulation or legislation, which are issued by appropriate professional and qualification authorities. (Optional)
- Category 4. Procurement process attributes required by governmental procurement regulations. (Optional)
- Category 5. Attributes normally required across supply chains by sector-specific contracts for the purposes of supply chain management through the life of a contract. (Optional)
- Category 6. Self-asserted attributes. (Optional).

In the case of attributes, the CAA for each attribute would digitally sign its attributes to enable their validation, using signatures at the appropriate LoA issued by a compliant CSP or IDP.

See Annex C - Attributes for Categories 1 and 2.

Three Attribute Sets shall be maintained:

- Initial Attribute Set (IAS). All attributes recorded during initial enrolment are saved in perpetuity, together with their LoA, source, date and (if appropriate) the digital signatures and public encryption keys of the appropriate CAA.
- Current Attribute Set (CAS). The most up-to-date set of attributes bound to the OrgID, which will be provided in response to a request by an authorised relying party.
- Archive Attribute Set (AAS). All superseded attributes are archived for reasons of forensics, resilience and data integrity.

11.5 Organisation IPV Scope

The scope is based upon the concept that any organisation conducting business on the Internet should be trustworthy and therefore registered in such a way that its trustworthiness can be demonstrated to others for reasons of regulatory compliance, due diligence, corporate responsibility and competitive advantage. The eventual scope for a ROO in any country should include:

- All legally defined organisations registered in a country.
- All legally defined organisations operating in a country but not currently registered.
- All organisations that are financially active in a country and conduct financial transactions.
- All voluntary sector organisations that are financially active, operate in regulated activities or are in receipt of government or international funding.
- Any foreign registered organisation that wishes to do business in a country with industry partners and government customers.
- Any government organisation in a country. The reason being that it is difficult and costly to detect impostor or fake government organisations unless real government organisations are registered either in ROO or a suitable government register, such that they able to prove their identities and their attributes.
- Any foreign government or industry organisation that wishes to conduct business with partners from the country or under the country's law. E.g. in a multinational satellite programme or an overseas development programme.
- Any organisation, anywhere, that is involved in a global supply chain and that seeks to be insured by a company registered in this country for shared risks associated with cybersecurity and the sharing of sensitive information.

11.6 Organisation Enrolment

The enrolment policy for new organisations will rely upon binding the organisation to directors, trustees and persons responsible in law, who shall already possess credentials at the desired LoA before a company is created. The number, provenance and accuracy of Category 1 and 2 attributes bound to the OrgID will vary by LoA.

The enrolment process for existing organisations will be at least as strong as the process for new organisations. For most established organisations in highly regulated industries that can evidence their trustworthiness, this should be straightforward. Others may require assistance.

11.7 Threats to Organisation IPV

Successful organisation enrolment depends on the persons and supporting EoI for the organisation being trusted to the required LoA. The threats to organisation enrolment are the same as those for person identity and to the provision of trusted attributes from Sources of Authority.

11.8 Controls for Organisation IPV

Table 8 identifies the controls that are appropriate to each LoA.

Threats	Controls	Required controls			
		LoA1	LoA2	LoA3	LoA4
Impersonation	IPV: PolicyAdherence		#1	#1	#1
	IPV: In Person		#2	#2	#2
	IPV: AuthoritativeInformation		#4	#5	#6

Table 8 - Controls for Organisational Enrolment

Note – In the above table, the identifiers #1 - #6 correspond to the specific controls required to provide protection at each LoA. The following controls against enrolment phase threats correspond to #1 - #6 listed in Table .

IPV: PolicyAdherence

#1. Publish the IPV policy, and perform all IPV in accordance with the published IPV policy.

IPV: In Person

#2. The Accountable Person shall be the applicant. The Accountable Person and other responsible persons, e.g. directors or trustees, shall appear in person to support their application for an OrgID.

IPV: AuthoritativeInformation

#3. For the LoA requested for the OrgID, the Accountable Person and other responsible persons shall possess a personal credential at the same as LoA or higher, and be able to authenticate with it to the Authoritative Source.

#4. The following controls apply:

- All controls from #3

In addition, the applicant shall provide EoI, including:

- Government documents proving registration, where the type of organisation is required to be registered by one or more government organisations,
- EoI from at least one authoritative source, where the type of organisation is not required to be registered by one or more government organisations.
- Depending on the Organisation Type, all attributes listed at Annex C

#5. The following controls apply:

- All controls from #4.
- In addition:
    - Category 3 attributes required to operate in one or more sectors.

#6. The following controls apply:

- All controls from #5.
- In addition:
    - Additional Category 3 attributes for very high assurance required by regulation e.g. national security, danger to life, high financial risk, reputational damage and critical national infrastructure.
    - Category 4, 5 and 6 attributes as required

11.9 Monitoring

Asserting party organisations should have the choice on whether they choose to distribute update notifications in real time or wait for information requests and respond within the appropriate timeliness.

Relying party organisations should have the choice on whether to request notifications or alerts (push mechanism) in real time or as agreed within the timeliness, or to pull status information from ROO as needed.

12 Device IPV

Most devices require some form of authentication to support a network connection and a session. This requires the device to have logical and physical unique identifiers. These identifiers may not be linked at lower LoAs, but they should be linked at LoA 3 and shall be at LoA4. However, many types of identifier exist, which work in an enterprise but don't scale for supply chain or cross-organisational purposes.

Trusted Platform Module (TPM) is becoming the leading standard for wide-scale device authentication and other trust functions. Over 750M TPM devices are already deployed. TPM 2.0 has been approved by all leading nations and includes a specification for mobile devices, which will increase adoption significantly. Other methods for device authentication are mainly for specific use cases. Hence, this International Standard considers IPV for TPM as an example that can be applied for other methods of device authentication. The first section describes IPV for TPM. The second section describes generic IPV controls for devices, based on TPM's functions.

12.1 Overview of TPM

TPM is both the name of a published specification detailing a secure crypto-processor that can store cryptographic keys to protect information, and the general name of implementations of that specification, often called the "TPM chip" or "TPM Security Device". The TPM specification is the work of the Trusted Computing Group. The current version of the TPM specification is Version 2.0.

TPM offers facilities for the secure generation of cryptographic keys, and limitation of their use, in addition to a random number generator. It also includes capabilities such as remote attestation and sealed storage.

- Remote attestation creates a nearly unforgeable hash-key summary of the hardware and software configuration. The program encrypting the data determines the extent of the summary of the software. This allows a third party to verify that the software has not been changed.
- Binding encrypts data using the TPM endorsement key, a unique RSA key burned into the chip during its production, or another trusted key descended from it.
- Sealing encrypts data in similar manner to binding, but in addition specifies a state in which the TPM must be in order for the data to be decrypted (unsealed).

Software can use a TPM to authenticate hardware devices. Since each TPM chip has a unique and secret RSA key burned in as it is produced, it is capable of performing platform authentication.

Generally, pushing the security down to the hardware level in conjunction with software provides more protection than a software-only solution. However even where a TPM is used, a key would still be vulnerable while a software application that has obtained it from the TPM, is using it to perform encryption/decryption operations, as has been illustrated in the case of a cold boot attack. This problem is eliminated if key(s) used in the TPM are not accessible on a bus or to external programs and all encryption/decryption is done in the TPM.

12.1.1 Endorsement Key (EK) Credential

The EK credential contains the public EK, as well as various assertions regarding the security qualities and provenance of the TPM. This credential is sometimes provided by the TPM manufacturer, but may also be provided by the platform manufacturer. In some cases, no EK credential is provided or present in devices when they are delivered to end consumers, so these may ultimately need to be provided by or for the consumer (e.g., by a deploying IT department).

The EK credential may be considered to be privacy-sensitive, as in typical deployments, only one EK is created over the lifetime of a TPM, implying that the EK uniquely identifies the TPM in which it resides.

12.1.2 Platform Credential

A platform credential attests that a specific platform contains a unique TPM permanently associated with a static or dynamic root of trust. The platform credential is typically issued by the platform manufacturer, and contains a reference to the associated EK certificate, as well as assertions regarding the platform manufacturer, platform model, and platform security properties (among other things).

The platform credential has been specified as an X.509v3 Attribute Certificate (as it contained no public key), but a lack of widespread attribute certificate support led to the pragmatic compromise of simply making this a standard X.509v3 certificate containing a copy of the EK public key.

12.1.3 Attestation Identity Key (AIK) Credential

The AIK credential is issued by an Attestation Certification Authority (ACA) that is trusted to validate the various credentials associated with the EK and platform, and to honour the privacy policies of the client. The primary goals of the AIK certificate are to attest that a TPM contains the AIK, that the AIK is tied to valid EK and platform credentials, and that use of the AIK is restricted to the operations defined in the TPM specification. The present specification is primarily concerned with the operation of the Attestation CA, and with the interaction between a platform and this CA.

12.1.4 Attestation CA

The Attestation CA is the primary CA associated with the TPM. It provides the AIKs and binding with the EK sufficient to maintain integrity and trust, yet also maintain the privacy of the EK and other AIKs where required.

12.1.5 Identity of a TPM and the AIK

Nominally, each TPM, once activated, has exactly one EK key pair, so that prior to activation, one TPM is indistinguishable from another. Once the EK pair is generated, it represents a unique identifier of a particular TPM hardware instance. As such, the EK and its certificate could be construed to be privacy sensitive. Thus, if protection of privacy is important to the TPM owner, then the EK and EK certificate should not be considered public, and should be available only to those entities which are trusted by the TPM owner.

By design, the EK is very limited in its uses. In particular, it can be used to decrypt the TPM_EK_BLOB, described in the enrolment protocol above. This means that an alternate key pair which can be used by the TPM to transact or communicate with the external world is desired. This alternate “identity” key pair is the Attestation Identity Key (AIK), which is an RSA key pair located within the TPM key hierarchy under the Storage Root Key (SRK).

An AIK is linked to an EK during AIK certificate enrolment, raising privacy concerns under some circumstances. In order to address the potential privacy issues arising from the use of an AIK key pair, the TCG adopts the following in its AIK design philosophy:

- Multiple AIKs. In order to reduce the possibility that an AIK can be used to identify a platform whose owner wishes to remain anonymous, a TPM is permitted to have any number of AIK key pairs and AIK certificates (subject to available resources). In theory, for each external entity with whom the TPM transacts, a separate AIK key pair and certificate could be used by the platform. In order to prevent services on the Internet from recognizing returning platforms, a unique AIK key pair could be created by the platform owner for each transaction.
- Issuance of an AIK certificate by an Attestation CA. The ACA is a trusted third party that performs the role of issuing AIK certificates to a given TPM-enabled platform. The core function of the ACA is to vouch for the TPM-enabled platform by issuing AIK certificates containing security assertions regarding the platform and the associated AIK. When a TPM-enabled platform requests an AIK certificate from the ACA, the platform must include a copy of the EK-certificate in the enrolment process. The ACA validates the EK-certificate, and may be expected to treat the EK-certificate as private information pertaining to the TPM. As such, the ACA may be trusted by the TPM Owner to never to reveal the EK certificate, or any information about the binding between the AIK and EK. The act of issuing an AIK certificate based on the received EK certificate provides some degree of "blinding" or indirection over the true EK certificate.

12.2 Device Enrolment

The enrolment policy for new devices will rely upon binding the device to the receiving organisation, which shall already possess credentials at the desired LoA. The number, provenance and accuracy of attributes bound to the DeviceID will vary by LoA.

The enrolment process for existing devices will be at least as strong as the process for new devices. At higher LoAs this may not be possible and, instead, require new devices whose manufacture and history can be assured.

12.3 Threats to Device IPV

The primary threats to device enrolment include:

- Subversion of the ordering process by an untrusted third party.
- Collusion and impersonation in the manufacture of a platform that contains devices, such as TPM.

12.4 Controls for Device IPV

Table 9 identifies the controls that are appropriate to each LoA.

Threats	Controls	Required controls			
		LoA1	LoA2	LoA3	LoA4
Impersonation	IPV: PolicyAdherence		#1	#1	#1
	IPV: Procurement		#2	#2	#2
	IPV: AuthoritativeInformation		#4	#5	#6
Collusion	IPV: SecureManufacture			#7	#7

Table 9 - Controls for Device Enrolment

Note – In the above table, the identifiers #1 - #6 correspond to the specific controls required to provide protection at each LoA. The following controls against enrolment phase threats correspond to #1 - #6 listed in Table .

IPV: PolicyAdherence

#1. Publish the IPV policy, and perform all IPV in accordance with the published IPV policy.

IPV: Procurement

#2. The Accountable Person or other responsible person shall authorise the procurement of a device at a specified LoA from a trusted manufacturer or its agent. All organisations shall possess OrgIDs at the required LoA or higher, in accordance with this International Standard.

IPV: AuthoritativeInformation

#3. For the LoA requested for the DeviceID, the Accountable Person and other responsible persons in each organisation shall possess a personal credential at the same as LoA or higher, and be able to authenticate with it to the Authoritative Source.

#4. The following controls apply:

- All controls from #3
- In addition:
    - The manufacturer shall confirm the order and, prior to delivery, provide the full details of the devices, including:
        - Manufacturers serial number, date of manufacture, place of manufacture
        - Key components and cryptography, their manufacturers and serial numbers
    - The receiving organisation shall confirm receipt of the devices, by serial number, and their incorporation in the organisation's asset register for accounting and network management purposes. Once configured by the organisation, it may then be activated for use.
    - Where applicable, the MAC address, fixed Internet Protocol address, IMEI and SIM card number shall be recorded and managed.

#5. The following controls apply:

- All controls from #4.
- In addition:
    - Where TPM is required,
        - The manufacturer shall provide and maintain a bill of materials for the device and its operating software via a secure and automated means.
        - The receiving organisation shall be able to operate TPM in Enterprise Mode, i.e. where the device TPM is managed at the enterprise level under the control of the owning organisation.
        - Monitoring shall occur after deployment.
    - Where TPM is not required, the device authentication technology shall be such that the same functionality shall exist as if it were a TPM to the extent that the alternative technology does not present any additional security or operational risks.

#6. The following controls apply:

- All controls from #5.
- In addition:
    - Only TPM shall be used.
    - For activation, TPM shall be deployed in Enterprise Mode, with the ability to access securely a 'Last Known Good' reference of the BIOS and operating system. When a TPM device is switched on, it shall be able to access the reference (locally or remotely) and match the reference to the internal BIOS and operating system to ensure that neither has been subverted. If this is successful, it should then be able to connect to the network and complete activation or registration with the receiving organisation, sufficient to operate.

IPV: SecureManufacture

#7. The following controls apply:

- The manufacturer shall be certified to manufacture, configure and enrol TPM devices in accordance with the TCG Infrastructure Working Group A: CMC Profile for AIK Certificate Enrollment Version 1 and other documents specified by TCG.

13 Software IPV

Separate multinational discussions are taking place on software IPV that will inform this Clause. SCAP remains an important specification for reference. This Clause will be completed in WD3.

14 Management and organizational considerations

EAA comes not from technical factors alone, but also from regulations, contractual agreements, and consideration of how the service provision is managed and organized. A technically rigorous solution without competent management and operation can fall short of its potential for providing security in the provision of EAA.

14.1 Service establishment

Service establishment addresses both the legal status of the service provider and the status of the functional service provision. For instance, knowing that the provider of identity management and authentication services is a registered legal entity gives confidence that the IPVSP is a bona fide enterprise in the jurisdiction within which it operates. This becomes more significant when service components are operated by different legal entities (e.g., registration as a separate function).

Although the basic requirements are the same for all LoAs, the higher LoAs should have greater dependency on the service provision being complete and reliable. For instance, at LoA3 and above, greater assurance about the service provision should also be taken from knowledge of its corporate ties and understanding of the level of independence it is permitted in its operations.

14.2 Legal and contractual compliance

All enrolment actors 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 A). Account should be taken of all jurisdictions within which actors operate. At LoA2 and higher, specific policy and contractual requirements should also be identified.

CSPs, RAs and IPVSPs 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 services 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.

14.3 Financial provisions

Where long-term availability of services is a consideration in both an entity's and relying parties' expectations, financial stability should be shown, sufficient to ensure the continued operation of the service and to underwrite the degree of liability exposure being carried. For LoA1 services and reliance, such provisions are unlikely to be a consideration, whereas services supporting more significant transactions at LoA2 and higher should address such needs.

14.4 Governance - Information security management and audit

At any LoA, where IPV and credential issuance 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; or,
- In 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 trust model shall require a collaborative governance and agreed common policy.

At LoA2 and higher, enrolment processes and actors shall have in place documented information security management practices, policies, approaches to risk management, and other recognized controls, 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. For Consumer identities, include PCI DSS. For LoA 3 and higher, this assurance shall be supported by security audits as described. An audit can be used by relying parties to check that parties' practices are in line with what has been agreed. Dispute resolution services may be used for disagreements.

14.5 External service components

When an organisation is dependent upon third parties for parts of its service, how it directs the actions of these parties and oversees them will contribute to the overall assurance of the service provision. The nature and extent of the arrangements should be proportional to the required LoA and to the information security management system being applied. At LoA1, such assurance should have minimal effect, but from LoA2 and up, these measures contribute to the overall assurance being given.

14.6 Trust Frameworks

To enable large-scale communities of trust, operational infrastructures require a trust framework based on common policy. In a trust framework, the actors support the information flow among one another. Depending on the agreements, additional actors may be called on to ensure that all actors are abiding by commitments and may provide an avenue for redress in the event they are not. IPV underpins any trust framework.

Policy makers set out the technical and contractual requirements for trust frameworks. As they establish these requirements, policy makers should include criteria by which potential trust framework entities can be measured. Rather than developing the criteria themselves, policy makers may wish to draw on standard criteria that experts have already elaborated, such as this International Standard. The more policy makers use standard criteria across different trust frameworks, the easier it will be for entities to understand and apply the criteria consistently. Moreover, named sets of criteria can serve as shorthand to indicate different degrees or types of rigour in requirements or capabilities at various LoAs.

15 Service assurance criteria

Trust framework operators that seek to comply with this International Standard shall establish specific criteria fulfilling the requirements of each LoA that they intend to support and shall assess the IPVSPs that claim compliance with this International Standard against those criteria. Likewise, IPVSPs shall determine the LoA at which their services comply with this International Standard by evaluating their overall business processes and technical mechanisms.

Annex A - Privacy and protection of PII

(This annex does not form an integral part of this International Standard)

The suitability of a particular authentication approach for a particular use will depend not only on an assessment of authentication effectiveness, but also on the risks and risk tolerance of the organizations involved. Misuse or lack of adequate protection of the PII of entities and principals entails significant risks for organizations, ranging from reputational damage to liability exposure. The use of PII for authentication purposes and its protection, therefore, needs to be carefully weighed and considered. This section provides informative guidance relating to some of the privacy considerations organizations should take into account when deciding on the use and implementation of a particular authentication approach.

Where entities are individuals, the majority of authentication approaches will involve processing and storage of PII during one or more of the following:

a) During the enrolment process when collecting, proofing, and verifying identity and other information relating to entities;

b) During the creation, issuance, and management of credentials of entities;

c) During the use of credentials by the entity and their verification by relying parties and verifiers.

It is possible to have strong authentication and strong privacy. There exist many cryptographically strong authentication approaches which have limited negative impact on privacy (e.g., anonymous credentials, group signatures). Additionally, it should be noted that the increased strength of the assurance level (e.g., LoA4 versus LoA2) can, but does not necessarily need to, adversely affect the privacy of an individual. Much will depend on the chosen authentication approach and how it is implemented. In making these decisions, every organization should carefully consider the need to protect the PII of entities, in addition to the needs of protecting their resources and holding entities accountable in case of unauthorized activities.

The majority of authentication approaches involve the use of distinguishing identifiers to unambiguously distinguish an entity from other possible entities in the context of an authentication. Use of distinguishing identifiers is often also necessary for a variety of other purposes, such as account management and the maintenance of an appropriate audit trail. The main privacy concerns relating to the use of distinguishing identifiers do not relate to the usage of a distinguishing identifier as such, but rather to the reuse of the same identifier in many different settings. For example, an account number assigned for a single purpose is generally considered to be less sensitive than a government administrative reference used for multiple purposes (e.g., taxation, healthcare, retirement). In certain jurisdictions, there may also be legislation restricting the use of certain identifiers.

In light of the previous considerations, organizations should implement effective safeguards to protect the PII of entities in the phases and processes described in this EAAF. In particular, the chosen authentication approach should be designed and implemented in a way that generally minimizes the processing of PII. In addition, the use of distinguishing identifiers that are also used in other contexts or domains should be restricted to instances where it is necessary to use them and the laws of the relevant jurisdiction(s) allow it.

Additional ISO/IEC guidance for the protection of PII can be found in two sources:

a) ISO/IEC 29100 describes basic privacy requirements in terms of three main factors: (1) legal and regulatory requirements for the safeguarding of the individual's privacy and the protection of his/her PII, (2) the particular business and use case requirements, and (3) individual privacy preferences of the PII entity. ISO/IEC 29100 describes the following basic privacy principles: Consent and Choice, Purpose Specification, Collection Limitation, Use, Retention and Disclosure Limitation, Data Minimization, Accuracy and Quality Openness, Transparency and Notice, Individual Participation and Access, Accountability, Security Controls, and Compliance. In addition to performing a risk assessment to analyze for threats, organizations should conduct a privacy impact assessment of their authentication approach to assess which components of their systems will require specific attention in terms of privacy protection measures.

b) ISO/IEC 29101 provides an architectural framework for ICT systems that process PII. This architecture framework is expressed in concerns and several architectural views. A set of components is provided for implementing ICT systems processing PII. The framework is meant to be used to construct system architectures that follow the privacy principles addressed in ISO/IEC 29100.

For detailed guidance on requirements, principles, and system design with regard to protection of PII, the reader is referred to the above standards.

Annex B - Evidence of Identity – Example Documents

(This annex forms an integral part of this International Standard)

Document	Online Evidence	Physically Supplied Evidence
Identity Category - Citizen		
Government issued document evidence with a biometric and security features that can be validated	Primary	Primary
National passport	Primary	Primary
ID card with biometric	Primary	Primary
Foreign passport with visa or residence permit	Primary	Primary
National biometric residence card for foreign workers and visitors	Primary	Primary
National Birth Certificate	Secondary	Secondary
National Government Travel Document/certificate of travel	Secondary	Secondary
National Vehicle Registration certificate	Secondary	Secondary
National Vehicle Licence renewal notification	Secondary	Secondary
National Adoption Certificate	Secondary	Secondary
National Asylum Seekers Registration Card	Secondary	Secondary
National Naturalisation or Registration Certificate	Secondary	Secondary
National Marriage/Civil Partnership certificate	Secondary	Secondary
Foreign ID Card	Secondary	Secondary
National Military ID card	Secondary	Secondary
Expired Passport	Secondary	Secondary
Foreign Birth certificate	Secondary	Secondary
Police registration of firearms certificate	Secondary	Secondary
National Government issued employee ID card	Secondary	Secondary
National Tax and employment data from government	Secondary	Secondary
Driving Licence	Secondary	Secondary
Divorce – decree absolute, decree nisi	Secondary	Tertiary
Dissolution of Civil partnership	Secondary	Tertiary
Identity Category - Money		
Bank account	Primary	Secondary
Building Society account	Secondary	Tertiary
Credit Reference Agency supplied evidence	Secondary	Tertiary
Student loans	Secondary	Tertiary
Bank Loans	Secondary	Tertiary
Credit cards	Secondary	Tertiary
Current charge card	Secondary	Tertiary
Closed accounts - Loan	Secondary	Tertiary
Store cards	Secondary	Tertiary
Current charge card	Secondary	Tertiary
Home credit	Secondary	Tertiary
Statement – bank/credit card/building society/credit union/ mortgage	Secondary	Tertiary
Current/open saving account book	Secondary	Tertiary
Identity Category - Living		
Mortgage account	Secondary	Tertiary
Land Registry Record	Secondary	Tertiary
Closed accounts – mortgage	Secondary	Tertiary
Life insurance	Secondary	Tertiary
Home insurance	Secondary	Tertiary
Car insurance	Secondary	Tertiary
Utility – Gas	Secondary	Tertiary

Utility – Electric	Secondary	Tertiary
Utility – Water	Secondary	Tertiary
Utility – Satellite TV	Secondary	Tertiary
Utility – Cable	Secondary	Tertiary
Utility – Home telephone	Secondary	Tertiary
Utility – Mobile contract	Secondary	Tertiary
TV Licence	Secondary	Tertiary
Court Records	Secondary	Tertiary
Evidence from a trusted source that independently corroborates an Internet based identity, its history of activity and its timeliness	Secondary	Tertiary

Annex C - Attributes for Organisation Identity - Categories 1 and 2

The attributes are shown as a list and not as hierarchy or taxonomy.

Every attribute would be date/time stamped. Against each attribute is also recorded the issuing authority, the Level of Assurance of the attribute assertion and the date it was last validated with an Authoritative Source (normally the Issuing Authority). Some attributes will require regular validation within timeframes specified in the Common Policy for the LoA.

Approach.

- Category 1. Establish the Organisation Type then select the appropriate list of attributes to be provided for the organisation.
- Category 2. Provide the attributes for Authority to Act.

1. Category 1

Organisation Type (these may subdivide further). Each nation should provide its own list of types of organisation. Below is an **example** based on a European country.

- Unlimited Partnership,
- Limited Liability Partnership (LLP),
- Private Limited Liability Company,
- Public Limited Liability Company (Plc),
- European Companies (Societas Europaea),
- Foreign companies with overseas branches registered in England and Wales.
- Company Limited by Guarantee
- Unlimited Company
- Receivers, Liquidators, Administrators, Supervisors, Public Guardian and trustees in bankruptcy.
- Credit Union and Industrial & Provident Society
- FSA Mutual Fund, Provident Society, Mutual Society
- Corporation Sole
- Sole Trader
- Companies incorporated by Royal Charter
- Lloyd's Syndicate
- Ecclesiastical Bodies, Churches and other religious groups and organisations.
- Trusts and Estates and Charities, Schools, Universities, Examination Boards, Voluntary Organisations & Pension Schemes of which some are unincorporated and others have special status.
- Charitable Incorporated Organisation (proposed)
- Government Owned, Company Operated (GOCO) organisations
- Miscellaneous bodies established by or accountable to Government, county and local authorities, Government departments and agencies, Secretaries of State,
- The Royal Household and the Services
- Foreign Embassies, Consulates and High Commissions
- The Courts System including its judges, bailiffs, sheriffs and other officers
- The Police and emergency services

If the Organisation Type is a Company.

- At initial enrolment (for permanent record):
  - Country of Registration
  - Registered Company Name
  - Registered Office Address
  - UPRN of registered address (if UPRN exists)
  - Registered Company Number
  - Legal Status
  - Date of Incorporation

  - Company Type
  - VAT Number (or equivalent)
  - Legal Entity Identifier (if applicable)
  - Accountable Person Name and additional details, including company email address, digital signature and public encryption key
  - Directors Names and additional details, including company email address, digital signature and public encryption key
  - Primary Beneficiaries' Names and additional details
  - Company domain names and WHOIS registration data
  - Company primary bank account details
  - Level of Assurance requested
  - Level of Assurance granted

- Operational data maintained in accordance with policy and Level of Assurance
  - Country of Registration
  - Registered Company Name
  - Registered Office Address
  - UPRN of registered address (if UPRN exists)
  - Registered Company Number
  - Legal Status
  - Company Type
  - VAT Number (or equivalent)
  - Legal Entity Identifier (if applicable)
  - Accountable Person Name and additional details
  - Directors Names and additional details
  - Primary Beneficiaries' Names and additional details
  - Company domain names and WHOIS registration data
  - Company primary bank account details
  - Level of Assurance
  - Level of Assurance Status (operational, suspended, revoked)
  - Identity Provider
  - Credential Service Provider
  - Trust Scheme
  - Scheme-certified Trust Auditor

If Organisation Type is a Charity / Trust / Provident / Mutual Society

- At initial enrolment (for permanent record):
  - Country of Registration
  - Registered Charity / Trust / Provident / Mutual Society Name
  - Registered Office Address
  - UPRN of registered address
  - Registered Charity / Trust / Provident / Mutual Society Number
  - Legal Status
  - Date of Incorporation
  - VAT Number (or equivalent)
  - Legal Entity Identifier (if applicable)
  - Accountable Person Name and additional details
  - Directors Names and additional details
  - Primary Beneficiaries' Names and additional details
  - Organisation domain names and WHOIS registration data
  - Organisation primary bank account details
  - Corporate liability insurance provider and account number (if applicable)
  - Level of Assurance requested
  - Level of Assurance granted

- Operational data maintained in accordance with policy (e.g. Level of Assurance)
    - Country of Registration
    - Registered Charity / Trust / Provident / Mutual Society Name
    - Registered Office Address
    - UPRN of registered address
    - Registered Charity / Trust / Provident / Mutual Society Number
    - Legal Status
    - Date of Incorporation
    - VAT Number (or equivalent)
    - Legal Entity Identifier (if applicable)
    - Accountable Person Name and additional details
    - Directors Names and additional details
    - Primary Beneficiaries' Names and additional details
    - Organisation domain names and WHOIS registration data
    - Organisation primary bank account details
    - Corporate liability insurance provider and account number (if applicable)
    - Level of Assurance
    - Level of Assurance Status (operational, suspended, revoked)
    - Identity Provider
    - Credential Service Provider
    - Trust Scheme
    - Scheme-certified Trust Auditor

If Organisation Type is a Sole Trader

- First name
- Middle name
- Last name
- Date of Birth
- Place of Birth
- Home Address
- Home UPRN (if UPRN exists)
- Known Aliases
- Nationality or nationalities
    - If a national citizen, the National ID Number or similar
    - If foreign or a dual national, the National ID Number of each citizenship
- Passport issuing authority
- Passport number, expiry date and remaining Machine Readable Zone data (ISO 3166-1 alpha-3).
- Primary telephone number
- Secondary telephone number
- Email address
- Associated entities – company registered name, registered number, country
- VAT Number (or equivalent)
- Legal Entity Identifier (if applicable)
- Organisation domain names and WHOIS registration data
- Organisation primary bank account details
- Corporate liability insurance provider and account number (if applicable)
- Level of Assurance
- Level of Assurance Status (operational, suspended, revoked)
- Identity Provider
- Credential Service Provider
- Trust Scheme
- Scheme-certified Trust Auditor

If Organisation Type is a Government Department / Agency:

- Country
- Department / Agency Name
- Registered Office Address
- UPRN (if UPRN exists)
- Accountable Person Name
- Accountable Person Appointment
- Primary telephone number
- Secondary telephone number
- Email address, digital signature and public encryption key
- Level of Assurance
- Level of Assurance Status (operational, suspended, revoked)
- Identity Provider
- Credential Service Provider
- Trust Scheme
- Scheme-certified Trust Auditor

Responsible Person (e.g. Director, Trustee) Details:

- First name
- Middle name
- Last name
- Date of Birth
- Place of Birth
- Home Address
- Home UPRN (if UPRN exists)
- Known Aliases
- Nationality or nationalities
    - If a national citizen, the National ID Number or similar
    - If foreign or a dual national, the National ID Number of each citizenship
- Passport issuing authority
- Passport number, expiry date and remaining Machine Readable Zone data.
- Appointment(s) in the organisation
- Work telephone number
- Home telephone number
- Email address
- Associated companies – company registered name, registered number, country
- Associated Charity / Trust / Provident / Mutual Society - registered name, registered number, country

Prime Beneficiaries Details:

- If the beneficiary is an organisation, the organisation itself must already be registered in ROO
    - ROO OrgID
- If the beneficiary is a person
    - Beneficiary First name
    - Beneficiary Middle name
    - Beneficiary Last name
    - % shareholding
    - Beneficiary Date of Birth
    - Place of Birth
    - Home Address
    - Home UPRN (if available)

- Known Aliases
- Nationality or nationalities
  - If a national citizen, the National ID Number or similar
  - If foreign or a dual national, the National ID Number of each citizenship
- Passport issuing authority
- Passport number, expiry date and remaining Machine Readable Zone data.
- Primary telephone number
- Secondary telephone number
- Primary email address
- Associated companies – company registered name, registered number, country
- Associated Charity / Trust / Provident / Mutual Society - registered name, registered number, country

2. Category 2 – Authority to Act

- ROO OrgID
- Appointment(s) in the organisation
- First name
- Middle name
- Last name
- Date of Birth
- Place of Birth
- Home Address
- Home UPRN (if UPRN exists)
- Known Aliases
- Nationality or nationalities
  - If a national citizen, the National ID Number or similar
  - If foreign or a dual national, the National ID Number of each citizenship
- Passport issuing authority
- Passport number, expiry date and remaining Machine Readable Zone data.
- Work telephone number
- Home telephone number
- Work email address
- Associated companies – company registered name, registered number, country
- Digitally signed mandate evidencing the authority to act, signed by either the organisation's Accountable Person or a Responsible Person (e.g. Director, Trustee)

Annex D - Bibliography

(This annex forms an integral part of this International Standard)

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/e-government/security-and-authentication/authentication-framework.html

[2] Australian Government Gatekeeper Public Key Infrastructure http://www.gatekeeper.gov.au/

[3] 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/

[4] ITU-T Focus Group: Report on Identity Management Report 6 Framework for Global Interoperability http://www.itu.int/ITU-T/studygroups/com17/fgidm/

[5] ITU-T Report on the Definition of the Term "Identity", April, 2008 http://www.itu.int/ITU-T/jca/idm/

[6] Kantara Initiative Identity Assurance Framework v2.0, http://kantarainitiative.org/confluence/display/GI/Identity+Assurance+Framework+v2.0

[7] New Zealand Standard: *Evidence of Identity (EOI)* June 2006 http://www.dia.govt.nz/diawebsite.nsf/wpg_URL/Resource-material-Evidence-of-Identity-Standard-Evidence-of-Identity-Standard-(html-version)?Open Document

[8] 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

[9] 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

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

[11] OMB M-04-04, *e-Authentication Guidance for Federal Organization* http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

[12] Principles for Electronic Authentication: A Canadian Framework, http://strategis.ic.gc.ca/epic/site/ecic-ceac.nsf/en/h_gv00240e.html

[13] 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.

[14] A. Menezes, P. van Oorschot, S. Vanstone, 'Handbook of Applied Cryptography', 1997, p. 3-4. http://www.cacr.math.uwaterloo.ca/hac/.

[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.2702 (2010), Next generation network authentication and authorization requirements.

[18] ITU-T Recommendation Y.2720 (2010), Next generation network identity management framework.

[19] ITU-T Recommendation Y.2721 (2010) NGN identity management requirements and use cases.

[20] ITU-T Recommendation Y.2722 (2010) NGN identity management mechanisms.

[21] ISO/IEC 9798:2010, Information technology – Security techniques – Entity authentication.

[22] ISO/IEC 19792:2009, Information technology – Security techniques – Security evaluation of biometrics.

[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 24760-1:2011, Information technology -- Security techniques – A framework for identity management -- Part 1: Terminology and concepts.

[27] ISO/IEC 19790: 2012, Information technology -- Security techniques – Security requirements for cryptographic modules.