Draft ETSI TS 119 461 V0.0.5 (2020-12)

Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects

Send comments ONLY to E-SIGNATURES_COMMENTS@list.etsi.org

Download the template for comments:

https://docbox.etsi.org/ESI/Open/Latest_Drafts/Template-for-comments-TS119461.doc

Reference
DTS/ESI-0019431-2

Keywords
electronic signature, security, trust services

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

The present document covers policy and security requirements for trust service components for identity proofing of trust service subjects. Currently, identity proofing is not defined as a trust service on its own but rather as a component of other trust services. This component can be provided as an integral part of a trust service by the trust service provider itself, or by a separate service provider acting as a sub-contractor to the trust service provider. Such a separate identity proofing service provider may provide its services to several trust service providers and services.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

The present document specifies policy and security requirements for TSP service components providing identity proofing for trust service subjects. Such a service component may be an integral part of a TSP's service or it may be a separate service that provides identity proofing to several trust services as well as for other purposes such as issuing of electronic identity or onboarding of customers e.g. for financial services. The term service component is used because identity proofing is at the time of writing not defined as a separate trust service.

These requirements are based on the general policy requirements specified in ETSI EN 319 401 [1] and on established best practice for use of selected means that can be used for identity proofing processes.

Introduction

Identity proofing is the process of verifying with the required degree of certainty that the identity of an applicant is correct. The scope of this specification is proof the identity of applicants to qualified and non-qualified trust services. This specification can be applicable also in other areas such as issuing of electronic identity (eID) and know-your-customer (KYC) processes in various industries.

Identity proofing is provided by an Identity Proofing Service Provider (IPSP) as an Identity Proofing Service Component (IPSC) supporting trust services. The primary target of this specification is to specify policy and security requirements that enable an IPSP to specify its IPSC in a way that enables Trust Service Providers (TSP) to make use of the IPSC, specifically for services as set out in TSP policy standards such as ETSI EN 319 411-1/-2, ETSI TS 119 431-1, and ETSI EN 319 521.

This specification defines best practice requirements for identity proofing as follows:

- General requirements on identity proofing service management and operation based on the requirements of ETSI EN 319 401.
- Identity proofing service requirements and specific requirements for selected identity proofing means covering applicable technologies.
- Requirements on the process and how to combine means into identity proofing processes.

Some specific contexts might require additional requirements, such as the EU specific requirements related to identity proofing resulting from Regulation (EU) No 910/2014; this is covered by annexes to this specification.

1 Scope

The present document provides policy and security requirements for trust service providers (TSP) implementing a service component supporting identity proofing.

The present document gives no restrictions on the type of TSP implementing such a service component.

The present document aims at supporting identity proofing in European and other regulatory frameworks.

NOTE 1: Specifically, but not exclusively, the present document aims to support trust services as defined in Regulation (EU) No 910/2014 [i.1]. Annexes indicates how to use the present sepcifications in the context of Regulation (EU) No 910/2014.

The present document may be used by competent bodies as the basis for confirming that an organization is trustworthy in its identity proofing service.

NOTE 2: See ETSI EN 319 403 [i.6] for guidance on assessment of TSP processes and services.

The present document identifies specific controls needed to address specific risks associated with services providing identity proofing.

This present document is suitable for issuing of certificates at the NCP/QCP policy levels defined by ETSI EN 319 411-1 and ETSI EN 319 411-2 for similar policies for other trust services. Annexes indicates how to use the present sepcifications in conjunction with these policies.

This specification does not target identity proofing with low level of confidence. The specification also does not target identity proofing at the level needed for issuing of national identity documents such as passports and national ID cards; requiring similar policy and security requirements for identity proofing in general is not realistic.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] ETSI EN 319 401: “Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers”.

[2] ISO/IEC 30107-1: “Information technology — Biometric presentation attack detection – Part 1: Framework”.

[3] ISO/IEC 30107-3: “Information technology — Biometric presentation attack detection – Part 3: Testing and reporting”.

[4] ISO/IEC 19795-1: “Information technology – Biometric performance testing and reporting – Part 1: Principles and framework”.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Regulation (EU) 910/2014 of the European parliament and of the council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[i.2] Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

[i.3] Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

[i.4] ETSI TR 119 001: “Electronic Signatures and Infrastrutures (ESI); The framework for standardization of signatures; Definitions and abbreviations”.

[i.5] ETSI EN 319 403: “Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers”.

[i.6] ETSI EN 319 411-1: “Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements”.

[i.7] ETSI EN 319 411-2: “Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates”.

[i.8] ETSI TS 119 431-1: “Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev”.

[i.9] CEN EN 419 241-1: “Trustworthy systems supporting server signing – Part 1: General system security requirements”.

[i.10] ETSI EN 319 521: “Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Delivery Service Providers”.

[i.11] ICAO Doc 9303: “Machine Readable Travel Document – Part 10: Logical data structure (LDS) for storage of biometrics and other data in the contactless integrated circuit (IC)”.

[i.12] ENISA: “Analysis of Methods to carry out identity proofing remotely” (to be published spring 2021).

[i.13] ISO/IEC 19989-3: “Information security – Criteria and methodology for security evaluation of biometric systems – Part 3: Presentation attack detection”.

3 Definition of terms, abbreviations and notations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TR 119 001 [i.6], ETSI EN 319 401 [1] and the following apply:

applicant: person (legal or natural) whose identity is to be proofed to become subject or subscriber (of a trust service)

authoritative evidence: evidence that holds identifying attribute(s) that are managed by an authoritative party / source

NOTE 1: This is one type of evidence of identity.

NOTE 2: Source ISO 29003

authoritative source: any source irrespective of its form that can be relied upon to provide accurate data, information and/or evidence that can be used to prove identity

NOTE: Source eIDAS [i.1]

attribute: a quality or characteristic ascribed to someone or something.

attribute evidence: information linking an attribute, or a series of attributes, to an entity e.g. a legal or natural person (see also **identity evidence** below)

NOTE: attribute evidence may be either physical (documentary) or purely digital, or a digital representation of physical attribute evidence (e.g., a digital representation of a paper or plastic driver's license) (see FATF Digital Identity Guidance March 2020).

eID (short form for **electronic identification means):** a material and/or immaterial unit containing person identification data, and which is used for authentication for an online service.

enrolment (registration): The process through which an applicant applies to become a subject or a subscriber of a trust service.

(identity) evidence: Information or documentation provided by the ***applicant*** or obtained from other sources to support the claimed identity.

false acceptance rate: measure of the likelihood that a biometric security system will incorrectly accept an access attempt by an unauthorized user.

false rejection rate: measure of the likelihood that a biometric security system will incorrectly reject an access attempt by an authorized use.

identity: attribute or set of attributes that uniquely describe an entity within a given context.

identity proofing context: the external requirements affecting the identity proofing process, given by the purpose of the identity proofing with related regulatory requirements and the acceptable risk regarding the result of the identity proofing process.

identity proofing: the process by which a (trust) service provider collects and validates information about an applicant and verifies that so collected and validated information actually belongs to the applicant.

identity proofing policy: an identity proofing policy describes the promised level of assurance, the jurisdiction and the applicable legislation, the intended usage, a description of the process, the attributes which are confirmed, eligible evidence, records retention period, etc.

identity provider: entity that makes available identity information

person identification data: set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established.

NOTE: Source eIDAS [i.1]

relying party: means a natural or legal person that relies upon an electronic identification or a trust service.

subject: a person (or organization, device, hardware, network, software, or service) that is enrolled to a trust service.

subscriber: legal or natural person bound by agreement with a trust service provider to any subscriber obligations.

(attribute) validation: the part of identity proofing process that involves determining that an evidence is genuine (not counterfeit or misappropriated) and that the information the evidence contains is accurate.

pseudonym: a name other than a “legal” name.

trusted information source: a register or other source of information that the IPSP can access based on attributes previously collected in the identity proofing process, and where the applicant is not involved in the access

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TR 119 001 [ref.] and the following apply:

APCER	Attack Presentation Classification Error Rate
BPCER	Bona fide Presentation Classification Error Rate
CA	Certification Authority
eID	Electronic Identification Means
eMRTD	Electronic Machine Readable Travel Document
FAR	False Acceptance Rate
FRR	False Rejection Rate
IPSC	Identity Proofing Service Component
IPSP	Identity Proofing Service Provider
LoA	Level of Assurance
LoIP	Level of Identity Proofing
LCP	Lightweight Certificate Policy
MRZ	Machine Readable Zone
NCP	Normalized Certificate policy
QCP	Qualified Certificate Policy
TSP	Trust Service Provider

3.3 Notation

The requirements identified in the present document include:

a) requirements applicable to any TSP conforming to the present document. Such requirements are indicated by clauses without any additional marking;

b) requirements applicable under certain conditions. Such requirements are indicated by clauses marked by "[CONDITIONAL]".

c) requirements applicable for an enhanced level. Such requirements are indicated by clauses marked by "[ENHANCED]".

The requirements in the present document are identified as follows:

<the 3 letters identifying the elements of services > **-** < the clause number> **-** <2 digit number - incremental>

The elements of services are:

- **OVR:** General requirement (requirement applicable to more than 1 component)
- **COL**: Requirements on attribute and evidence collection

- **VAL**: Requirements on attribute and evidence validation
- **BIN**: Requirements on binding to applicant
- **PRO**: Requirements on identity proofing processes

The management of the requirement identifiers for subsequent editions of the present document is as follows:

- When a requirement is inserted at the end of a clause, the 2 digit number above is incremented to the next available digit.
- When a requirement is inserted between two existing requirements, capital letters appended to the previous requirement identifier are used to distinguish new requirements.
- The requirement identifier for deleted requirements are left and completed with "VOID".
- The requirement identifier for modified requirement are left void and the modified requirement is identified by capital letter(s) appended to the initial requirement number.

4 Identity proofing process overview

4.1 Overview

Identity proofing is the process of proving with the required degree of certainty that a person (the applicant) claiming an identity is the correct person. A person may be a natural person, a legal person, or a natural person representing a legal person.

An identity proofing process can be carried out by physical presence of the applicant or remotely by communication with the applicant using a communications network. An identity proofing process can be carried out by a human operator, or be automated, or a combination of human controlled and automated.

The required degree of certainty is determined by the **identity proofing context**. The context is given by:

- The purpose of the identity proofing (e.g. for enrolment to a trust service),
- Any regulatory environment that the identity proofing process must comply with,
- The acceptable risk regarding the result of the identity proofing process.

The identity proofing context will influence all aspects of identity proofing, e.g. the identity attributes to collect, the freshness of the attribute values (at which time they were assessed to be correct), and the types of evidence accepted or even mandated. The identity proofing context will need to be reflected in policy requirements, with identity proofing processes fulfilling the contextual requirements defined in practice statements.

Identity proofing is done for a purpose, which in this specification is assumed to be enrolment for a trust service. The TSP may subcontract identity proofing to an identity proofing service provider (**IPSP**). Since the IPSP carries out its tasks as a part of the trust service provider's service, the IPSP's service is defined as an identity proofing service component (**IPSC**).

NOTE: The definition of an IPSC as a service component can apply also for other contexts than trust services, e.g. issuing of eID or KYC for a service provider.

This specification defines policy and security requirements for an IPSC as follows:

- General requirements to the IPSP based on the requirements of ETSI EN 319 401 [1].
- Specific security and policy requirements for the IPSC.

When the applicant is a natural person, identity proofing processes covered by this specification require the applicant to produce one or more of the following evidences:

- A physical or digital identity document,
- An eID that can be used to authenticate the applicant,
- A digital signature supported by a certificate that identifies the applicant.

A digital signature can also be used as evidence when the applicant is a legal person.

An identity document is preferably an official, national document such as a passport or national identity card but can be another type of document depending on the identity proofing context. Regarding digital identity document, this specification currently only considers eMRTD according to ICAO 9303 [i.13].

Identity proofing processes covered by this specification can use additional evidences to enhance the confidence of the identity proofing or to obtain evidence for additional identity attributes. The following types of additional evidence are covered by this specification:

- Trusted information sources that are accessed by the IPSP without involvement of the applicant,
- Documents and attestations provided by the applicant,
- Proof of possession provided by the applicant.

Trusted information sources can be official registers, but also existing customer records or other sources that are considered reliable for the identity proofing context. Trusted information sources and documents and attestations can be used both for natural and legal persons and for a natural person representing a legal person to provide evidence for identity attributes including authorizations.

Examples of proof of possession are bank account or credit card, mobile phone number, or email address. Proof of possession can evidence the specific attribute, e.g. the phone number of the applicant, but can also be used to obtain evidence for further attributes, e.g. from the applicant's bank related to the verified account.

4.2 Identity proofing process

The components of an identity proofing process are shown in the figure below (from [i.14]).

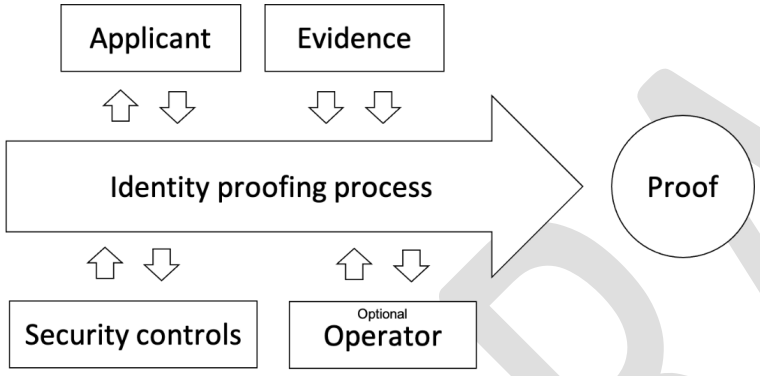

Figure 1: Components of an identity proofing process

The applicant is identified by a set of identity attributes, and evidence is provided to link these attributes to the applicant. The identity proofing process, which can be carried out automated, by a human operator, or by a combination of human controlled and automated, is commonly broken down into three tasks:

1. Attribute and evidence collection,
2. Attribute and evidence validation,
3. Binding to applicant.

Attribute and evidence collection specify the attributes constituting the identity to be proven and the evidence(s) required to prove the identity. Attribute and evidence validation cover the processes to validate that presented evidence is genuine and valid, and that the attributes collected are verified by the evidence. Binding to applicant consists of the process to ensure that the person presenting the evidence really is the person identified by the evidence.

The tasks are not necessarily carried out as consecutive steps of an identity proofing process. For some processes, they can be intertwined, e.g. that attributes are collected from an identity document integral to the validation of the same document. The identity proofing process is preceded by an **initiation** where the applicant is presented with the terms and conditions, and is concluded by the **issuing of proof.**

The process can be illustrated by the figure below (from [i.14]), showing also that an identity proofing process can be iterative.

This specification covers initial identity proofing for a new applicant. The specification does not consider possible simplifications of the process when the applicant is a known subject, e.g. in cases where identity proofing must be repeated regularly.

In some cases, identity proofing can be regarded as a continuous process, where the behaviour of the subject over time can be used to determine risk/likelihood that the identity is correct. In such cases, the confidence in the correct identity of a subject can increase or decrease over time. Continuous identity proofing is out of scope of this specification.

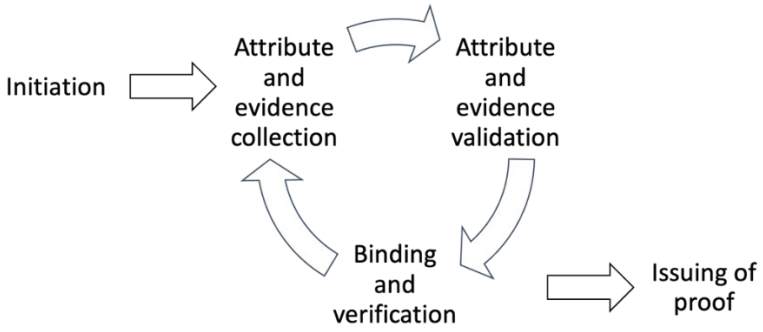

Figure 2: Tasks of an identity proofing process.

Regarding issuing of proof, the **primary result** of an identity proofing process is a verified identity, or an error report if the identity proofing is unsuccessful. This is the result mediated from the IPSP to the trust service provider. This can at a minimum be just YES or NO, meaning that the applicant is proven for correctness against an identity supplied by the TSP, or it can be a set of attributes for the identity of the applicant. Together with the result, the IPSP can provide indication of the confidence level of the complete result or of individual attributes.

The identity proofing process also has a **secondary result**, which is the documentation of the process as it was carried out. The IPSP must be prepared to face regulatory requirements to produce evidence on how the identity of an applicant was proven. Requirements can exist to preserve such evidence for several years.

4.3 Consideration of risks

This specification aims to provide controls against two main categories of identity proofing threats, namely:

- **Falsified evidence** : An applicant claims an incorrect identity using forged evidence.
- **Identity theft** : An applicant uses valid evidence associated with another person.

The first threat is countered by attribute and evidence validation, while the second threat is countered by binding to applicant. As stated above, the required degree of certainty in the result of the identity proofing is determined by the identity proofing context. Identity proofing processes must meet the acceptable risk and security requirements for the applicable identity proofing context.

NOTE: This specification is not intended to cover identity proofing processes that yield a low level of confidence in the result.

This calls for an risk-based and outcome-based approach where requirements can be tuned to the desired degree of certainty of the result. This specification seeks to meet such requirements by a two-step approach:

1. Specify best practice requirements on how to use selected means to implement the three tasks of attribute and evidence collection, attribute and evidence validation, and binding to applicant.
2. Specify how identity proofing processes can be constructed by combining means to meet the desired outcome of the identity proofing process.

NOTE: While this specification addresses use of only certain means, this does not prevent an IPSP from using other means, e.g. other types of evidence, to achieve a comparable degree of certainty.

Regarding item 1 above, requirements are to a large extent sufficiently open for the IPSP to specify various strengths for use of particular means. As one example, when identity documents are used as evidence, the IPSP is required to specify acceptable identity documents based on the identity proofing context; this allows restriction to the most secure type of documents for some processes, while other processes can use less secure documents.

Regarding item 2 above, a process can specify several alternative means that can be considered to result in the same confidence in the result, e.g. physical presence and remote identity proofing as independent alternatives. Processes can also combine means to enhance the outcome by running several means in parallel or in sequence.

The risk dimensions that must be considered by an identity proofing process are shown in the table below.

	Desired property	Related risk	Countermeasures
FALSIFIED EVIDENCE	**AUTHORITATIVE EVIDENCE**	**The identity proofing process can be compromised by the use of non-recognised data source**	Use authoritative (trusted) sources only Use the required set of attributes allowing unique identification
FALSIFIED EVIDENCE	**PROTECTED EVIDENCE**	**The identity proofing process can be compromised by counterfeited and/or manipulated evidence**	Verify the security features and/or assurance level of the evidence
FALSIFIED EVIDENCE / IDENTITY THEFT	**VALID EVIDENCE**	**The identity proofing process can be compromised by use of evidence that is terminated, revoked or reported as lost/stolen**	Verify that the evidence is still valid, have not been revoked or declared lost/stolen
IDENTITY THEFT	**SECURE TRANSMISSION**	**The identity proofing process can be compromised by manipulation of image capturing systems or transmission channels (for remote identity proofing)**	Use secure image capturing systems and transmission channels and transport layer
IDENTITY THEFT	**LEGITIMATE OWNERSHIP**	**The identity proofing process can be compromised by an imposter claiming the legitimate identity of another person**	Ensure that only the legitimate holder of the evidence can claim the identity

Figure 3: Desired properties, risks and countermeasure for identity proofing.

The secure transmission dimension only applies to remote identity proofing processes but can affect both the falsified evidence and identity theft risks. If an identity proofing process is compromised, this may cause incidents related to one or both of the falsified evidence and identity theft risks.

4.4 Use of face biometrics

Face biometrics consists of automated comparison between the facial picture extracted from an identity document presented by the applicant (from an eMRTD digital identity document or by optical scanning of a physical identity document) and a photo of the applicant's face obtained in the identity proofing session. When used with remote identity proofing, both the pictures will be captured on the user's device, and the security of the process must protect against threats in the complete processing chain as shown in the figure below (from ISO/IEC 30107-1 [2]).

Of particular importance for remote identity proofing is presentation attack detection (PAD) as described by the ISO/IEC 30107 [2][3] family of standards, and the quality of the biometric system. This specification covers requirements for all steps in the processing chain shown in the figure, assuming the steps signal processing, comparison, decision, and data storage to be performed in a controlled environment.

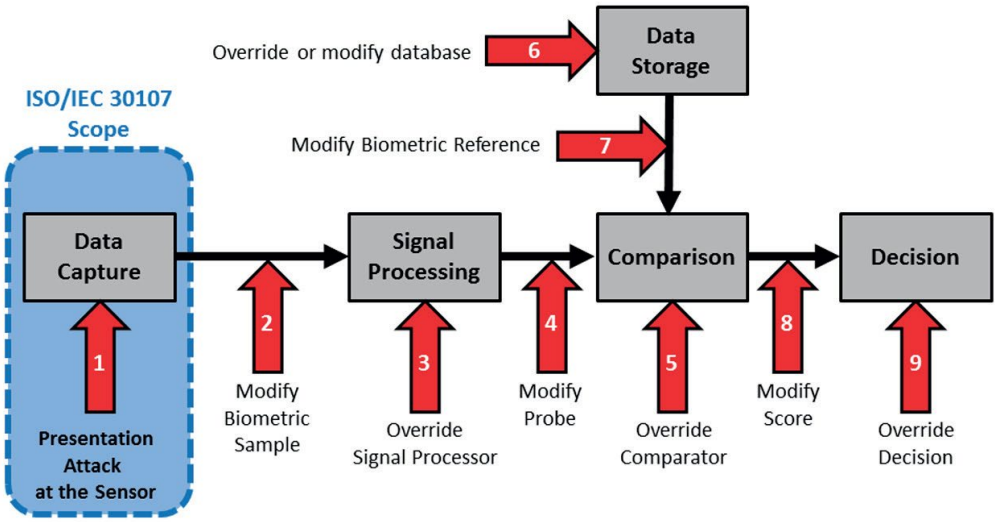

Figure 4: Processing chain for biometric bindling to applicant.

4.5 Normalized and enhanced requirements

The present specification provides requirements at two levels:

1. A normalized level, providing general best practice requirements for the identity proofing process and underlying technologies in order to:
   a. meet industry-standard **performance criteria** in respect of all dimensions and
   b. withstand [customary threats][moderate potential attacks] for professional services offered in a business context
2. An enhanced level, providing extra requirements to achieve better confidence in the identity proofing such that the identity proofing process and underlying technology combination:
   a. meets [enhanced] **performance criteria** in respect of all dimensions
   b. withstands **[enhanced threats][high potential attacks]** for professional services offered in a business context

IPSPs conforming to the present document's normative requirements (i.e. except those marked [ENHANCED] and those defined in annexes) may use in its documentation the following specific OID:

itu-t(0) identified-organization(4) etsi(0) IDENTITY-PROOFING-policies(xx) policy-identifiers(1) main (1)

IPSPs conforming to the present document's enhanced requirements except those defined in annexes may use in its documentation the following specific OID:

itu-t(0) identified-organization(4) etsi(0) IDENTITY-PROOFING-policies(xx) policy identifiers(1) enhanced (2)

Editor's note: The number of policies and identifiers needed is for further study. Defining processes that combine means may lead to a larger number of pre-defined policies but may also be reflected in clause 10.

5 Risk assessment

OVR-5-01: The requirements specified in ETSI EN 319 401 [1], clause 5 shall apply.

6 Policies and practices

6.1. Overview

The present document is structured in line with ETSI EN 319 401 [1]. It incorporates ETSI EN 319 401 requirements by reference and adds requirements relevant for identity proofing.

See ETSI EN 319 401, clause 4 for guidance for guidance on general policy requirements.

6.2 Trust service practice statement

OVR-6.2-01: The requirements specified in ETSI EN 319 401 [1], clause 6.1 shall apply.

In addition, the following particular requirements apply:

OVR-6.2-02: The IPSP practices shall describe identity proofing contexts for which the IPSC can be applicable.

NOTE: For example that the IPSC aims to be compatible with requirements for identity proofing for a particular trust service under a particular regulation.

OVR-6.2-03: The IPSP practices shall be aligned with the policies and practices of TSPs that decide to rely upon the IPSC.

OVR-6.2-04: For each of the identity proofing means covered in clause 8 of this specification, the IPSP shall include separately the applicable requirements selected.

OVR-6.2-05: The IPSP shall describe the identity proofing processes supported based on requirements in clause 9 of this specification.

6.3 Terms and Conditions

OVR-6.3-01: The requirements specified in ETSI EN 319 401 [1], clause 6.2 shall apply.

Editor's note: This clause is for further study, including how IPSP terms and conditions are disclosed in conjunction with terms and conditions for trust services relying upon the IPSC.

6.4 Information security policy

OVR-6.4-01: The requirements specified in ETSI EN 319 401 [1], clause 6.3 shall apply.

7 Identity proofing service management and operation

Editor's note: Further requirements specific to an IPSP may be needed. This is left for further work.

7.1 Internal organization

OVR-7.1-01: The requirements specified in ETSI EN 319 401 [1], clause 7.1 shall apply.

7.2 Human resources

OVR-7.2-01: The requirements specified in ETSI EN 319 401 [1], clause 7.2 shall apply.

7.3 Asset management

OVR-7.3-01: The requirements specified in ETSI EN 319 401 [1], clause 7.3 shall apply.

7.4 Access control

OVR-7.4-01: The requirements specified in ETSI EN 319 401 [1], clause 7.4 shall apply.

7.5 Cryptographic controls

OVR-7.5-01: The requirements specified in ETSI EN 319 401 [1], clause 7.5 shall apply.

7.6 Physical and environmental security

OVR-7.6-01: The requirements specified in ETSI EN 319 401 [1], clause 7.6 shall apply.

7.7 Operation security

OVR-7.7-01: The requirements specified in ETSI EN 319 401 [1], clause 7.7 shall apply.

7.8 Network security

OVR-7.8-01: The requirements specified in ETSI EN 319 401 [1], clause 7.8 shall apply.

7.9 Incident management

OVR-7.9-01: The requirements specified in ETSI EN 319 401 [1], clause 7.9 shall apply.

7.10 Collection of evidence

OVR-7.10-01: The requirements specified in ETSI EN 319 401 [1], clause 7.10 shall apply.

7.11 Business continuity management

OVR-7.11-01: The requirements specified in ETSI EN 319 401 [1], clause 7.11 shall apply.

7.12 Termination and termination plans

OVR-7.12-01: The requirements specified in ETSI EN 319 401 [1], clause 7.12 shall apply.

7.13 Compliance and legal requirements

OVR-7.13-01: The requirements specified in ETSI EN 319 401 [1], clause 7.13 shall apply.

8 Identity proofing service requirements

8.1 Attribute and evidence collection

8.1.1 General requirements

COL-8.1.1-01 The IPSP shall collect the required set of attributes for unique identification for the identity proofing context.

COL-8.1.1-02 The set of attributes shall be collected from one or more evidences issued by authoritative source.

COL-8.1.1-03 [CONDITIONAL]: When images need to be captured, the IPSP shall use secure image capturing systems.

COL-8.1.1-04 [CONDITIONAL]**:** When information needs to be transferred, the IPSP shall use secure communication means.

8.1.2 Attribute collection for natural person

COL-8.1.2-01: Identity attributes for a natural person may be collected via various means or combinations of means.

EXAMPLES:

- From a physical identity document by transcription or scanning (e.g. OCR reading),
- From a digital identity document,
- From use of an eID authenticating the subject,
- From a certificate supporting a digital signature applied by the subject,
- Directly from the subject by typing in information or otherwise,
- From existing information in registers, customer databases or similar.
- From querying auxiliary data sources based on existing attributes,
- From other documents supplied by the subject or from other sources.

COL-8.1.2-02: The attributes collected shall uniquely identify the applicant as a natural person in the identity proofing context.

COL-8.1.2-03: The following attributes shall at a minimum be collected when the applicant is a natural person:

a) current family name(s), current first name(s);
b) information sufficient to uniquely identify the subject in the identity proofing context.

NOTE 1: Requirements for the naming attributes can depend on the identity proofing context. In some contexts, full name (all family names and first names) can be required, while in other contexts full name is not needed. In rare cases, a person can have only one name, classified as either first name or family name.

NOTE 2: Depending on the identity proofing context, unique identification can be in the form of a single attribute such as a national identity number, or as one or more additional attributes that together with the full name provide unique identification.

NOTE 3: ETSI EN 319 412-2 specifies X.509 certificate profile for natural persons. In addition to the name of the subject, a country attribute with undefined semantics is mandatory, and usually a serialNumber attribute is required to guarantee unique identity. While values for country and serialNumber can be part of the attributes collected, these values can also be generated and added by the certification authority.

NOTE 4: Although the outcome of the identity proofing can be a pseudonym identity, identity proofing conforming to this specification requires identification of the real identity of the person.

COL-8.1.2-04: The attributes collected shall be as complete as needed for the identity proofing context.

COL-8.1.2-05: The identity proofing process shall not collect more information than necessary for the outcome of the identity proofing, except when such additional information is necessary for attribute and evidence validation and/or binding.

COL-8.1.2-06: The IPSP shall evaluate the information freshness requirements of the identity proofing context against the freshness provided by the evidence used.

NOTE 1: For example, a passport can have a lifetime of 10 years, and an eID or signing certificate can typically have a lifetime of 2-5 years, meaning the identity information obtained from these evidences can have changed since the evidence was created. Some evidences issuers can apply revocation and re-issuing if information changes.

NOTE 2: If the information conveyed from an identity document or eID or signing certificate does not fulfil the information freshness requirements, the IPSP can compensate by additional means, e.g. use of trusted information sources, documents and attestations, or proof of possession.

8.1.3 Evidence collection for natural person

8.1.3.1 General requirements

COL-8.1.3.1-01: The evidence means applied shall meet the requirements for the identity proofing context regarding authoritative, protected and valid evidence.

COL-8.1.3.1-02: The evidences shall be issued by entities trusted by the IPSP.

8.1.3.2 Physical and digital identity documents

When physical and/or digital identity documents are used as evidence, the following requirements apply:

COL-8.1.3.2-01: An identity document used as evidence may be in physical or digital form.

COL-8.1.3.2-02: When physical and/or digital identity documents are used as evidence of identity, only documents containing a facial photography and/or other information that can be verified by comparison with the applicant's physical appearance shall be accepted.

NOTE: Comparison is typically by biometric technology or by human judgement or a combination of the two.

COL-8.1.3.2-03: When physical and/or digital identity documents are used as evidence of identity, the IPSP shall list in its practice statement the identity documents that can be accepted.

NOTE: For example, the list can consist of document types, e.g. all passports, or named documents, e.g. passports and national identity cards from specific countries.

COL-8.1.3.2-04 [ENHANCED]: When physical or digital identity documents are used as evidence of identity, only passports, national ID cards and other official identity documents that offer the same level of confidence in the identity should be accepted.

COL-8.1.3.2-05 [ENHANCED]: When identity documents are used as evidence of identity, only eMRTD digital documents according to ICAO 9303 part 10 [i.13] and other digital documents providing a comparable level of confidence should be accepted.

8.1.3.3 Use of existing eID

When an existing eID for authentication is used as evidence, the following requirements apply.

COL-8.1.3.3-01: When authentication by use of eID is accepted as evidence of identity, the IPSP shall list in its practice statement the eIDs that are accepted for identity proofing.

NOTE: The list can consist of named eIDs or eID schemes, and/or description of the necessary characteristics of eIDs or eID schemes e.g., by referring to a required LoA for the eID towards a well-establish assurance level framework. As an example, the practice statement can refer to one of the LoAs low, substantial, or high as defined by CIR (EU) 2015/1502 [ref] as minimum LoA accepted.

COL-8.1.3.3-02: When authentication by use of eID is accepted as evidence of identity, the IPSP should list in its practice statement any other condition that an eID must fulfil to be accepted.

NOTE: For example that certain identity attributes must be asserted by the eID.

COL-8.1.3.3-03: The eID should at least conform to eIDAS substantial.

COL-8.1.3.3-04 [ENHANCED]: The eID shall conform to eIDAS high.

8.1.3.4 Use of existing digital signature means with certificate

When an existing eID for authentication is used as evidence, the following requirements apply.

COL-8.1.3.4-01: When a certificate supporting a digital signature is accepted as evidence of identity, the IPSP shall list in its practices statement the certificates that are accepted for identity proofing.

NOTE: The list can consist of named certificate issuers, and/or description of the necessary characteristics of the certificates, e.g. by referring a required minimum certificate policy level.

NOTE 2: As examples, the practice statement can refer to LCP, NCP, NCP+, or QCP policy levels as defined by ETSI EN 319 411-1/-2, or to a requirement for the CA to be listed in the EU Trusted List system.

COL-8.1.3.4-02: When a certificate of a digital signature is accepted as evidence of identity, the IPSP should list in its practice statement any other condition that a certificate must fulfil to be accepted.

NOTE: For example that certain identity attributes must be present for the subject named in the certificate.

COL-8.1.3.4-03: When a certificate of a digital signature is accepted as evidence of identity, the IPSP should list conditions that a digital signature must fulfil to be accepted, e.g. that the signature must conform to specific formats or quality level, or that specific cryptographic algorithms must be used.

NOTE 1: An example requirement is that the signature must be an advanced electronic signature, or a qualified electronic signature, according to the eIDAS regulation.

NOTE 2: The conditions can be stated in the form of a signature policy.

NOTE 3: This specification makes no assumption on the format or content of the document signed.

COL-8.1.3.4-04 [ENHANCED]: When a certificate of a digital signature is accepted as evidence of identity, the certificate shall at least conform to the NCP policy level as defined by ETSI EN 319 411-1.

COL-8.1.3.4-05 [ENHANCED]: When a certificate of a digital signature is accepted as evidence of identity, the certificate should conform to the NCP+ policy level as defined by ETSI EN 319 411-1.

8.1.3.5 Trusted information sources

The main use cases for trusted information sources are:

1. To validate attributes that are already collected to ensure that the attribute values are up to date.
2. To fetch additional attributes.

Availability of trusted information sources can vary between countries, ranging from no availability of trusted sources to use of particular sources being mandated by national regulation.

When a trusted information source is used as additional evidence, the following requirements apply.

COL-8.1.3.5-01: The IPSP shall document in its practice statement the trusted information sources that can be used to collect and/or validate attributes, and whether lookup in these information sources is mandatory or optional.

EXAMPLE 1: Lookup in a national population register, which can be mandated by the identity proofing context.

EXAMPLE 2: Lookup of existing information in a customer register of a TSP.

COL-8.1.3.5-02: The IPSP shall assess that the confidence in attributes from a trusted information source is sufficient for the identity proofing context.

COL-8.1.3.5-03 [ENHANCED]: The confidence in the attributes from trusted information sources shall be at least the same as the confidence in attributes obtained from the identity documents and/or eIDs and/or digital signature certificates accepted as evidence for the identity proofing process.

COL-8.1.3.5-04 [ENHANCED]: Only official national registers should be accepted as trusted information sources.

8.1.3.6 Proof of possession, documents and attestations

When documents and attestations and/or proof of possession are used as additional evidence, the following requirements apply.

COL-8.1.3.6-01: The IPSP shall list in its practices statement documents or attestations required or accepted as additional evidence of identity and the attributes that are obtained from this documentation.

NOTE: E.g. utility bill or attestation as evidence of address.

COL-8.1.3.6-02: The IPSP shall list in its practices statement proof of possession mechanisms that are required or accepted as additonal proof of identity and the attributes that are obtained from these mechanisms.

NOTE: E.g. possession of bank account with identity information obtained from the bank.

COL-8.1.3.6-03: The IPSP shall evaluate the confidence in attributes obtained from documents and attestations and from proof of possession mechanisms and document in its practice statement all cases of attributes that are considered to have a lower level of confidence than attributes validated from the identity document, eID and/or signing certificate presented by the applicant.

COL-8.1.3.6-04 [ENHANCED]: The IPSP shall only use attributes obtained from documents and attestations or proof of possession mechanisms if the attributes have the same level of confidence as attributes obtained from the identity document, eID and/or signing certificate presented by the applicant.

COL-8.1.3.6-05 [ENHANCED]: Acceptance of digital documents and attestations should be limited to digital documents and attestations that are evidenced by a digital signature by the issuer.

8.1.4 Attribute and evidence collection for natural person representing legal person

COL-8.1.4-01: When the applicant is a natural person representing a legal person, identity attributes and evidence for the natural person shall be collected according to the requirements in clauses 8.1.1 and 8.1.2 of this specification.

COL-8.1.4-02: The IPSP shall in its practice statement list the accepted means to evidence the link between a natural person identity and a legal person identity.

NOTE: For example trusted information sources like registers, or required documents and attestations.

COL-8.1.4-03: The IPSP shall in its practice statement list the acceptable roles or relationships entitling the natural person to represent the legal person.

COL-8.1.4-04 [ENHANCED]: The role of the natural person with respect to the legal person shall be collected from or verified against an appropriate, trusted business register or other trusted information source.

8.1.5 Attribute and evidence collection for legal person

COL-8.1.5-01: Identity attributes for a legal person may be collected via various means or combination of means.

EXAMPLE: Depending on the identity proofing context, attribute collection for a legal person may vary from basic company information to a full record of the company, including beneficial owners and personnel in key roles, e.g. for KYC/AML purposes. As examples, attributes can be collected from business registers, commercial information providers, and documents and attestations.

COL-8.1.5-02: The attributes collected shall uniquely identify the applicant as a legal person in the identity proofing context.

COL-8.1.5-03: When the applicant is a legal person, the following attributes shall as a minimum be collected:

a) full name and legal status of the legal person;
b) country of registration of the legal person;
c) unique identifier and type of identifier for the legal person (unless such identifier does not exist).

NOTE: Unique identifier can be national registration number, VAT number, or LEI (Legal Entity Identifier).

COL-8.1.5-04: The attributes collected for a legal person should be verified against an appropriate, trusted business register to the extent that the required attributes are present in the register.

NOTE: There can be a need to do identity proofing of entities that do not possess a unique identifier and that are not present in any business register, e.g. public sector agencies in some countries.

COL-8.1.5-05 [CONDITIONAL]: When a certificate supporting a digital signature is accepted as evidence of identity for a legal person, the IPSP shall list in its practices statement the certificates that are accepted for identity proofing.

NOTE 1: The list can consist of named certificate issuers, and/or description of the necessary characteristics of the certificates, e.g. by referring a required minimum certificate policy level.

NOTE 2: As examples, the practice statement can refer to LCP, NCP, NCP+, or QCP policy levels as defined by ETSI EN 319 411-1/-2, or to a requirement for the CA to be listed in the EU Trusted List system.

COL-8.1.5-06 [CONDITIONAL]: When a certificate of a digital signature is accepted as evidence of identity for a legal person, the IPSP should list in its practice statement any other condition that a certificate must fulfil to be accepted, e.g. that certain identity attributes must be present for the subject named in the certificate.

COL-8.1.5-07 [CONDITIONAL]: When a certificate of a digital signature is accepted as evidence of identity for a legal person, the IPSP should list conditions that a digital signature must fulfil to be accepted, e.g. that signatures must conform to specific formats or quality levels, or that specific cryptographic algorithms must be used.

NOTE 1: An example requirement is that the signature must be an advanced electronic seal, or a qualified electronic seal, according to the eIDAS regulation.

NOTE 2: The conditions can be stated in the form of a signature policy.

NOTE 3: This specification makes no assumption on the format or content of the document signed.

COL-8.1.5-08: The IPSP shall list in its practices statement any other document or attestation required or accepted as additional proof of identity.

NOTE: E.g. attestation that the legal person exists and further information on its legal status.

COL-8.1.5-09: A statement from a natural person verified to represent the legal person may be accepted as evidence.

8.2 Attribute and evidence validation

8.2.1 General requirements

The requirements in this clause 8.2 apply to natural persons, legal persons, and natural person representing legal person, except for the clauses 8.2.2 and 8.2.3 that only apply to natural persons.

NOTE: Trusted information sources and documents and attestations, see clauses 8.2.6 and 8.2.7 below, can be of particular importance as evidence for legal person and natural person representing legal person.

VAL-8.2.1-01: The IPSP shall verify the security features and/or assurance level of the evidence.

VAL-8.2.0-02: The IPSP shall verify that the evidence is valid and that it has not been revoked or declared lost/stolen.

NOTE: For identity documents, lookup services for status of documents may not be available to the IPSP.

COL-8.2.1-03: The identity proofing process shall prove that the identity evidence is genuine.

COL-8.2.1-04: The identity proofing process shall prove that the identity evidence is in the possession of the applicant.

8.2.2 Validation of digital identity document

This scope of this specification is limited to eMRTD digital identity documents according to ICAO 9303 [i.13] read over the NFC interface of the chip embedded in a passport or national identity card. An eMRTD digital identity document can be used with both physical presence and remote identity proofing. Remote reading of a digital identity document requires the user to be in possession of a device equipped with an NFC reader.

NOTE 1: Other types of digital identity documents than eMRTD can come in scope for future versions of this specification, e.g. there is ongoing standardisation efforts in CEN on "digital breeder documents" that can become relevant in the future.

NOTE 2: The limitation of scope of this specification to eMRTD does not preclude an IPSP from using other types of digital identity documents in identity proofing processes according to the IPSP's own requirements and the requirements of the identity proofing context.

Editor's note: To be verified to what extent the "REGULATION (EU) 2019/1157 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement" will restrict access to face photo in eMRTD when the regulation enters into force 2nd August 2021. If access to face photo is restricted, use of digital identity documents and face biometrics will in general be limited to passports.

When a digital identity document is used as identity evidence, the following requirements apply:

VAL-8.2.2-01: The digital identity document shall only be accepted if validation of the issuer's digital signature on the document yields TOTAL_PASSED.

VAL-8.2.2-02: No processing of the digital identity document shall be done on a device controlled by the applicant.

NOTE: For remote identity proofing, processing will usually be in the IPSP's servers in a secured environment. When used with physical presence, processing can be done in dedicated equipment on site.

VAL-8.2.2-03: When a user device is used to read the digital identity document, the IPSP shall ensure that the digital identity document is transferred to the IPSP's equipment in a manner that ensures authenticity, integrity, and confidentiality of both the document and the communication channel.

VAL-8.2.2-04: When a user device is used to read the digital identity document, the user device should be equipped with an app that is approved by the IPSP, properly installed on the user device, protected against modifications from other applications on the device, and that prevents other apps on the device access to identity information.

VAL-8.2.2-05: When the IPSP approves an app for reading a digital identity document on a user device, the IPSP shall ensure that the app only transfers digital identity documents to approved server instances at the IPSP side.

VAL-8.2.2-06: The process shall ensure that the digital identity document really is read from the chip of an identity document present at the applicant's device.

VAL-8.2.2-07: It shall not be possible for the applicant or an external attacker to inject into the process a digital identity document that has previously been copied and stored by the attacker.

VAL-8.2.2-08: The process shall validate that the identity document is within its validity period.

VAL-8.2.2-09 [CONDITONAL]: If an online status service to confirm validity of the document exists and is available to the IPSP, the process shall use this service to verify that the document is not revoked.

NOTE: Not all countries have available lookup services to check validity, and in some countries access to the lookup services is restricted.

VAL-8.2.2-10: The digital identity document and log information for the process shall be retained for the necessary retention time given by the identity proofing context.

8.2.3 Validation of physical identity document

8.2.3.1 General requirements

When a physical identity document is used as identity evidence, the following requirements apply.

NOTE: An identity document can be validated both by physical presence and remotely, and by manual or automated control. Clause 8.2.3.2 below provides additional requirements specifically for remote validation of a physical identity document.

VAL-8.2.3.1-01: The process shall verify that the document presented corresponds to an existing document type that is accepted according to the IPSP practice statement.

NOTE: An identity proofing process can use more than one document, either routinely, or with a second document added if identity proofing using the first document yields an uncertain result.

VAL-8.2.3.1-02: The process shall verify that the document presented is visually equal to the expected visual appearance of the document type.

VAL-8.2.3.1-03: The process shall validate security elements of the document to the extent needed to obtain sufficient certainty in the genuiness of the document.

NOTE: Examples of security elements are watermarks, holograms, printing techniques, infrared light visual patterns, and see-through elements.

VAL-8.2.3.1-04: The identity information and other information printed on the card shall be extracted either by manual transcription or by automated means.

NOTE: Automated may for example be by optical scanning and OCR techniques.

VAL-8.2.3.1-05: The process shall verify that the document is within its validity period (not expired).

VAL-8.2.3.1-06 [CONDITIONAL]: If an online status service to confirm validity of the document exists and is available to the IPSP, the process shall use this service to verify that the document is not revoked.

NOTE: Not all countries have available lookup services to check validity, and in some countries access to the lookup services is restricted.

VAL-8.2.3.1-07 [CONDITIONAL]: When the process is performed with manual validation of the document, the registration officer shall have access to authoritative sources of information on document appearance and document validation.

NOTE: For example PRADO (Public Register of Authentic Travel and Identity Documents Online) for the EU and the EEA countries.

VAL-8.2.3.1-08 [CONDITIONAL]: When the process is performed with physical presentation of the document, the registration officer should verify haptic / tactile security features if any.

VAL-8.2.3.1-09 [CONDITIONAL]: When the process is performed with physical presentation of the document, a photo or photocopy of the document (one or two pages) shall be produced and retained for the necessary retention time given by the identity proofing context.

VAL-8.2.3.1-10 [CONDITIONAL]: When the process is performed with physical presentation of the document, a photo of the applicant's face may be produced and retained for the necessary retention time given by the identity proofing context.

VAL-8.2.3.1-11 [CONDITIONAL]: When validation of the identity document is done manually, the validation shall only be carried out by a registration officer that has received appropriate training.

VAL-8.2.3.1-12 [CONDITIONAL]: When validation of the identity document is done manually, the training of the registration officer shall cover at least the following :

a) Fraud prevention / detection of forgery
b) Data protection
c) Communication training
d) Training on software and equipment used

VAL-8.2.3.1-13 [CONDITIONAL]: When validation of the identity document is done manually, the training of the registration officer should be repeated or refreshed annually.

VAL-8.2.3.1-14 [ENHANCED]: The process shall use automated means and machine-learning technology to analyze the identity document's characteristics against the expected appearance of the document, including analysis of security elements of the document and of potential manipulation of the document.

NOTE 1: The document type, e.g. a passport of a specific country, can be an input parameter to the analysis, or the analysis can determine the type by automated means.

NOTE 2: If automated analysis yields an uncertain result, the process can apply an additional manual check.

VAL-8.2.3.1-15: Documentation of the validation process shall be retained for the necessary retention time given by the identity proofing context.

8.2.3.2 Requirements for remote validation

When a physical identity document is used as identity evidence in a remote validation process, the following requirements apply.

VAL-8.2.3.2–01: At least one high-resolution still photo of each relevant side of the identity document presented by the applicant shall be captured as part of the identity proofing process.

NOTE 1: Submission of a pre-existing photo of an identity document is considered to not meet the requirements for identity proofing of trust service subjects.

NOTE 2: Examples of two-sided documents where both sides must be captured are most national identity cards and some passports.

VAL-8.2.3.2-02: The process shall ensure that the document presented by the applicant is a real, physical identity document.

NOTE: Recording of a video sequence with movement of the identity document is a possible mechanism.

VAL-8.2.3.2-03 [CONDITIONAL]: If face biometrics is applied for binding of the identity document to the applicant, the facial photo printed on the identity document shall be extracted.

VAL-8.2.3.2-04 [CONDITIONAL]: If the identity document has an MRZ (machine readable zone), the information from the MRZ should be extracted and validated.

VAL-8.2.3.2-05 [CONDITIONAL]: If the identity document is validated by manual procedures, the validation task should be assigned randomly among available registration officers.

VAL-8.2.3.2-06 [CONDITIONAL]: If the identity document is validated by manual procedures, the information security policy of the IPSP shall cover the location and equipment used by the registration officers.

8.2.4 Validation of eID as identity evidence

When authentication by use of an existing eID is used as identity evidence, the following requirements apply.

VAL-8.2.4-01: The IPSP shall execute an authentication protocol that ensures that the eID is valid (not expired or revoked) and is used by the person identified by the eID.

NOTE 1: Successful authentication means that the eID as evidence is validated, that the identity information conveyed from the eID is validated, and that the identity information is bound to the applicant.

NOTE 2: The eID can represent a natural person, a legal person, or a natural person representing a legal person.

VAL-8.2.4-02: The identity assertion obtained from the authentication protocol, identification (e.g. serial number) of the eID used, and if needed additional proof that the eID was valid at the time of authentication, shall be retained as required by the identity proofing context as evidence of the identity proofing.

8.2.5 Validation of digital signature with certificate as identity evidence

When a digital signature is used as identity evidence the following requirement apply;

VAL-8.2.5-01: The IPSP shall validate the digital signature and use the signing certificate for validation of identity attributes only if the signature validation result is TOTAL-PASSED.

NOTE 1: When the digital signature is validated, the information obtained from the certificate supporting the digital signature is validated and bound to the applicant.

NOTE 2: The certificate can represent a natural person, a legal person, or a natural person representing a legal person.

VAL-8.2.5-02: The signed document, the signature with the signing certificate, and supporting evidence shall be retained as required by the identity proofing context as evidence of the identity proofing.

NOTE: E.g. by use of a long-term signature format and/or a preservation service for digital signatures.

8.2.6 Validation against trusted information sources

When the IPSP uses trusted information sources in an identity proofing process, the following requirements apply.

VAL-8.2.6-01 [CONDITONAL]: If the communication between the IPSP and the data source is online, the communication channel shall be secured by use of the TLS protocol version 1.2 or higher or by another protocol offering the same level of security.

VAL-8.2.6-02 [CONDITONAL]: If the communication between the IPSP and the data source is online, the IPSP and the data source provider shall be mutually authenticated.

VAL-8.2.6-03 [CONDITIONAL]: If the communication between the IPSP and the data source is message-based, all messages shall be authenticated and integrity protected.

VAL-8.2.6-04 [CONDITIONAL]: If the communication between the IPSP and the data source is message-based, all messages containing personal identity information shall be encrypted end to end between the data source and the IPSP.

VAL-8.2.6-05: The IPSP shall validate integrity and authenticity of the information obtained from the trusted information source.

VAL-8.2.6-06: The IPSP shall in the practice statement document the procedure to apply in case of discrepancies between the information obtained from the trusted information source and information from other evidence.

NOTE: For example, the trusted information source can be regarded as an authoritative source that overrides other sources of information, or other evidence can be regarded as authoritative, or an arbitration procedure can be used.

VAL-8.2.6-07: The information obtained from the trusted information source shall be securely retained for the time period needed for the identity proofing process.

8.2.7 Validation of proof of possession, documents and attestations

8.2.7.1 Proof of possession

When the IPSP uses proof of possession in an identity proofing process, the following requirements apply.

VAL-8.2.7.1-01: The IPSP shall execute a sufficiently secure proof of possession protocol, or rely on a protocol executed by a party trusted by the IPSP, to ensure that the item in question is possessed by the applicant.

NOTE: E.g. to confirm possession of mobile phone number, email address, or bank account or credit card.

VAL-8.2.7.1-02 [CONDITIONAL]: When proof of possession is used to obtain further identity attributes, the IPSP shall validate integrity and authenticity of the information obtained.

NOTE: E.g. an existing customer record from a bank or a telecommunications service provider.

VAL-8.2.7.1-03 [CONDITIONAL]: When proof of possession is used to obtain further identity attributes**,** the IPSP shall in the practice statement document the procedure to apply in case of discrepancies between the information obtained and information from other evidence.

NOTE: For example, the information obtained can be regarded as authoritative and override other sources of information, or other evidence can be regarded as authoritative, or an arbitration procedure can be used.

VAL-8.2.7.1-04: The information obtained from the proof of possession shall be securely retained for the required retention period for the identity proofing context.

8.2.7.2 Documents and attestations

When the IPSP uses documents and attestations in an identity proofing process, the following requirements apply.

VAL-8.2.7.2-01: The IPSP shall verify that all documents or attestations presented correspond to an existing document type that is accepted according to the IPSP practice statement.

NOTE: This can imply that only digital documents are accepted.

VAL-8.2.7.2-02: The IPSP shall verify the identity of the issuer of the document or attestation.

NOTE 1: For a digital document, this can imply validation of a digital signature from the issuer.

NOTE 2: For a physical document, this can for example be by physical signatures or seals, logos and other visual elements.

VAL-8.2.7.2-02 [CONDITIONAL]: If a document or attestation is in physical form, the IPSP shall verify that the document presented is visually equal to the expected visual appearance.

VAL-8.2.7.2-03 [CONDITIONAL]: If a document or attestation is in physical form and the document type contains security elements, the IPSP shall verify these security elements.

VAL-8.2.7.2-03 [CONDITIONAL]: When documents and attestations are used to obtain further identity attributes**,** the IPSP shall in the practice statement document the procedure to apply in case of discrepancies between the information obtained and information from other evidence.

NOTE: For example, the information obtained can be regarded as authoritative and override other sources of information, or other evidence can be regarded as authoritative, or an arbitration procedure can be used.

VAL-8.2.7.2-04: The the documents and attestations shall be securely retained for the required retention period for the identity proofing context.

8.3 Binding with applicant

8.3.1 General requirements

BIN-8.3.1-01: The IPSP shall ensure that only the legitimate holder of the evidence can claim the identity.

BIN-8.3.2-02: The IPSP shall shall prove that that the applicant presenting the evidence really is the person identified by the document.

BIN-8.3.2-03: For the following types of evidence, the binding to applicant shall be covered by requirements on attribute and evidence collection and/or attribute and evidence validation:

- [CONDITIONAL] When an eID is used for identity proofing **VAL-8.2.4-01** to **02** apply.
- [CONDITIONAL] When a digital signature is used for identity proofing **VAL-8.2.5-01** to **02** apply.
- [CONDITIONAL] When trusted information sources are used, **VAL 8.2.6-01** to **07** apply.
- [CONDITIONAL] When proof of possession is used, **VAL 8.2.7.1-01** to **04 apply**
- [CONDITIONAL] When documents and attestations are used, **VAL 8.2.7.2-01** to **04** apply.

NOTE: For eID and digital signature, the binding to the applicant when the eID or signature is validated is under the assumption that only the applicant can use the eID or signing means.

BIN-8.3.1-04: Binding of an identity document with the applicant may be done by manual procedures or automated by face biometrics.

NOTE 1: An identity proofing process can use a combination of automated and manual means.

NOTE 2: Use of other biometrics than face is currently out of scope but can be a future possibility.

8.3.2 Binding by automated face biometrics

8.3.2.1 Biometric data capture of face photo of the applicant

When face biometrics is used for binding of evidence to applicant, the following requirements apply.

BIN-8.3.2.1-01: A high resolution photo of the applicant's face shall be captured as part of the identity proofing process.

BIN-8.3.2.1-02: The biometric data capture shall apply PAD measures for liveness detection as specified by ISO/IEC 30107 parts 1 [2] and 3 [3].

NOTE: To ensure that a live person is present in front of the camera.

BIN-8.3.2.1-03: The biometric data capture shall apply PAD measures for obscuration detection as specified by ISO/IEC 30107 parts 1 [2] and 3 [3].

NOTE: E.g. to detect that the face of the applicant is partly covered.

BIN-8.3.2.1-04: The biometric data capture shall apply PAD measures for non-conformance detection as specified by ISO/IEC 30107 parts 1 [2] and 3 [3].

NOTE: E.g. to detect insufficient light for proper capture of face photo.

BIN-8.3.2.1-05: The biometric data capture should apply measures to detect morphed photos in identity documents.

NOTE: A morphed photo is created by merging the face photos of two or more different persons into one photo. Since some countries allow persons to bring their own photo for the issuing of a passport or national identity card, there is a risk that documents are issued with morphed photos. With a morphed photo, there is a risk that both/all the persons can be recognized by face biometrics with a confidence above the applied threshold, meaning more than one person can use the identity document containing the morphed photo.

BIN-8.3.2.1-06: The biometric data capture should apply measures to detect artificially generated or manipulated face appearance.

NOTE: Such attacks are sometimes termed "deep fake" attacks.

8.3.2.2 Biometric comparison of face photo towards identity document

When automated face biometric is used the following requirements apply.

BIN-8.3.2.2-01 The process shall provide a reliable automated comparison between the facial picture extracted from the identity document presented by the applicant (from an eMRTD digital identity document or by optical scanning of a physical identity document) and a photo of the applicant's face obtained in the identity proofing session.

BIN-8.3.2.2-02 [CONDITIONAL]: When used with remote identity proofing, both the pictures will be captured on the applicant's device, and the process shall protect the pictures' authenticity and integrity from capture to storage in the IPSP's system.

BIN-8.3.2.2-03: No biometric processing, except from data capture, shall be done in equipment controlled by the applicant.

BIN-8.3.2.2-04: Biometric presentation attack detection, signal processing, comparison, data storage, and decision shall be carried out in secure processing equipment, protecting against attacks as identified by clause 5.1 in ISO/IEC 30107-1 [2].

NOTE: See figure 4 in clause 4.4 of the present document.

BIN-8.3.2.2-05 [CONDITIONAL]: When biometric face recognition is used with physical presence of the applicant, properly secured equipment shall be used to read the identity document presented by the applicant (optical scanning or reading of digital identity document) and to obtain a high-resolution face photo of the applicant.

BIN-8.3.2.2-06 [CONDITIONAL]: When biometric face recognition is used with physical presence of the applicant, locally installed and properly secured equipment may be used for the biometric face recognition processing.

Editor's note: Values for results in requirement below needs consideration.

BIN-8.3.2.2-10: The biometric system applied shall be tested according to the relevant clauses for face biometrics in ISO/IEC 19795-1 [4] with measured error rates below TBD.

BIN-8.3.2.2-11: The PAD should be evaluated according to ISO/IEC 19989-3 [i.15].

NOTE: Common Criteria evaluation of the presentation attack detection.

BIN-8.3.2.2-12: Test results for the PAD shall achieve APCER (attack presentation classification error rate) as defined by ISO/IEC 30107-3 [3] below 5 %.

BIN-8.3.2.2-13: Test results for the PAD shall achieve BPCER (bona fide presentation classification error rate) as defined by ISO/IEC 30107-3 [3] below TBD %.

BIN-8.3.2.2-14: Test results for the biometric face recognition shall show a FAR (false acceptance rate) below 5 %.

BIN-8.3.2.2-15 [ENHANCED]: Test results for the biometric face recognition shall show a FAR (false acceptance rate) below 1 %.

BIN-8.3.2.2-16: Test results for the biometric face recognition shall show a FRR (false rejection rate) below TBD %.

BIN-8.3.2.2-17 [ENHANCED]: Test results for the biometric face recognition shall show a FRR (false rejection rate) below TBD %.

8.3.3 Binding by manual face verification

Editor's note: This clause is incomplete and needs best practice requirements for manual process both with physical appearance and for remote identity proofing. It is likely that ENHANCED requirements will be suggested to define two levels of manual processing.

8.3.3.1 General requirements

When manual binding of the applicant to an identity document is used, the following requirements apply:

BIN-8.3.3-01: The human operator shall compare the facial photo obtained from the applicant's identity document with the physical appearance of the applicant, either from the physical presence of the applicant or from a photo/video obtained in a remote identity proofing session.

BIN-8.3.3-02: The personnel performing the comparison of the applicants' face with the photo of the identity document shall receive training in facial recognition before being allowed to do any comparison and repeatedly at least yearly.

BIN-8.3.3-03: The personnel shall be allowed to spend sufficient time for the face comparison.

8.3.3.2 Physical appearance

Editor's note: This clause will be added later

8.3.3.3 Remote identity proofing

Editor's note: This clause will be added later

8.3.4 Binding to applicant for legal person and natural person representing legal person

Editor's note: This clause will be added later.

8.4 Issuing of proof

8.4.1 Result of the identity proofing process

PRO-8.4.1-01: The IPSP shall describe in its practice statement what constitutes evidence of the result of identity proofing process.

NOTE: For example a document (e.g. PDF), structured data (e.g. XML, JSON), identity assertion (e.g. OIDC, SAML).

PRO-8.4.1-02: The result of the identity proofing shall be delivered in a secure way to the trust service provider, regarding authenticity, integrity, and confidentiality of the result.

PRO-8.4.1-02: The IPSP should digitally sign the result of the identity proofing.

PRO-8.4.1-04: The result of the identity proofing process shall be at minimum a 'success' or 'failure' statement.

NOTE: Success means that there is confirmation of identity attributes provided before the process starts, meaning that the IPSP is asked to confirm a specific identity.

PRO-8.4.1-05: The result of the identity proofing may be a set of identity attributes requested by the trust service provider.

PRO-8.4.1-06: The result of the identity proofing, and individual identity attributes where relevant, may be delivered together with an indication of the confidence achieved by the identity proofing process.

8.4.2 Evidence of the identity proofing process

PRO-8.4.2-01: The IPSP shall gather evidence of the identity proofing process according to the requirements from the identity proofing context.

NOTE: Evidence can be in digital and/or paper format.

PRO-8.4.2-02: The evidence should completely document the identity proofing process.

NOTE: For example including video sequences used in a remote identity proofing process.

PRO-8.4.2-03: The IPSP shall digitally sign all digital evidence or otherwise ensure that the evidence is stored in a tamper-proof way.

NOTE: This can take be a seal by the IPSP or a signature by an operator.

PRO-8.4.2-04: Evidence of the identity proofing process shall be reliably stored according to the requirements from the identity proofing context and as required by the trust service provider's policy.

NOTE 1: A typical requirement from a TSP is as long as the applicant remains a subject/subscriber of the TSP plus a number of years after that time.

NOTE 2: Storage can be by the IPSP, the TSP, or an external service.

PRO-8.4.2-05: Storage shall ensure that search, retrieval, and re-verification of the identity proofing result is possible.

NOTE: Offline storage or other means that will result in a prolonged response time are acceptable.

PRO-8.4.2-06: At the end of the retention time defined by **PRO 8.4.2-04**, the evidence of the identity proofing process and all personal data on the subject shall be deleted.

9 Process requirement

9.1 General requirements

PRO-9.1-01: The IPSP shall combine means described in clause 8 of the present document into a coherent identity proofing process meeting the requirements of the applicable identity proofing context.

NOTE: National or sectorial requirements that constitute parts of the identity proofing context can influence the selection of means for the identity proofing.

PRO-9.1-02: The combination of means for an identity proofing process shall cover all tasks of attribute and evidence collection, attribute and evidence validation, and binding to applicant.

PRO-9.1-03: The combination of means for the identity proofing process may specify that alternative means can be selected leading to the same outcome.

NOTE: For example an identity proofing process can allow both physical presence and remote identity proofing as long as the outcome of both alternatives fulfil the requirements of the identity proofing context.

PRO-9.1-04: An identity proofing process may require a combination of two or more means for one identity proofing task (collection, validation, binding).

NOTE: For example that both an eID and an identity document are used as evidence in the process.

9.2 Normalized identity proofing process, natural person

Normalized identity proofing is the basis level supported by this specification. All means specified in clause 8 of the present document can be used for this level of identity proofing.

NOTE: Normalized identity proofing can be considered for example for issuing of certificates according to NCP and QCP policies as define by ETSI EN 319 411-1 [i.6] and ETSI EN 319 411-2 [i.7] and for issuing of eID at assurance level substantial according to CIR EU 1015/1502 [i.3].

PRO-9.2-01: A normalized identity proofing process for a natural person shall not refer to requirements identified as [ENHANCED] in the current specification.

PRO-9.2-02: A normalized identity proofing process for a natural person shall comply with requirements of the following clauses of this specification:

1. For attribute and evidence collection:
   - Clause 8.1.1 and clause 8.1.2 for identity attribute collection,
   - For evidence collection clause 8.1.3.1 and either:
     - Clause 8.1.3.2 for physical or digital identity documents, and/or
     - Clause 8.1.3.3 for existing eID, and/or
     - Clause 8.1.3.4 for existing digital signature means.
2. For attribute and evidence validation, as pertinent to the evidence collected, clause 8.2.1 and either:
   - Clause 8.2.3 for digital identity documents, and/or
   - Clause 8.2.4 for physical identity documents
   - Clause 8.2.5 for existing eID, and/or
   - Clause 8.2.6 for existing digital signature means, and/or
   - .
3. For binding to applicant, as pertinent to the evidence collected, clause 8.1.1 and either:
   - Clause 8.2.1 for existing eID (integrated with evidence validation), and/or
   - Clause 8.2.2 for existing digital signature means (integrated with evidence validation), and/or
   - Clause 8.3.2 for face biometrics, and/or
   - Clause 8.3.3 for manual face verification.

PRO-9.2-03: An normalized identity proofing process for a a natural person may additionally use means that comply with the the following clauses of this specification:

- Trusted information sources according to clauses 8.1.3.5 and 8.2.7, and/or
- Documents and attestations according to clauses 8.1.3.6 and 8.2.7.2, and/or
- Proof of possession according to clauses 8.1.3.6 and 8.2.7.1.

EXAMPLE: An remote identity proofing process with manual procedures for attribute and evidence validation and binding to applicant can refer to the following clauses: 8.1.1 and 8.1.2 (identity attribute collection), 8.1.3.2 (identity document as evidence), 8.2.1 and 8.2.3 including 8.2.3.2 (validation of physical identity document remote process), 8.3.1, 8.3.3.1 and 8.3.3.3 (manual binding to applicant, remote process).

9.3 Enhanced identity proofing process, natural person

Enhanced identity proofing is an elevated level of identity proofing. All means specified in clause 8 of the present document can be used for this level of identity proofing.

NOTE: Enhanced identity proofing can be considered for example for issuing of eID at assurance level high according to CIR EU 1015/1502 [i.3].

PRO-9.3-01: An enanced identity proofing process for a natural person shall comply with requirements of the following clauses of this specification, including requirements identified as [ENHANCED]:

1. For attribute and evidence collection:
   - Clause 8.1.1 for identity attribute collection,
   - For evidence collection either:
     - Clause 8.1.2.1 for physical or digital identity documents, and/or
     - Clause 8.1.2.2 for existing eID, and/or
     - Clause 8.1.2.3 for existing digital signature means.
2. For attribute and evidence validation, as pertinent to the evidence collected, either:
   - Clause 8.2.1 for existing eID, and/or
   - Clause 8.2.2 for existing digital signature means, and/or
   - Clause 8.2.3 for digital identity documents, and/or
   - Clause 8.2.4 for physical identity documents.
3. For binding to applicant, as pertinent to the evidence collected, either:
   - Clause 8.2.1 for existing eID (integrated with evidence validation), and/or
   - Clause 8.2.2 for existing digital signature means (integrated with evidence validation), and/or
   - Clause 8.3.2 for face biometrics, and/or
   - Clause 8.3.3 for manual face verification.

PRO-9.3-02: An enhanced identity proofing process for a a natural person may additionally use means that comply with the the following clauses of this specification:

- Trusted information sources according to clauses 8.1.3.5 and 8.2.6, and/or
- Documents and attestations according to clauses 8.1.3.6 and 8.2.7.2, and/or
- Proof of possession according to clauses 8.1.3.6 and 8.2.7.1.

PRO-9.3-03 [CONDITIONAL]: When additional means according to PRO-9.3-02 are applied for an enhanced identity proofing process for a natural person, requirements identified as [ENHANCED] should apply.

9.4 Normalized identity proofing process, legal person

Editor's note: This clause will be added later

9.5 Enhanced identity proofing process, legal person

Editor's note: This clause will be added later

9.6 Normalized identity proofing process, natural person representing legal person

Editor's note: This clause will be added later

9.7 Enhanced identity proofing process, natural person representing legal person

Editor's note: This clause will be added later

10 Framework for definition of identity proofing policy built on the present document

Editorial note: To be developed.

Annex A (informative): Table of contents for identity proofing service component practice statement

Editor's note: To be developed.

Annex B (informative): Application of the present specification for current versions of ETSI TSP policy requirements standards

B.1 Introduction

This Annex specifies how an IPSP is intended to meet the requirements currently specified by relevant ETSI standards on policy and security requirements for trust services. The following standards have requirements for identity proofing:

- ETSI EN 319 411-1/-2 [i.7][i.8] for issuance of certificates,
- ETSI EN 319 521 [i.10] for electronic registered delivery services,
- ETSI TS 119 431-1 [i.9] for remote electronic signing services that in turn refers to CEN EN 419 241-1 [i.10].

When the ETSI TS 119 461 (the present document) is published, this may lead to updates in existing standards to reference ETSI TS 119 461.

B.2 Application for issuance of NCP and QCP certificates as specified in ETSI EN 319 411-1/-2

Editor's note: This will be completed similarly for legal person and natural person representing legal person.

The current requirements for the identity proofing process for the issuance of a **NCP certificate** to a natural person are as quoted from ETSI EN 319 411-1 [i.7]:

> **When the subject is a natural person (i.e. physical person as opposed to legal person):**
>
> **REG-6.2.2-05 [NCP] [CONDITIONAL]: If the subject is a natural person (i.e. physical person as opposed to legal person), evidence of the subject's identity (e.g. name) shall be checked against this natural person either directly by physical presence of the person (the subject shall be witnessed in person unless a duly mandated subscriber represents the subject), or shall have been checked indirectly using means which provides equivalent assurance to physical presence.**
>
> > **NOTE 3: An example of the required indirect evidence of identity is one or more registration documents electronically signed by a person trusted to have checked the persons' identity in line with the requirements of this clause.**

The requirements of clauses 5 to 9 of the present document, excluding the requirements marked [ENHANCED], are intended to fulfil requirements for issuance of a NCP certificate.

In particular, referring to the above requirement **REG-6.2.2-05** from ETSI EN 319 411-1, the requirement for identity proofing "*by the physical presence of the natural person*" can e.g. be met through application of the clauses: 8.1.2 (attribute collection), 8.1.3.2 (identity document as evidence), 8.2.3.1 (validation of physical identity document, general requirements), and 8.3.3 (binding by manual face verification). Other combinations of means are possible.

Referring to the above requirement **REG-6.2.2-05** from ETSI EN 319 411-1, the requirement for identity proofing "*by methods which provide equivalent assurance … to the physical presence*" can be met through application of means described by clause 8 excluding clauses that are specific to physical appearance.

ETSI EN 319 411-2 specifies requirements for a QTSP issuing qualified certificate as defined in the eIDAS Regulation (EU) No 910/2014 (eIDAS), Article 24 (1) of eIDAS. The additional requirements for the issuance of a qualified certificate, **QCP certificate**, quoted from ETSI EN 319 411-2 [i.8] are:

> **REG-6.2.2-02 [QCP-n] and [QCP-n-qscd]: The identity of the natural person and, if applicable, any specific attributes of the person, shall be verified:**
>
> **a) by the physical presence of the natural person; or**
>
> **b) using methods which provide equivalent assurance in terms of reliability to the physical presence and for which the TSP can prove the equivalence.**
>
> **NOTE 1: The proof of equivalence can be done according to the Regulation (EU) No 910/2014.**
>
> **NOTE 2: The proof of equivalence needs to consider the impersonation risks inherent to remote applications. In particular, an uninterrupted chain of subsequent remote registrations can increase such risks, because the person can never be actually seen for years, and/or because the traceability with the initial face to face is weakened.**

As the policy level NCP from ETSI EN 319 411-1 and QCP from ETSI EN 319 411-2 are intended to be at the same level of security, an IPSP that offers service in support of the issuance of QCP certificates is expected to comply with the same requirements as for NCP above.

In particular, the above requirements **REG-6.2.2-02** from ETSI EN 319 411-2 regarding physical presence and equivalence to physical presence can be met by the combination of means/clauses as indicated above for NCP policy.

B.3 Application of the present specification to ETSI EN 319 521

The current requirement in ETSI EN 319 521 [i.10] states requirements for a qualified electronic registered delivery service (QERDS) as quoted:

> **REQ-QERDS-5.2.1.1-01 The QERDSP shall verify the identity of the sender and the recipient either directly or by relying on a third party:**
>
> **a) by the physical presence of the natural person or of an authorized representative of the legal person; or**
>
> **b) remotely, using electronic identification means, for which a physical presence of the natural person or of an authorized representative of the legal person was ensured and which meets the requirements set out in Article 8 of the Regulation (EU) N° 910/2014 with regard to the assurance levels 'substantial' or 'high'; or**
>
> **c) by means of a certificate of an advanced electronic signature or of an advanced electronic seal; or**
>
> **d) by using other identification methods recognized at national level which provide equivalent assurance in terms of reliability to physical presence. The equivalence of the assurance level shall be confirmed by a conformity assessment body.**
>
> **NOTE: The third party verifying the identity of the sender and the recipient can be another QERDSP in the case that the sender or the recipient or both are subscribed to another QERDSP.**

Editor's note: Mapping the content of the present specification to these requirements is for further study.

B.4 Application of the present specification to ETSI TS 119 431-1 and CEN EN 419 241-1

Editor's note: To be added.

Annex C (informative): Application of the present specification for issuance of eID means related to Regulation (EU) No 910/2014 Article 8

This Annex suggests how an IPSP may use the present specification for the identity proofing steps as specified in clauses 2.1.1, 2.1.2 and 2.2.3 of the Annex of EU CID 2015/1502 [i.3] for the issuance of eID means conforming to the requirements for level **substantial** and **high**.

The requirements of clauses 5 to 8 of the present document, except the requirements marked [ENHANCED], can be considered for the requirements for level substantial as defined by EU CID 2015/1502.

The requirements of clauses 5 to 8 of the present document, including the requirements marked [ENHANCED], can be considered for the requirements for level high as defined by EU CID 2015/1502.

Identity attribute collection and validation must fulfil the requirements of clause 11 and the Annex of EU CIR 2015/1501 [i.2].

NOTE: When an eID is issued according to national requirements, these requirements will be part of the identity proofing context and can influence selection of means conforming to requirements in clause 8 of this specification.

Editor's note: As for Annex B, here we may provide a mapping that shows how the CID 2015/1502 and related guidance requirements are covered by our specifications.

History

Document history		
V0.0.1a	October 2020	First draft as STF internal skeleton document with ToC and some content
V0.0.1.b	November 2020	Draft submitted to ESI#71 meeting for discussion.
V0.0.2	November 2020	Consolidated working draft of STF 25 November 2020.
V0.0.3	December 2020	Working draft for approval by STF before ESI submission
V0.0.4	December 2020	Draft submitted for review by ETSI/ESI 2020.12.03
V0.0.5	December 2020	Draft for public review 2020.12.18