ETSI TS 119 461 V2.1.1 (2025-02)

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

Reference
RTS/ESI-0019461v211

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

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

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.

Introduction

Identity proofing is the process of verifying with the required degree of reliability that the purported identity of an applicant is correct. The scope of the present document is identity proofing of applicants to be enrolled as subjects or subscribers of a Trust Service Provider (TSP).

Identity proofing can be carried out by the TSP as an integral part of the trust service provisioning. It can also be the task of a specialized Identity Proofing Service Provider (IPSP) acting as a subcontractor to the TSP; such a separate IPSP can provide services to several TSPs. The present document applies to both of these scenarios.

The present document aims to meet the general requirements of the international community to provide trust and confidence in electronic transactions, including, amongst others, applicable requirements from both the original eIDAS regulation published in 2014, Regulation (EU) No 910/2014 [i.1], and the amended eIDAS regulation [i.25] incorporating legal amendments approved in 2024 [i.34].

The present document poses policy and security requirements specific to identity proofing covering applicable technologies and use cases, resulting in identity proofing to either a Baseline or an Extended Level of Identity Proofing (LoIP) that are considered applicable to all relevant ETSI trust services standards.

Since neither the original eIDAS regulation [i.1] nor the amended eIDAS regulation [i.25] define identity proofing as a trust service on its own, a specialized IPSP is not a TSP per se, but acts under the responsibility of the TSP that has subcontracted the identity proofing. The IPSP will provide a component of the TSP's trust service, hence the name of the present document refers to policy and security requirements for identity proofing as a trust service component.

1 Scope

The present document specifies policy and security requirements for trust service components providing identity proofing of trust service subjects. Such a trust service component can be provided by the Trust Service Provider (TSP) itself as an integral part of the trust service or by a specialized Identity Proofing Service Provider (IPSP) acting as a subcontractor to the TSP. The term "trust service component" is used because identity proofing is not considered as a trust service on its own but as a component of the trust service for which the identity proofing is done.

The present document provides requirements for two Levels of Identity Proofing (LoIP), Baseline and Extended. These LoIPs aim to support identity proofing for ETSI trust services standards such as ETSI EN 319 411-1 [i.7], ETSI EN 319 411-2 [i.8] and ETSI EN 319 521 [i.12]. The present document also provides requirements to enhance an identity proofing from Baseline LoIP to Extended LoIP when the Baseline LoIP has been reached by use of electronic Identification means (eID) at Level of Assurance (LoA) 'substantial' according to the amended eIDAS regulation [i.25] or a similar LoA based on a comparable assurance level framework.

The present document aims at supporting identity proofing in European and other regulatory frameworks. Specifically, but not exclusively, the Baseline LoIP aims to support identity proofing for qualified certificates as defined in Regulation (EU) No 910/2014 [i.1] (the original eIDAS regulation) Article 24.1, while the Extended LoIP aims to support identity proofing for qualified certificates and qualified attestations of attributes as defined in Articles 24.1, 24.1a, and 24.1b of the amended eIDAS regulation [i.25]. The present document aims to meet the requirements of the original eIDAS regulation [i.1] by the requirements in clause C.2 and the requirements of the amended eIDAS regulation [i.25] by the requirements in clause C.3.

The present document is intended to be applicable for reference from an implementing act according to Article 24.1c of the amended eIDAS regulation [i.25], setting out minimum technical specifications, standards and procedures with respect to the verification of identity and attributes in accordance with Articles 24.1, 24.1a, and 24.1b of the amended eIDAS regulation [i.25].

The present document aims to meet the requirements of Article 44 of the aforementioned regulations on identity proofing for qualified electronic registered delivery services by the requirements in clause C.4. eIDAS has no specific requirements for identity proofing for other qualified trust services.

The present document can be used by Conformity Assessment Bodies (CAB) as the basis for confirming that an organization is trustworthy and reliable in its identity proofing process.

NOTE 1: See ETSI EN 319 403-1 [i.6] for guidance on the assessment of TSP processes and services.

NOTE 2: The present document has the potential to have wider applicability than the defined scope, but any application for other purposes than trust services is out of scope.

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 in the ETSI docbox.

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 Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

[2] ICAO Doc 9303 part 10: "Machine Readable Travel Document - Part 10: Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC)".

[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".

[5] TS 18099: "Biometric data injection attack detection", (produced by CEN).

[6] ISO/IEC 19989-3: "Information security — Criteria and methodology for security evaluation of biometric systems — Part 3: Presentation attack detection".

[7] ETSI TS 119 172-4: "Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists".

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.

NOTE: The eIDAS regulation as published in 2014 and before amendments approved in 2024, sometimes called "eIDAS v1", shorthand notation "original eIDAS regulation".

[i.2] Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication.

[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 Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".

[i.5] ETSI EN 319 102-1: "Electronic Signatures and Trust Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".

[i.6] ETSI EN 319 403-1: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers".

[i.7] 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.8] 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.9] ETSI EN 319 412-2: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons".

[i.10] Void.

[i.11] Void.

[i.12] ETSI EN 319 521: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers".

[i.13] ETSI TS 119 172-1: "Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents".

[i.14] Void.

NOTE: Moved to normative reference [7].

[i.15] ENISA: "Remote ID proofing - Analysis of methods to carry out identity proofing remotely", February 2021.

[i.16] ISO/IEC 30107-1: "Information technology — Biometric presentation attack detection — Part 1: Framework".

[i.17] Void.

NOTE: Moved to normative reference [4].

[i.18] Void.

NOTE: Moved to normative reference [6].

[i.19] ISO/IEC TS 29003: "Information technology — Security techniques — Identity proofing".

[i.20] Facial Identification Science Working Group (FISWG): "Facial Comparison Overview and Methodology Guidelines", Version 1.0, October 2019.

[i.21] Facial Identification Science Working Group (FISWG): "Facial Image Comparison Feature List for Morphological Analysis", Version 2.0, September 2018.

[i.22] Facial Identification Science Working Group (FISWG): "Minimum Training Criteria for Assessors Using Facial Recognition Systems", Version 1.0, July 2020.

[i.23] European Network of Forensic Science Institutes (ENFSI): "Best Practice Manual for Facial Image Comparison", ENFSI-BPM-DI-01, Version 01, January 2018.

[i.24] ISO/IEC 15408-1: "Information technology — Security techniques — Evaluation criteria for IT security - Part 1: Introduction and general model".

[i.25] Regulation (EU) No 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, consolidated version: 18/10/2024.

NOTE: The eIDAS regulation including the amendments of Regulation (EU) 2024/1183 [i.34], sometimes called "eIDAS v2", shorthand notation "amended eIDAS regulation".

[i.26] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

[i.27] Public Register of Authentic Travel and Identity Documents Online (PRADO): "Glossary - Technical terms related to security features and to security documents in general".

[i.28] ENISA: "Methodology for Sectoral Cybersecurity Assessments", EU Cybersecurity Certification Framework, September 2021.

[i.29] ISO/IEC 19792: "Information technology — Security techniques — Security evaluation of biometrics".

[i.30] ISO/IEC 19989-1: "Information security — Criteria and methodology for security evaluation of biometric systems — Part 1: Framework".

[i.31] Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services.

[i.32] ISO/IEC FDIS 29794-5: "Information technology — Biometric sample quality — Part 5: Face image data".

[i.33] ISO/IEC DIS 20059: "Information technology — Methodologies to evaluate the resistance of biometric recognition systems to morphing attacks".

[i.34] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.

3 Definition of terms, symbols, abbreviations and notations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TR 119 001 [i.4], ETSI EN 319 401 [1] and the following apply:

amended eIDAS regulation: Regulation (EU) No 910/2014 as amended by Regulation (EU) 2024/1183 and Directive (EU) 2022/2555

NOTE: The combination of the original eIDAS regulation [i.1] published in 2014 and the identified amendments approved in 2024, sometimes called "eIDAS v2" - see **original eIDAS regulation** below.

applicant: person (legal or natural) whose identity is to be proven

attack potential: measure of the effort needed to exploit a vulnerability in a Target Of Evaluation (TOE)

NOTE: Source ISO/IEC 15408-1 [i.24], which has the following note to the definition: The effort is expressed as a function of properties related to the attacker (e.g. expertise, resources, and motivation) and properties related to the vulnerability itself (e.g. window of opportunity, time to exposure).

Attack Presentation Classification Error Rate (APCER): proportion of attack presentations using the same presentation attack instrument species incorrectly classified as bona fide presentations in a specific scenario

NOTE: Source ISO/IEC 30107-3 [3]. Measure for rate of successful presentation attacks.

attended remote identity proofing: identity proofing process by remote use of identity document where the capture of the identity document (physical or digital document) and the face video of the applicant are performed in a session supervised by a registration officer

authentic source: repository or system, held under the responsibility of a public sector body or private entity, that contains and provides attributes about a natural or legal person or object and that is considered to be a primary source of that information or recognized as authentic in accordance with Union or national law, including administrative practice

NOTE: Source amended eIDAS regulation [i.25]. In the present document, the term "trusted register" is used as the general term while "authentic source" is used where the scope is explicitly the eIDAS legal context.

authoritative evidence: evidence that is presented by the applicant, holds identifying attribute(s) of the identity, and is trusted for the binding of these attributes to the applicant

NOTE: In the present document, authoritative evidence for a natural person is a physical or digital identity document, an eID used for authentication, and a certificate of a digital signature. For a legal person, documents and attestations are typically used as authoritative evidence.

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 CIR (EU) 2015/1502 [i.3]. Authoritative evidence is an authoritative source, but also trusted register and other sources can be authoritative sources. Use can be to supply more attributes than those obtained from authoritative evidence, to validate attributes obtained from different sources, and to provide more updated attributes than those obtained from authoritative evidence.

(identity) attribute: characteristic, quality, right or permission of a natural or legal person or of an object

NOTE: Source amended eIDAS regulation [i.25].

Baseline LoIP: Level of Identity Proofing (LoIP) reaching a substantial level of confidence based on the fulfilment of good practice minimum requirements for the identity proofing process

NOTE: This level is considered suitable for identity proofing for the NCP policy level defined in ETSI EN 319 411-1 [i.7] and for issuing qualified certificates according to the original eIDAS regulation [i.1].

binding to applicant: part of an identity proofing process that verifies that the applicant is the person identified by the presented evidence

Bona fide Presentation Classification Error Rate (BPCER): proportion of bona fide presentations incorrectly classified as presentation attacks in a specific scenario

NOTE: Source ISO/IEC 30107-3 [3]. Measure of genuine presentations incorrectly classified as presentation attacks.

digital identity document: identity document that is issued in a machine-processable form, that is digitally signed by the issuer, and that is in purely digital form

NOTE 1: Machine-processable, in this case, does not include optical scanning and processing of a physical identity document.

NOTE 2: A digital identity document can be contained in a physical identity document, e.g. an eMRTD contained in a passport or national identity card.

NOTE 3: The eMRTD part of a passport or national identity card is sometimes called "electronic identity" or even "eID". In the present document, this part of a passport or national identity card is a digital identity document.

electronic attestation of attributes: attestation in electronic form that allows attributes to be authenticated

NOTE: Source amended eIDAS regulation [i.25]. In the present document, the term "attestation" is used as the general term while "(qualified) electronic attestation of attributes" is explicitly used in the eIDAS legal context.

electronic Identification means (eID means, eID): material and/or immaterial unit containing person identification data and which is used for authentication for an online service or, where appropriate, for an offline service

NOTE: Source amended eIDAS regulation [i.25].

eID scheme: governance model and technical specifications allowing interoperability between eID means from different eID providers

eIDAS certified eID: eID or eID scheme certified according to Article 12a of the amended eIDAS regulation

eIDAS high eID: eID or eID scheme fulfilling the requirements for assurance level high in Article 8 of the amended eIDAS regulation and CIR (EU) 2015/1502

eIDAS notified eID: eID or eID scheme notified according to Article 9 of the amended eIDAS regulation

eIDAS signature validation: validation of an electronic signature or electronic seal in compliance with the eIDAS regulation

NOTE: Requirements for validation of signatures and seal are set by Article 32 of the amended eIDAS regulation [i.25]. The text of Article 32 is the same in the original [i.1] and the amended eIDAS regulation [i.25].

eIDAS substantial eID: eID or eID scheme fulfilling the requirements for assurance level substantial in Article 8 of the amended eIDAS regulation and CIR (EU) 2015/1502

NOTE: The text of Article 8 and Article 9 is the same in the original [i.1] and the amended [i.25] eIDAS regulation. CIR (EU) 2015/1502 [i.3] has not changed with the amended eIDAS regulation [i.25].

(identity) evidence: information or documentation provided by the applicant or obtained from other sources, trusted to prove that claimed identity attributes are correct

extended LoIP: Level of Identity Proofing (LoIP) reaching a high level of confidence based on the fulfilment of good practice minimum requirements for the identity proofing process

NOTE: This level is considered suitable for identity proofing for issuing of qualified certificates and qualified electronic attestations of attributes according to the amended eIDAS regulation [i.25].

False Acceptance Rate (FAR): proportion of verification transactions with false biometric claims erroneously accepted

NOTE: Source ISO/IEC 19795-1 [4].

False Rejection Rate (FRR): proportion of verification transactions with true biometric claims erroneously rejected

NOTE: Source ISO/IEC 19795-1 [4].

freshness: time between time of issuance of an evidence and time of use/validation of the evidence

high attack potential: measure of the effort needed by a highly skilled adversary with significant resources and opportunity to exploit a vulnerability in a Target Of Evaluation (TOE)

NOTE: Based on ENISA: "Methodology for Sectoral Cybersecurity Assessments" [i.28].

identity: attribute or set of attributes that uniquely identify a person within a given context

identity document: physical or digital identity document issued by an authoritative source and attesting to the applicant's identity

identity proofing context: external requirements affecting the identity proofing process, given by the purpose of the identity proofing, the related regulatory requirements, and any resulting restrictions on the selection of attributes and evidence and on the identity proofing process itself

identity proofing (process): process by which the identity, and possibly additional attributes, of an applicant is verified by the use of evidence attesting to the required identity attributes

identity proofing service policy: set of rules that indicates the applicability of an identity proofing service to a particular community and/or class of application with common security requirements

injection attack: attack consisting of injecting content controlled by the attacker into the data capture process

EXAMPLE: Bypassing the camera on the user device injecting a recorded or generated video stream purporting to come from the camera. A generated video stream can be a deep fake video of a face or of the visual appearance of a physical identity document.

Injection Attack Detection (IAD): automated determination of an injection attack

legitimate evidence holder: person for whom the evidence is issued

Level of Identity Proofing (LoIP): confidence achieved in the identity proofing

NOTE 1: Source ISO/IEC TS 29003 [i.19].

NOTE 2: In the present document, the term applies to the Baseline LoIP and the Extended LoIP.

liveness detection: measurement and analysis of anatomical characteristics or involuntary or voluntary reactions, to determine if a biometric sample is being captured from a living subject present at the point of capture

NOTE: Source ISO/IEC 30107-1 [i.16]. Liveness detection is a subset of presentation attack detection.

moderate attack potential: measure of the effort needed by a skilled adversary with significant resources and opportunity to exploit a vulnerability in a Target Of Evaluation (TOE)

NOTE: Based on ENISA: "Methodology for Sectoral Cybersecurity Assessments" [i.28].

original eIDAS regulation: Regulation (EU) No 910/2014 as published in 2014 and without the amendments approved in 2024

NOTE: Sometimes called "eIDAS v1" - see **amended eIDAS regulation** above.

physical identity document: identity document issued in physical and human-readable form

EXAMPLE: The printed (non-digital) representation of passports and national identity cards.

physical presence: identity proofing where the applicant is required to be physically present at the location of the identity proofing

(IPSP) practice statement: statement of the practices that an IPSP employs in providing the identity proofing trust service component

NOTE: Source ETSI EN 319 401 [1].

presentation attack: presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system

NOTE: Source ISO/IEC 30107-1 [i.16].

Presentation Attack Detection (PAD): automated determination of a presentation attack

NOTE: Source ISO/IEC 30107-1 [i.16].

proof of access: any source irrespective of its form that can be trusted for reliable data, information and/or evidence that can be used in an identity proofing process, provided that the applicant is able to demonstrate access to the source

EXAMPLE: Bank account, phone number, email or other resource owned by the applicant.

pseudonym: fictitious identity that a person assumes for a particular purpose, which differs from their original or true identity

NOTE: A pseudonym identity can, as opposed to an anonymous identity, be linked to the person's real identity.

qualified electronic seal: advanced electronic seal, which is created by a qualified electronic seal device, and that is based on a qualified certificate for electronic seal

NOTE: Source amended eIDAS regulation [i.25].

qualified electronic signature: advanced electronic signature, which is created by a qualified electronic signature device, and that is based on a qualified certificate for electronic signature

NOTE: Source amended eIDAS regulation [i.25].

registration officer: human being carrying out all or selected parts of an identity proofing process

remote identity proofing: identity proofing process where the applicant is physically distant from the location of the identity proofing

subject: legal or natural person that is enrolled to a trust service

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

supplementary evidence: evidence that is used in addition to authoritative evidence to strengthen the reliability of the identity proofing and/or as evidence for attributes that are not evidenced by the authoritative evidence

trusted register: public register, database, or other source that is an authoritative source for the conveyance of identity attributes in the identity proofing context

trust service component: one part of the overall service of a TSP

NOTE 1: Source ETSI EN 319 403-1 [i.6].

NOTE 2: A typical example of such component services are those identified in clause 4.4 of ETSI EN 319 411-1 [i.7], where an IPSP as a subcontractor to a TSP will take on all or core parts of the registration service component.

unattended remote identity proofing: identity proofing process by remote use of identity document where the capture of the identity document (physical or digital document) and the face video of the applicant are performed in an automated, interactive session without human supervision

NOTE: Validation of the captured evidence and binding to applicant can afterwards be done by manual, hybrid manual and automated, and fully automated means.

validation: part of an identity proofing process that determines whether or not attributes are validated by the presented evidence and whether or not the evidence is genuine, authoritative, and valid

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TR 119 001 [i.4] and the following apply:

AI	Artificial Intelligence
APCER	Attack Presentation Classification Error Rate
BPCER	Bona fide Presentation Classification Error Rate
CAB	Conformity Assessment Bodies
EAA	Electronic Attestation of Attributes
eID	electronic Identification
eMRTD	electronic Machine Readable Travel Document
ENISA	European Cybersecurity Agency
FAR	False Acceptance Rate
FRR	False Rejection Rate
GDPR	General Data Protection Regulation
IAD	Injection Attack Detection
ICAO	Internation Civil Aviation Organization
IPSP	Identity Proofing Service Provider
LEI	Legal Entity Identifier
LoA	Level of Assurance
LoIP	Level of Identity Proofing
MRZ	Machine Readable Zone
NCP	Normalized Certificate Policy
OID	Object IDentifier
PAD	Presentation Attack Detection
PRADO	Public Register of Authentic travel and identity Documents Online
QERDS	Qualified Electronic Registered Delivery Service
QTSP	Qualified Trust Service Provider
TLS	Transport Layer Security
TSP	Trust Service Provider

3.4 Notations

The requirements identified in the present document include:

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

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

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)
- **INI:** Requirements on the initiation of the identity proofing
- **COL:** Requirements on attribute and evidence collection
- **VAL:** Requirements on attribute and evidence validation
- **BIN:** Requirements on binding to applicant
- **ISS:** Requirements on issuing of result of the identity proofing and evidence of the identity proofing process
- **USE:** Requirements on use cases
- **QTS:** Requirements specific to identity proofing for EU qualified trust services (Annex C)

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 at the start of a clause, the 2 digit number 00 is used.
- 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 a deleted requirement is left and completed with "VOID".
- When a requirement is modified from the previous edition of the present document, the requirement number is amended by a capital 'X' letter.

4 General concepts

4.1 Identity proofing actors

Neither the original eIDAS regulation [i.1] nor the amended eIDAS regulation [i.25] define identity proofing as a trust service on its own. In the present document, identity proofing is defined as a trust service component. The identity proofing service component can be an integral part of the Trust Service Provider's (TSP) service provisioning, but the service component can also be the task of a specialized Identity Proofing Service Provider (IPSP) acting as a subcontractor to the TSP under the TSP's responsibility. The present document is applicable to both of these scenarios.

An IPSP as a specialized service provider can provide identity proofing subcontracted to many different TSPs as well as to other types of service providers.

The main actors of an identity proofing process are the TSP that requests the identity proofing and is the receiver of the identity proofing result, where relevant the IPSP that delivers the identity proofing service subcontracted to the TSP, and the applicant whose identity is to be proven. The applicant can be a natural person, a legal person, or a natural person representing a legal person. If the identity proofing process uses manual procedures, these procedures are carried out by personnel in the role of registration officer.

4.2 Identity proofing process

Identity proofing is the process of proving with the required degree of reliability that the purported identity of an applicant is correct. In the present document, the required degree of reliability is assumed to be either the Baseline LoIP or the Extended LoIP.

The applicant is identified by a set of identity attributes, and evidence is provided to link these attributes to the applicant. Especially for Electronic Attestation of Attributes (EAA), further identifying or non-identifying attributes can be collected and linked to the applicant; the term identity proofing as used in the present document covers proofing of such additional attributes where relevant. The identity proofing process can be carried out automated, by a registration officer, or by a combination of human-controlled and automated. The identity proofing process can be based on the physical presence of the applicant, or on remote identity proofing based on remote communication with the applicant using a communications network. The different approaches imply different risks. For each approach, the present document sets the minimum requirements to mitigate those risks to reach either Baseline or Extended LoIP.

The identity proofing process is commonly broken down into five tasks:

1) Initiation.
2) Attribute and evidence collection.
3) Attribute and evidence validation.
4) Binding to applicant.
5) Issuing of identity proofing result.

The subsequent use of the identity proofing result by a TSP or other type of service provider is out of scope of the present document.

EXAMPLE 1: A typical case is issuing of a digital signature certificate for the proven identity.

The process can be illustrated by Figure 1 (from [i.15]), also showing that an identity proofing process can be iterative. 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. An identity proofing process can be synchronous, meaning that all steps of the identity proofing process, including issuing of proof, are carried out in one continuous process, or asynchronous, where the validation and binding tasks and issuing of proof are done at a later time.

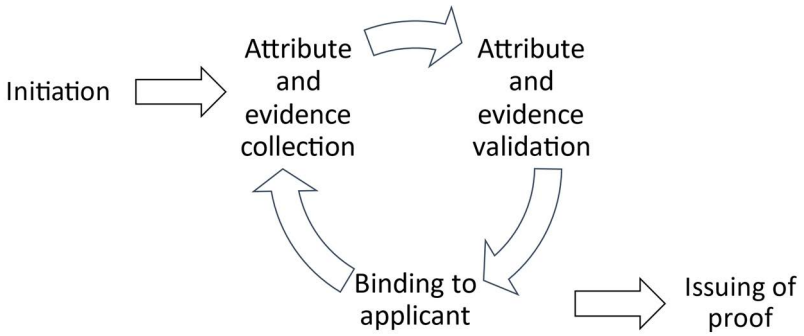

Figure 1: Tasks of an identity proofing process

The present document covers initial identity proofing of a new applicant to become a subject or a subscriber of a trust service. The present document does not consider possible simplifications of the process if the applicant is a known subject, e.g. in cases where identity proofing is required to 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 the risk or the likelihood that the identity is correct. In such cases, the reliability of the correct identity of a subject can increase or decrease over time. Continuous identity proofing is out of the scope of the present document.

The present document poses requirements to identity proofing processes in the following structured manner.

Clause 5 has requirements for risk assessment and threats intelligence to ensure the IPSP's service stays up to date.

Clause 6 states requirements on identity proofing services practice statement, terms and conditions, and information security policy.

Clause 7 sets requirements for service management and operation, requiring an IPSP to adhere to the same requirements as a TSP.

Clause 8 is structured into subclauses that serve as building blocks for different identity proofing use cases:

- Clause 8.1 states requirements for initiation of an identity proofing process.
- Clause 8.2 states requirements for the collection of attributes, meaning the identity information to prove, and for collection of the evidence needed to prove the identity attributes.
- Clause 8.3 states requirements for validation of attributes against the provided evidence and requirements to ensure that the evidence in itself is genuine and valid.
- Clause 8.4 states requirements for binding to applicant, meaning ensuring that the applicant presenting the authoritative evidence really is the person identified by the evidence. Binding to applicant can be done manually by a registration officer, or automated, notably by face biometrics for natural persons, or by a combination of manual and automated. Other biometric modes than face are currently out of scope of the present document.
- Clause 8.5 states requirements for issuing the identity proofing result and for the creation of evidence of the identity proofing process to be able to prove in retrospect why the identity proofing process yielded the given identity proofing result.

Clause 9 sets requirements for the combination of the building blocks from clause 8 into some typical identity proofing use cases that are considered to fulfil the requirements for the Baseline and Extended LoIP. Requirements are specified for six use cases and sub-cases when the applicant is a natural person:

1) Use of an identity document in a physical presence context:
    a) Manual operation.
    b) Hybrid manual and automated operation.
    c) Automated operation.
2) Use of an identity document in an attended remote context, where the applicant presents an identity document in a remote session and communicates in real-time with a registration officer:
    a) Manual operation with validation and binding to applicant done manually by the registration officer - only accepted for Baseline LoIP.
    b) Hybrid manual and automated operation.
3) Use of an identity document in an unattended remote context, where the applicant presents an identity document in a remote session without human supervision:
    a) Manual operation with validation and binding to applicant done afterwards by a registration officer - only accepted for Baseline LoIP.
    b) Hybrid manual and automated operation with validation and binding to applicant done afterwards by a combination of automated analysis and a registration officer.
    c) Automated operation with no involvement of a registration officer.

4) Use of eID means.

5) Use of digital signature with certificate.

6) Additional identity proofing to enhance an identity proven to Baseline LoIP by use of eID means to Extended LoIP.

Table 1 below shows an overview of the use cases for use of identity documents for identity proofing.

Table 1: Use cases for identity proofing using identity documents

Applicant presence	Operation	Clause	Identity document	Evidence validation	Binding to applicant	Example
Physical	Manual	9.2.1.2	Physical	Manual	Manual	Manual enrolment at registration office.
	Hybrid	9.2.1.3	Digital	Automated	Manual	Similar to manual border control, with automated validation of digital doc. and manual face verification by registration officer.
	Automated	9.2.1.4	Digital	Automated	Automated	Similar to unassisted border control with automated validation of digital doc. and biometric face verification.
Remote attended	Manual	9.2.2.2	Physical	Manual	Manual	Manual enrolment at a virtual registration office where registration officer manually verifies physical doc. and face - only for Baseline LoIP.
	Hybrid	9.2.2.3	Digital	Automated	Manual	Manual enrolment at a virtual registration office with automated validation of digital doc. and manual face verification.
			Digital	Automated	Combined manual and automated	Manual enrolment at a virtual registration office with automated validation of digital doc. and both biometric and manual face verification.
			Physical	Combined automated and manual	Manual	Manual enrolment at a virtual registration office with both automated and manual validation of doc. and manual face verification.
			Physical	Combined automated and manual	Combined automated and manual	Manual enrolment at a virtual registration office with both automated and manual validation of doc. and both manual and biometric face verification.

Applicant presence	Operation	Clause	Identity document	Evidence validation	Binding to applicant	Example
Remote unattended	Manual	9.2.3.2	Physical	Manual	Manual	Remote enrolment process, with subsequent manual verification of doc. and manual face verification - only for Baseline LoIP.
	Hybrid	9.2.3.3	Digital	Automated	Manual	Remote enrolment process with automated validation of digital doc. and subsequent manual face verification - only for Baseline LoIP.
			Digital	Automated	Combined manual and automated	Remote enrolment process with automated validation of digital doc. and subsequent both manual and biometric face verification.
			Physical	Combined automated and manual	Manual	Remote enrolment process with subsequent both automated and manual validation of doc. and manual face verification - only for Baseline LoIP.
			Physical	Combined automated and manual	Combined automated and manual	Remote enrolment process with subsequent both automated and manual validation of doc. and both manual and biometric face verification.
	Automated	9.2.3.4	Digital	Automated	Automated	Fully automated process.

Annex B provides (from [i.15]) an overview of typical threats to identity proofing and how the present document addresses these threats.

Annex C further profiles the use cases of clause 9 specifically for identity proofing to support EU qualified trust services according to both the original eIDAS regulation [i.1] and the amended eIDAS regulation [i.25].

To claim compliance with the present document, an IPSP is obliged to identify the use case(s) from clause 9 and/or Annex C that the IPSP applies in its service, and fulfil all relevant requirements from the present document for each use case.

Automated operation is considered not relevant to the attended remote case since a registration officer is anyway needed for communication with the applicant. For the unattended remote case, while the communication with the applicant is automated, the tasks of validation and binding to applicant can be done by all the three alternatives manual, hybrid, or automated. Manual only validation of a physical identity document is considered to only be able to reach Baseline LoIP. For the unattended remote case, manual only binding to applicant is considered to only be able to reach Baseline LoIP.

Use of hybrid manual and automated operation is strongly encouraged for both validation of physical identity document and binding to applicant. Fully automated, remote operation with use of an identity document requires the use of a digital identity document and face biometrics for binding to applicant.

An identity proofing context can pose limitations on the selection of use cases to apply. Clause 8 specifies means that can be combined into identity proofing use cases in a flexible way to be able to fulfil restrictions imposed by a wide variety of identity proofing contexts. Other use cases than those specified in clause 9 can be possible to achieve the Baseline or Extended LoIP, notably when specific combinations of different evidence are required by an identity proofing context.

The present document does not pose requirements on the process flow of an identity proofing process. Each of the use cases specified in clause 9 can be fulfilled by various process flows leading to the same LoIP result.

The building block structure of clause 8 ensures that requirements regarding specific means are consistent across identity proofing use cases.

EXAMPLE 2: All use cases that use physical identity document as evidence will adhere to the same set of base requirements, whether the physical identity document is used with physical presence, remote with automated validation, or remote with manual validation, but conditional requirements are used where use cases differ. For example, some checks of a physical identity document are only possible with physical presence.

4.3 Identity proofing context

The identity proofing context is the set of external framing conditions that an identity proofing process is subject to and that can impose requirements and restrictions on identity proofing. A core element of the identity proofing context is the regulatory requirements imposed on identity proofing for the defined purpose by the applicable legislation.

EXAMPLE 1: Issuing of qualified certificates for electronic signatures in the EU is subject to the requirements of the amended eIDAS regulation [i.25] and possibly additional requirements from the national legislation of the country where the TSP is registered.

The identity proofing context will vary between purposes of identity proofing and between countries. The identity proofing context can restrict at least the following aspects of an identity proofing process:

- The required LoIP, assumed to be Baseline or Extended as defined by the present document.
- The identity attributes to collect, meaning attributes that are mandatory, prohibited, or optional.

EXAMPLE 2: In some countries, the collection of a national identity number can be mandatory for the identity proofing context, while other countries do not use such numbers or the use of the national identity number is prohibited for most identity proofing contexts.

- The evidence to use, meaning evidence or combinations of evidence that can be mandated or prohibited by legislative rules or that can be assumed to be available.

EXAMPLE 3: National legislation can restrict identity documents to passports and national identity cards from the same country or from selected countries.

EXAMPLE 4: In some countries, validation of identity attributes against a national population register can be mandatory, while other countries do not have such registers.

EXAMPLE 5: In some countries, all citizens can be assumed to possess a national identity card, while other countries do not issue such cards.

- The means to use for attribute and evidence validation and for binding to applicant, meaning that certain process steps can be mandated or prohibited.

EXAMPLE 6: In some countries, physical presence can be mandated for certain purposes of identity proofing, or remote identity proofing can be restricted to allow only specific use cases.

- The issuing of the result of the identity proofing process and the evidence of the identity proofing process, meaning what information can be conveyed to the TSP and what information can be retained as evidence of the process.

EXAMPLE 7: In some countries, a photo or photocopy of a physical identity document can be required as part of the evidence of the identity proofing process, while in other countries retaining such copies can be prohibited.

Specification of identity proofing contexts is out of the scope of the present document, but the present document is intended to provide means to fulfil the requirements of a wide variety of identity proofing contexts.

4.4 Authoritative evidence and supplementary evidence

An identity proofing process requires authoritative evidence on the identity of the applicant. Authoritative evidence is issued by an authoritative source and is hence trusted regarding the identity attributes the evidence conveys and for the binding of these attributes to the applicant presenting the evidence.

When the applicant is a natural person or a natural person representing a legal person, an identity proofing process compliant with the present document uses at least one of the following types of evidence as authoritative evidence: physical identity document, digital identity document, eID means used in an authentication protocol, or certificate of a digital signature. Use of these evidence types as authoritative evidence requires fulfilment of the relevant requirements of the present document.

NOTE: This does not exclude the case where identity proofing for a trust service is done by a government authority, e.g. issuing of a (qualified) certificate in conjunction with issuing of a national identity card. If the identity proofing process is sufficient to issue an identity document that could subsequently be used in identity proofing for a trust service, then the process in itself is clearly also sufficient for identity proofing for the same trust service.

The present document additionally specifies the use of the following as supplementary evidence: trusted register (including authentic source as defined by the amended eIDAS regulation [i.25]), proof of access (in particular of a bank account), and documents and attestations (including electronic attestation of attributes as defined by the amended eIDAS regulation [i.25]).

Depending on the identity proofing context, such supplementary evidence can be the authoritative source for identity attributes, but, as specified by the present document, only when combined with the use of one of the authoritative evidence types listed above.

EXAMPLE 1: A national population register can be considered as the authoritative source for information about the applicant, but only if the applicant's identity is additionally proven by one of the authoritative evidence listed above.

EXAMPLE 2: In certain identity proofing contexts, identity information obtained from a bank can be regarded as authoritative.

None of the authoritative evidence identity document, eID means, and digital signature can be expected to be commonly available for legal persons. While the use of eID means and digital signature is not ruled out, trusted register and documents and attestations are expected to take an authoritative role. Hence, the identity proofing use case for a legal person in clause 9.3 of the present document does not mandate use of any of the authoritative evidence types.

Multiple evidence of the same type or different types can be used. Other evidence in addition to those covered by the present document can be used.

4.5 Consideration of threats

The requirements in the present document are provided in the form of requirements (numbered controls) that aim to achieve **security objectives** perceived necessary to address operational risks (clauses 6 and 7) as well as the inherent risks specific to identity proofing (clauses 8 and 9). These specific risks result from two main categories of threats, namely:

1) The imposter attempts to use **falsified or counterfeited evidence**, meaning the evidence is fake or has been tampered with in order for the applicant to obtain an approved identity proofing with an incorrect identity. This can be the real identity of another person or a non-existent identity.

2) The imposter attempts an **impersonation**, meaning the imposter uses genuine evidence associated with another person in order to obtain an approved identity proofing under this other person's identity.

Two other categories of threats are in scope:

1) **Attacks on the system** where the imposter breaks the security of the information systems used for identity proofing to illegitimately change information or enforce a specific identity proofing result.

2) **Social engineering** where the imposter misleads or forces the legitimate owner of the evidence to carry out the identity proofing in a way that results in the imposter obtaining control of credentials issued as a result of the identity proofing.

Figure 2 summarizes typical attack scenarios for falsified/counterfeited evidence and impersonation and the related countermeasures specified by the present document.

Two specific attack types of concern for remote identity proofing using identity documents are:

- Presentation attack, where use of falsified or counterfeited evidence or impersonation is attempted in front of the camera used to capture evidence.
- Injection attack, where camera or other sensors are bypassed injecting recorded or artificially generated video streams as falsified or counterfeited evidence or impersonation.

Artificially generated content, also called "deep fakes", is increasingly used by imposters. This can be a deep fake of a victim's face or an artificially generated representation of a physical identity document showing a victim's identity. An attacker needs to combine artificially generated content with presentation or injection attack. State of the art in artificially generated content is rapidly evolving, including artificial intelligence based logic, such as "face swapping", to react in real time to instructions such as movements or speech. At the same time, protection measures, also based on artificial intelligence, are rapidly evolving to detect deep fakes. Protection measures include both prevention of presentation and injection attacks and detection of the same types of attacks and of deep fakes.

		Related attack	Countermeasures
FALSIFIED OR COUNTERFEITED EVIDENCE		The identity proofing process is compromised by the use of evidence of insufficient quality	**AUTHORITATIVE EVIDENCE** Use authoritative (trusted) sources Use the required set of attributes allowing unique identification ***ADRESSED IN CLAUSE 8.2***
		The identity proofing process is compromised by counterfeited and/or manipulated evidence	**GENUINE EVIDENCE** Verify the security features and/or assurance level of the evidence ***ADRESSED IN CLAUSE 8.3***
		The identity proofing process is compromised by use of evidence that is terminated, revoked or reported as lost/stolen	**VALID EVIDENCE** Verify that the evidence is still valid, have not been revoked or declared lost/stolen ***ADRESSED IN CLAUSE 8.3***
	IMPERSONATION	The identity proofing process is compromised by manipulation of image capturing systems or transmission channels (for remote identity proofing)	**SECURE COLLECTION AND TRANSMISSION OF EVIDENCE AND APPLICANT APPEARANCE (see note)** Use solutions that ensure authenticity and integrity of evidence from capture to the system that does the validation. Similarly for capture and transmission of the applicant's appearance where relevant. ***ADRESSED IN CLAUSES 8.3 and 8.4***
		The identity proofing process is compromised by an imposter claiming the legitimate identity of another person	**LEGITIMATE OWNERSHIP** Ensure that only the legitimate holder of the evidence can claim the identity ***ADRESSED IN CLAUSE 8.4***

NOTE: The secure collection and transmission of evidence dimension only applies to remote identity proofing and addresses both the falsified or counterfeited evidence and impersonation threats.

Figure 2: Risks and countermeasure for identity proofing

Following the EU Cybersecurity Act [i.26], it can be expected that the whole or parts of an identity proofing system or service serving the EU market in the future will become subject to European cybersecurity certification. Especially, this can be expected for biometrics, where CEN TC/224 WG18 is in the process of developing a multi-part standard for "European requirements for biometric products". TS 18099 [5] "Biometric data injection detection" can also be referenced from a European certification scheme. Several ISO/IEC standards cover testing of biometric systems, e.g. ISO/IEC 19792 [i.29] and ISO/IEC 19795-1 [4], ISO/IEC 30107 Parts 1 [i.16] and 3 [3], and ISO/IEC 19989-1 [i.30]. The Cybersecurity Act specifies three assurance levels for certification, 'basic', 'substantial', and 'high'. Identity proofing for EU qualified trust services could in the future be subject to certification at assurance level 'high', which will imply requirements for testing and certification by independent, accredited laboratories under the auspices of an accredited cybersecurity certification body. This could apply to all of manual, automated, and hybrid manual/automated services.

The present document requires an IPSP's means for biometric injection attack detection and presentation attack detection to go through independent testing by an accredited laboratory every second year. To allow IPSPs, laboratories, and national accreditation authorities reasonable time to prepare for these requirements, the time for the first independent testing is set to before end of 2026. As the European cybersecurity certification system and related standards evolve, this can be referenced from future versions of the present document.

The present document poses requirements for an IPSP to perform cyberthreat intelligence, keep the security of the service updated according to changes in the threats and risk landscape, and to test security and performance. No normative requirements on how to perform these tasks are defined in the present document, but a good reference, also considering preparation for possible cybersecurity certification schemes, is the ENISA report "Methodology for sectoral cybersecurity assessments" [i.28] under the EU Cybersecurity Certification Framework. The report covers topics such as cyberthreat intelligence, types of attackers, characterization of attackers, and attack potential.

More detailed examples of threats are provided in Annex B, based on ENISA's report "Remote ID proofing - Analysis of methods to carry out identity proofing remotely" [i.15], with an indication of coverage by the countermeasures specified by the present document. Annex B can help organizations relying on an identity proofing process to assess the requirements of the present document against the organization's risk assessment for the identity proofing.

4.6 Identity proofing service policy

When identity proofing is provided by an IPSP subcontracted to the TSP, the IPSP can define an identity proofing service policy that describes what is offered, and that can contain diverse information beyond the scope of the present document. An identity proofing service policy can indicate the applicability of the identity proofing service component and the identity proofing contexts to which the identity proofing service component can be applied. The recipients of the policy can be the TSPs and other actors that the IPSP provides its services to, and Conformity Assessment Bodies (CAB) performing audits of the IPSP and the concerned TSPs.

The present document can be referred by an identity proofing service policy to provide information about the LoIP of the service.

An IPSP conforming to the present document's normative requirements for Baseline LoIP or Extended LoIP for at least one use case defined in clause 9 or Annex C of the present document may use in its documentation the following specific Object Identifiers (OID) in addition to reference to the specific use cases from clause 9 and/or Annex C of the present document supported by the IPSP:

- itu-t(0) identified-organization(4) etsi(0) IDENTITY-PROOFING-policies(19461) policy-identifiers(1) baseline(1)
- itu-t(0) identified-organization(4) etsi(0) IDENTITY-PROOFING-policies(19461) policy-identifiers(1) extended(2)

5 Operational risk assessment

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

NOTE 1: When the identity proofing is done by the TSP itself, the TSP's risk assessment can cover the identity proofing.

OVR-5-02: The IPSP's risk assessment shall be updated yearly.

OVR-5-03: The IPSP's risk assessment shall cover relevant risks related to identity proofing and at least:

a) An assessment of the risks related to identity fraud; and

b) An assessment of the risks related to information systems security.

OVR-5-04: The IPSP's risk assessment shall be updated if an identity proofing process is changed.

OVR-5-05: The IPSP shall have a documented and effective procedure for threats intelligence that ensures that the IPSP's service is adapted to new threats.

EXAMPLE: Based on the ENISA report "Methodology for sectoral cybersecurity assessments" [i.28].

OVR-5-06: The IPSP's risk assessment shall be updated according to findings from the threats intelligence procedure.

[CONDITIONAL] OVR-5-07: If the Baseline LoIP is claimed, the risk assessment shall consider at least attackers with moderate attack potential.

[CONDITIONAL] OVR-5-08: If the Extended LoIP is claimed, the risk assessment shall consider at least attackers with high attack potential.

NOTE 2: See clause 3.1 of the present document for definitions of moderate and high attack potential. The ENISA report "Methodology for sectoral cybersecurity assessments" [i.28], clauses 5 (especially clause 5.4) and 9 can be used as basis for describing attack potential.

OVR-5-09: Based on findings from the threats intelligence procedure and changes to the risk assessment, the need for training of personnel shall be assessed and training be carried out if needed.

OVR-5-10: The IPSP shall state in its practice statement goals for quality and security in terms of resilience to false acceptance and false rejection of applicants and perform regular testing of the performance against these goals.

NOTE 3: While false acceptance and rejection are terms normally used for biometrics, the terms in this requirement apply to all use cases of clause 9 and Annex C of the present document, e.g. including physical presence.

6 Policies and practices

6.1 Identity proofing service practice statement

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

OVR-6.1-02: An IPSP claiming compliance with the present document shall identify in its practice statement the use cases for which compliance is claimed.

NOTE 1: When the identity proofing is done by the TSP itself, the TSP's practice statement can cover the information on the identity proofing and there is no need for a specific practice statement for identity proofing.

OVR-6.1-03: Identification of use cases for which compliance is claimed shall be by reference to specific parts of clause 9 and/or Annex C of the present document

NOTE 2: An IPSP will typically only support some of the use cases defined in the present document.

6.2 Terms and Conditions

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

NOTE: Terms and conditions for identity proofing can be part of the terms and conditions for use of the trust service for which the identity proofing is done.

6.3 Information security policy

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

7 Identity proofing service management and operation

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.

OVR-7.8-02: The information system making the identity proofing decision shall be logically or physically separated from non-critical information systems at the IPSP.

NOTE: E.g. separated from office support systems.

7.9 Vulnerabilities and incident management

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

OVR-7.9-02: Reporting obligations according to ETSI EN 319 401 [1] **REQ-7.9.2-02X** and clause 7.9.3 shall be fulfilled as required by the identity proofing context and the obligations of the TSPs relying on the IPSP's service.

EXAMPLE: Reporting to the supervisory authority supervising a TSP can be done in co-operation between the IPSP and the TSP; similar for identity proofing for other actors than TSPs.

7.10 Collection of evidence

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

NOTE 1: Long-term requirements for retention of evidence can be fulfilled by the TSP requesting the identity proofing instead of by the IPSP when the TSP and the IPSP are different entities.

NOTE 2: The requirements of clause 8.5.2 of the present document apply.

7.11 Business continuity management

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

OVR-7.11-02: Processes for crisis management according to ETSI EN 319 401 [1], **REQ-7.11.3-01X** shall be as required by the identity proofing context and the obligations of the TSPs relying on the IPSP's service.

7.12 Termination and termination plans

OVR-7.12-01: The requirements specified in ETSI EN 319 401 [1], clause 7.12, excluding **REQ-7.12-11**, shall apply.

NOTE: When the IPSP and the TSP requesting the identity proofing are different entities, they can agree mutual or unilateral assistance in establishing termination plans.

7.13 Compliance

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

7.14 Supply chain

OVR-7.14-01: The requirements specified in ETSI EN 319 401 [1], clause 7.14 shall apply.

8 Identity proofing service requirements

8.1 Initiation

INI-8.1-01X: The applicant shall be informed of, and shall actively accept before the identity proofing process is started, the purpose of the identity proofing and the related terms and conditions as required by the identity proofing context.

INI-8.1-02X: If alternative identity proofing processes are available to achieve the purpose of the identity proofing, the applicant should be allowed to select which of the alternative processes to use.

INI-8.1-03X: The applicant shall receive clear guidance regarding how the identity proofing process will be carried out, regarding the identity information that will be collected, regarding what data is kept and for how long, regarding the evidence that the applicant is required to present, and regarding any tool that the applicant is required to use.

EXAMPLE 1: Information on the applicable data protection rules, notably GDPR if the identity proofing process is carried out under the legislation of an EU Member State.

EXAMPLE 2: The identity proofing process can require the use of a specific type of device (e.g. a smartphone) with the installation of specific software (e.g. an app).

INI-8.1-04: The identity proofing process, or at least one process if alternative processes are available, shall be available to persons with disabilities in accordance with the applicable legislation.

EXAMPLE 3: Directive (EU) 2019/882 [i.31] in the EU.

8.2 Attribute and evidence collection

8.2.1 General requirements

COL-8.2.1-01X: Mandatory and optional identity attributes to collect shall be defined for each identity proofing context.

COL-8.2.1-01A: All mandatory attributes for a specific identity proofing context shall be collected.

COL-8.2.1-02: The identity attributes collected shall provide unique identification of the applicant for the identity proofing context.

COL-8.2.1-03X: The identity attributes collected shall be validated by use of one or more authoritative evidence and optionally one or more supplementary evidence.

NOTE 1: An identity proofing process can use multiple evidence, including several evidence of the same type, e.g. several identity documents, either routinely, or with further evidence added if identity proofing using the initial evidence yields insufficient reliability of the result.

COL-8.2.1-04: The evidence collected shall meet the requirements of the identity proofing context.

NOTE 2: The identity proofing context can pose requirements for the use of specific types of evidence, e.g. resulting from applicable legislation.

COL-8.2.1-05: The evidence shall be issued by entities trusted in the identity proofing context.

NOTE 3: Meaning that the evidence can be validated and that the reliability of the attributes conveyed can be assessed.

COL-8.2.1-06X: The identity proofing practice statement shall identify a list of the identity proofing use cases supported, the authoritative and optionally supplementary evidence that shall be trusted, and, as far as possible, the identity proofing contexts supported.

NOTE 4: Identification of use cases can be by reference to clause 9 or Annex C of the present document.

NOTE 5: While the list of evidence that can be trusted is required to be comprehensive, a specific identity proofing context can place restrictions on the selection of evidence applicable to the identity proofing context.

COL-8.2.1-07: The freshness of the identity attributes obtained from evidence shall be evaluated against the freshness requirements of the identity proofing context.

EXAMPLE: A passport can have a lifetime of 10 years, and an eID or signing certificate can have a lifetime of 2-5 years, meaning the identity attributes obtained from this evidence can have changed since the evidence was issued. Some evidence issuers can apply revocation and re-issuing if information changes.

NOTE 6: If the identity attributes conveyed from an evidence do not fulfil the information freshness requirements of the identity proofing context, the situation can be compensated by the use of supplementary evidence.

8.2.2 Attribute collection

8.2.2.1 Attribute collection for natural person

[CONDITIONAL] If the applicant is a natural person, the requirements in the present clause apply.

COL-8.2.2.1-01X: The identity proofing practice statement shall identify for each identity proofing context supported, the means used to collect identity attributes for a natural person.

EXAMPLES:

- From a physical identity document by transcription or scanning (e.g. OCR reading).
- From a digital identity document.

- From the use of an eID authenticating the applicant.
- From a certificate supporting a digital signature applied by the applicant.
- Directly from the applicant by typing in information or otherwise; such information is required to be validated against authoritative sources.
- From authoritative sources such as public registers.

NOTE 1: Identity attributes from authoritative sources can be conveyed directly from the source or in the form of attribute attestations issued by a trusted provider of electronic attestation of attributes.

- From existing information in auxiliary data sources such as customer records and databases.
- From other documents supplied by the applicant or from other sources.

NOTE 2: For attributes obtained from other sources than authoritative sources, validation against an authoritative source is needed.

COL-8.2.2.1-02: The following attributes shall at a minimum be collected if the applicant is a natural person:

a) family name(s), first name(s), which should be current names;

b) further information as needed to uniquely identify the applicant as a natural person in the identity proofing context.

NOTE 3: There can be cases where the name attributes collected need to match the name provided by an evidence, which is not necessarily the current name when a name change occurred after the evidence was issued.

NOTE 4: Requirements for the presence of naming attributes can depend on the identity proofing context. In some contexts, a 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 5: 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 name provide unique identification.

NOTE 6: ETSI EN 319 412-2 [i.9] 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 a unique identity. While values for the country and the serialNumber attributes can be part of the attributes collected, these values can also be generated and added by the certification authority.

COL-8.2.2.1-02A: The outcome of the identity proofing process may be a pseudonymous identity.

NOTE 7: Although the outcome of the identity proofing can be a pseudonym identity, identity proofing conforming to the present document requires identification of the real identity of the person as determined by applicable identity documents, trusted registers or other authoritative sources.

COL-8.2.2.1-03: The attributes to collect shall be as determined by the identity proofing context.

NOTE 8: Given the identity proofing context, the legal basis for collecting certain attributes can be laws or regulations allowing collection or consent by the applicant. Applicant's consent can be extended to the collection of attributes additional to the minimum set needed for the identity proofing context.

NOTE 9: When the identity proofing context is for issuing of electronic attestations of attributes as defined by the amended eIDAS regulation [i.25], the attribute set to collect can be extensive and span multiple authoritative sources.

COL-8.2.2.1-04: The identity proofing process shall not collect identity attributes that are not included in the result of the identity proofing, except when such attributes are required for attribute and evidence validation and/or binding to applicant.

8.2.2.2 Attribute collection for legal person

[CONDITIONAL] If the applicant is a legal person, the requirements in the present clause apply.

COL-8.2.2.2-01X: For each identity proofing context supported, the means used to collect identity attributes for a legal person shall be identified by the identity proofing practice statement.

NOTE: Depending on the identity proofing context, attribute collection for a legal person may vary from basic company information to an extensive record of information about the legal person, including information such as beneficial owners and personnel in key roles.

EXAMPLE 1: Attributes can be collected from business registers, commercial information providers, documents and attestations, electronic attestation of attributes, or by manual input in the course of the identity proofing process. For attributes obtained from other sources than authoritative sources, validation against an authoritative source can be needed.

COL-8.2.2.2-02: The attributes collected shall uniquely identify the applicant as a legal person in the identity proofing context.

COL-8.2.2.2-03: The following attributes shall, as a minimum, be collected if the applicant is a legal person:

a) full name 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).

EXAMPLE 2: Unique identifier can be national registration number, tax number, VAT number, or Legal Entity Identifier (LEI).

8.2.2.3 Attribute collection for natural person representing legal person

[CONDITIONAL] If the applicant is a natural person representing a legal person, the requirements in the present clause apply.

COL-8.2.2.3-01: Identity attributes for the natural person shall be collected according to the requirements in clause 8.2.2.1 of the present document.

COL-8.2.2.3-02: Identity attributes for the legal person shall be collected according to the requirements in clause 8.2.2.2 of the present document.

COL-8.2.2.3-03: The role of the natural person with respect to the legal person and identification of the source of the authorization of the natural person to represent the legal person shall be collected.

EXAMPLE: Roles and authorizations can be collected from business registers, commercial information providers, documents and attestations, electronic attestation of attributes, or by manual input in the course of the identity proofing process.

8.2.3 Use of physical or digital identity document as evidence

[CONDITIONAL] If physical and/or digital identity documents are used as evidence, the requirements in the present clause apply.

COL-8.2.3-01X: An identity document used as evidence shall be in physical or digital form.

NOTE 1: A physical or digital identity document as defined in the present document will usually represent a natural person only. Identity documents that evidence that a natural person represents a legal person can be envisaged but cannot be assumed to be generally available.

COL-8.2.3-02X: A document used as authoritative evidence shall contain a face photo and/or other information that can be used to uniquely identify the applicant when compared with the applicant's physical appearance.

NOTE 2: Required for verification against the applicant's physical appearance for binding to applicant. The binding is by biometric technology or by manual verification, or a combination of the two, see clause 8.4 of the present document.

NOTE 3: This does not exclude the use of documents without a face photo or similar information as supplementary evidence.

NOTE 4: The present document only specifies requirements for binding to applicant using face biometrics and/or manual face verification. Requirement **COL-8.2.3-02X** does not exclude the possibility of using other biometrics, e.g. fingerprint or iris, but the present document does not specify requirements for such use cases.

COL-8.2.3-03X: For each identity proofing context supported, a list of the identity documents that are accepted shall be identified by the identity proofing practice statement.

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.

[CONDITIONAL] COL-8.2.3-04X: If physical identity documents are used as authoritative evidence, only passports, national identity cards and other official identity documents that according to the identity proofing context offer the same or higher reliability of the identity shall be accepted, where the judgement on comparable reliability shall be based on an assessment of the security features and issuance process of the other identity document towards the security features and issuance process of passport and/or identity card.

NOTE 5: The comparable reliability of other identity documents can be based on a comparison of protection against known threats.

NOTE 6: Some countries issue national identity cards or have valid national identity cards that are below current practice in the security of national identity documents. Identity proofing context requirements can be to not accept such national identity cards.

[CONDITIONAL] COL-8.2.3-05X: If a physical identity document is used as evidence, the IPSP shall verify that the document is presented in its original form.

NOTE 7: Meaning the applicant is required to present the original in the identity proofing process to evidence proof of possession of the identity document; the identity proofing process can subsequently capture another representation of the document, e.g. by a video sequence, image, or scan.

[CONDITIONAL] COL-8.2.3-06X: If digital identity documents are used as authoritative evidence, only eMRTD digital identity documents according to ICAO 9303 part 10 [2] and other digital documents that according to the identity proofing context offer the same or higher reliability of the identity shall be accepted, where the judgement on comparable reliability shall be based on an assessment of the security features and issuance process of the other identity document towards the security features and issuance process required by ICAO 9303 part 10 [2].

NOTE 8: The comparable reliability of other identity documents can be based on a comparison of protection against known threats.

[CONDITIONAL] COL-8.2.3-07: If required attributes to be collected cannot be validated by the identity document, these attributes shall be collected from other sources and validated, including assessing that the attributes are bound to the applicant, by use of other authoritative sources in accordance with the identity proofing context.

8.2.4 Use of existing eID means as evidence

[CONDITIONAL] If existing eID means for authentication is used as evidence, the requirements in the present clause apply.

COL-8.2.4-01X: For each identity proofing context supported, the conditions that an eID or eID scheme is required to fulfil to be accepted for identity proofing shall be identified by the identity proofing practice statement.

NOTE 1: Most eID solutions today represent a natural person, although eID means for a legal person or a natural person representing a legal person are possible.

EXAMPLE 1: The documentation can list named eIDs or eID schemes or describe the necessary characteristics of eIDs or eID schemes by referring to a required LoA as defined by an assurance level framework.

EXAMPLE 2: Acceptance for an identity proofing context can require that certain identity attributes are asserted by the eID means.

EXAMPLE 3: The identity proofing context can state that only eIDs notified according to the amended eIDAS regulation [i.25] Article 9 can be used.

[CONDITIONAL] COL-8.2.4-02X: If the Baseline LoIP is targeted, the eID shall at least conform to eIDAS LoA substantial or conform to another assurance level framework offering comparable assurance to eIDAS LoA substantial.

[CONDITIONAL] COL-8.2.4-02A: If the Extended LoIP is targeted, the eID shall conform to eIDAS LoA high or conform to another assurance level framework offering comparable assurance to eIDAS LoA high.

NOTE 2: eIDAS LoAs are specified by CIR (EU) 2015/1502 [i.3]. The identity proofing context can require conformance to specifically the eIDAS LoA framework and can also require that eIDs are notified according to the amended eIDAS regulation [i.25] Article 9.

EXAMPLE 4: The eID can conform to a national assurance level framework of an EU Member State or an assurance level framework of a non-EU state; in both cases, the assurance level framework can be aligned with the eIDAS LoAs.

NOTE 3: The comparable assurance to an eIDAS LoA level can be assessed by an independent, accredited conformity assessment body.

NOTE 4: The identity proofing context can place further requirements on the issuing of the eID, e.g. to avoid a long chain of eID renewals where the presence (physical or remote) of the eID subject is a long time in the past, or to avoid a long chain of eIDs that are all issued based on another eID.

[CONDITIONAL] COL-8.2.4-03X: If required attributes to be collected cannot be validated by the authentication using the eID means, these attributes shall be collected from other sources and validated, including assessing that the attributes are bound to the applicant, by use of other authoritative sources in accordance with the identity proofing context.

NOTE 5: Typically, this happens when required attributes are not present in the identity assertion obtained from the authentication protocol.

NOTE 6: When the eID used is a European Digital Identity Wallet as specified by the amended eIDAS regulation [i.25] or similar type of eID, the authentication can convey an extended set of attributes.

[CONDITIONAL] COL-8.2.4-04: VOID, moved to clause C.2.

8.2.5 Use of existing digital signature means as evidence

[CONDITIONAL] If an existing digital signature means with a supporting certificate is used as evidence, the requirements in the present clause apply.

COL-8.2.5-01X: For each identity proofing context supported, the conditions under which digital signatures and certificates are accepted shall be identified by the identity proofing practice statement.

NOTE 1: A digital signature can be applied by a natural person (electronic signature as defined by eIDAS), a legal person (electronic seal as defined by eIDAS), or a natural person representing a legal person, depending on the identity attributes included in the certificate and the semantics of these attributes.

NOTE 2: The conditions can be stated in the form of a signature policy; see ETSI TS 119 172-1 [i.13].

NOTE 3: The present document makes no assumption on the format or content of the document signed. Identity attributes are evidenced by the certificate, not by the signed document.

EXAMPLE 1: Regarding digital signature, the identity proofing context can require that a qualified electronic signature/seal, according to the amended eIDAS regulation [i.25], is used.

EXAMPLE 2: Regarding certificate, the list can consist of named certificate issuers or describe the necessary characteristics of the certificate, e.g. by referring to a policy level as defined by ETSI EN 319 411-1 [i.7] or ETSI EN 319 411-2 [i.8].

EXAMPLE 3: Acceptance for an identity proofing context can pose requirements for certificate content, e.g. require that certain identity attributes are present for the named subject.

[CONDITIONAL] COL-8.2.5-02: If a digital signature with a supporting certificate is accepted as evidence of identity for a natural person representing a legal person, the certificate should evidence the connection between the natural and the legal person.

NOTE 4: For an X.509 certificate, this will typically imply that the Subject field of the certificate identifies both the natural and the legal person; however, such identification in itself does not evidence that the natural person is authorized to represent the legal person for the identity proofing.

[CONDITIONAL] COL-8.2.5-03X: If the Baseline LoIP is claimed, the certificate of the digital signature shall have been issued based on identity proofing to Baseline or Extended LoIP.

[CONDITIONAL] COL-8.2.5-03A: If the Extended LoIP is claimed, the certificate of the digital signature shall have been issued based on identity proofing to Extended LoIP.

NOTE 5: The identity proofing context can place further requirements on the issuing of the certificate, e.g. to avoid a long chain of certificate renewals where the presence (physical or remote) of the certificate subject is a long time in the past, or to avoid a long chain of certificates that are all issued based on another certificate. A requirement for the certificate to be issued based on one of the use cases defined in the present document can be recommended.

[CONDITIONAL] COL-8.2.5-04X: If required attributes to be collected are not present in the certificate, these attributes shall be collected from other sources and validated, including assessing that the attributes are bound to the applicant, by use of other authoritative sources in accordance with the identity proofing context.

[CONDITIONAL] COL-8.2.5-05: VOID, moved to clause C.2.

COL-8.2.5-06X: The digital signature shall be made under a guarantee of sole control by the signer when the signer is a natural person and under a guarantee of control when the signer is a legal person.

8.2.6 Use of trusted register as supplementary evidence

[CONDITIONAL] If a trusted register is used as supplementary evidence, the requirements in the present clause apply.

COL-8.2.6-01X: For each identity proofing context supported, a list of the trusted registers used to collect and/or validate attributes, and whether lookup in these registers is mandatory or optional, shall be identified by the identity proofing practice statement.

NOTE 1: Availability of trusted registers can vary between countries, ranging from no availability to lookup in particular sources, e.g. national population registers or business registers, mandated by national regulation.

EXAMPLE 1: Trusted registers can be used both to validate attributes that are already collected to ensure that the attribute values are correct and up to date, and to fetch additional attributes.

COL-8.2.6-01A: Attributes collected from a trusted register shall be reliably linked to the applicant**.**

COL-8.2.6-02: Only official national or nationally approved registers should be accepted as trusted registers.

EXAMPLE 2: Authentic sources as defined by the amended eIDAS regulation [i.25].

EXAMPLE 3: Depending on the identity proofing context, identity attribute sources such as existing customer databases of TSPs or other service providers can be defined as trusted registers.

[CONDITIONAL] COL-8.2.6-03X: If the applicant is a legal person and is registered in an available trusted register accepted as authoritative source, this register shall be used for collection and/or validation of the attributes of the legal person.

NOTE 2: 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.

8.2.7 Use of proof of access as supplementary evidence

[CONDITIONAL] If proof of access is used as supplementary evidence, the requirements in the present clause apply.

COL-8.2.7-01X: For each identity proofing context supported, a list of the proof of access mechanisms that are required or accepted as supplementary evidence of identity and the attributes that are collected and/or validated from these mechanisms shall be identified by the identity proofing practice statement.

NOTE: Proof of access will usually be relevant only for natural persons.

EXAMPLE 1: Proof of access to a bank account with identity attributes obtained from the bank.

EXAMPLE 2: Proof of access to a mobile phone with identity attributes obtained from the mobile operator's subscription register.

COL-8.2.7-02: The attributes returned from the proof of access shall be reliably linked to the applicant.

EXAMPLE 3: Proof of access to a bank account owned by another person could result in attributes for the other person to be returned.

COL-8.2.7-03X: The reliability of attributes obtained from proof of access mechanisms shall be evaluated and be sufficient for the identity proofing context.

EXAMPLE 4: The general outcome of an identity proofing process is Baseline or Extended, but a mobile phone number obtained from proof of access can have lower reliability.

8.2.8 Use of documents and attestations as supplementary evidence

[CONDITIONAL] If documents and attestations are used as supplementary evidence, the requirements in the present clause apply.

COL-8.2.8-01X: For each identity proofing context supported, a list of the documents and/or attestations required or accepted as supplementary evidence of identity and the attributes that are collected or validated from this documentation shall be identified by the identity proofing practice statement.

EXAMPLE 1: Qualified or non-qualified electronic attestation of attributes as defined by the amended eIDAS regulation [i.25].

EXAMPLE 2: For a natural person, in some countries, utility bills or similar can be required as evidence of address.

EXAMPLE 3: Attestations can be used as evidence that a legal person exists and for further information on its legal status, and as evidence that a natural person is entitled to represent the legal person.

COL-8.2.8-01A: Attributes collected from documents and attestations shall be reliably linked to the applicant.

[CONDITIONAL] COL-8.2.8-02: If the applicant is a legal person, a statement from a natural person verified to represent the legal person may be accepted as evidence.

COL-8.2.8-03X: The reliability of attributes obtained from documents and attestations shall be evaluated and be sufficient for the identity proofing context.

EXAMPLE 4: The general outcome of an identity proofing process is Baseline or Extended, but an address obtained from a utility bill can have lower reliability.

COL-8.2.8-04: Acceptance of digital documents and attestations should be limited to digital documents and attestations that are evidenced by the issuer's digital signature.

NOTE: The identity proofing context can pose requirements that a digital signature is required to fulfil to be accepted.

EXAMPLE 5: Qualified electronic attestation of attributes as defined by the amended eIDAS regulation [i.25] requires the qualified electronic seal or qualified electronic signature of the issuer.

8.2.9 Evidence collection for natural person representing legal person

[CONDITIONAL] If the applicant is a natural person purporting to represent a legal person, the requirements in the present clause apply.

COL-8.2.9-01: Evidence for the natural person's identity shall be collected according to the relevant requirements from clauses 8.2.3 to 8.2.8 of the present document.

COL-8.2.9-02: Evidence for the legal person's identity shall be collected according to the relevant requirements from clauses 8.2.3 to 8.2.8 of the present document.

COL-8.2.9-03X: For each identity proofing context supported, the accepted means to evidence the link between the natural person's identity and the legal person's identity shall be identified by the identity proofing practice statement.

EXAMPLE 1: Trusted registers like business registers, or required documents and attestations.

EXAMPLE 2: Authentic source or electronic attestation of attributes as defined by the amended eIDAS regulation [i.25].

COL-8.2.9-04X: For each identity proofing context supported, the positions, roles, or other relationships accepted for a natural person to represent a legal person shall be identified in the identity proofing practice statement.

EXAMPLE 3: Directors, executives, board members, employees or a natural person with authorization duly delegated from another natural person in an authorized role.

COL-8.2.9-05X: For each identity proofing context supported, any freshness (current) requirement applicable to any statement or document regarding the natural person's relationship to the legal person shall be identified by the identity proofing practice statement.

[CONDITIONAL] COL-8.2.9-06X: If the legal person is listed in a trusted register, the role of the natural person concerning the legal person shall be collected from or validated against this register to the extent that the register is accessible and that the required attributes are present in the register.

EXAMPLE 4: A trusted register can be appointed as authentic source according to the amended eIDAS regulation [i.25] and the role of the natural person concerning the legal person can be conveyed by a qualified or non-qualified electronic attestation of attributes.

NOTE: Practices for registration vary between countries. As one example, public sector entities are not registered in business registers in all countries.

[CONDITIONAL] COL-8.2.9-07X: If the legal person is not listed in a trusted register, or the required attributes to collect or validate the role of the natural person concerning the legal person are not present in the register, the role of the natural person concerning the legal person shall be collected or validated by other means providing the same confidence as a trusted register would do.

EXAMPLE 5: Information source can be a public notary, other registers than business registers, contacts with representatives of the legal person other than the concerned natural person, etc.

COL-8.2.9-08: Documents and attestations from the concerned legal person may be used as evidence of a natural person's authorization to represent the legal person.

8.3 Attribute and evidence validation

8.3.1 General requirements

VAL-8.3.1-01X: All necessary identity attributes shall be validated to the required reliability by an authoritative source.

VAL-8.3.1-02: Evidence of the identity proofing process shall be collected and secured supporting requirements in clause 8.5.2 of the present document.

VAL-8.3.1-03X: The handling of differences in encoding of identity attributes between different evidence or between evidence and attributes collected from other sources than evidence shall be specified in the practice statement.

EXAMPLE 1: Typical sources of differences are transcription between alphabets (e.g. between Cyrillic and Latin) or from non-alphabetical scripts (e.g. Chinese) to an alphabet, transcription of national language characters (e.g. Norwegian æ, ø, å) into Latin characters, and transcription of diacritics (e.g. French é, è, ê) into Latin characters.

VAL-8.3.1-04X: The handling of differences in name attributes between different evidence or between evidence and attributes collected from other sources than evidence shall be specified in the practice statement.

EXAMPLE 2: Missing names (middle names or first names), change of name not reflected (e.g. evidence contains a name before a later change of name), use of initials, truncation (e.g. limited number of characters that can be printed on an identity document), use of prefix (e.g. Dr) or suffix (e.g. Jr).

VAL-8.3.1-05: The identity proofing process shall verify that the evidence is of a type accepted according to the identity proofing context.

VAL-8.3.1-06X: The identity proofing process shall verify that the issuer of evidence is trusted according to the identity proofing context.

[CONDITIONAL] VAL-8.3.1-07: If the evidence has an explicit validity period, the identity proofing process shall verify that the time of the identity proofing is within this validity period.

EXAMPLE 3: Valid from and valid to attributes of a digital signature certificate, date of expiry of an identity document.

VAL-8.3.1-08X: The identity proofing process shall verify the authenticity and integrity of the evidence, i.e. that the evidence is genuine and presented in its original form.

NOTE 1: An evidence of a type that actually exists, and that is not counterfeit, has not been tampered with and, where applicable, is not a copy of the original.

VAL-8.3.1-09: VOID (merged with VAL-8.3.1-08X).

VAL-8.3.1-10X: The IPSP shall for all accepted evidence document the security features that are to be verified.

NOTE 2: This needs not be all security elements of e.g. a physical identity document. A selection of suitable elements sufficient for assessing that the evidence is genuine can be applied, see requirements **VAL-8.3.3-07X** and **VAL-8.3.3-07A**.

NOTE 3: Publication of the selection of features is not recommended. Internal documentation is assumed.

NOTE 4: A remote identity proofing process might not allow verification of all security elements.

VAL-8.3.1-11X: The identity proofing process shall whenever practically possible verify that the evidence is valid at the time of the identity proofing.

EXAMPLE 4: An identity document can be declared lost, stolen, or revoked, but not all document issuers provide an online status service that can be used to check current status, and if an online status service exists, its availability can be restricted.

EXAMPLE 5: Certificates and eIDs can be revoked before their expiry time. This includes certificates of evidence issuers, where the identity proofing context determines if an evidence is accepted or not if the issuer's certificate has expired or is revoked.

VAL-8.3.1-12: Validation of evidence shall be done in an environment controlled by the actor responsible for the identity proofing process.

NOTE 5: This requirement does not prohibit remote access to this environment by registration officers.

NOTE 6: This requirement does not prohibit cloud service hosting of the environment.

8.3.2 Validation of digital identity document

[CONDITIONAL] If a digital identity document is used as authoritative evidence, the requirements in the present clause apply.

NOTE 1: Some legislations restrict access to the chip of national identity cards for reading of the digital identity document or of the face photo. If such restrictions apply to a document used in an identity proofing context, the digital document cannot be used as evidence.

VAL-8.3.2-00: Successful validation of a digital identity document shall imply that the identity document as evidence is validated and that the identity attributes conveyed from the identity document are validated.

[CONDITIONAL] VAL-8.3.2-01: If the digital identity document is used in a remote identity proofing process, the data from the identity document shall be transferred to an environment controlled by the actor responsible for the identity proofing process in a manner that ensures authenticity, integrity, and confidentiality of the document content.

VAL-8.3.2-02: The digital identity document shall only be accepted if the issuer's digital signature on the document is successfully validated.

NOTE 2: Usually this means that the validation result is TOTAL-PASSED as defined by ETSI EN 319 102-1 [i.5].

NOTE 3: For an eMRTD document following ICAO 9303 part 10 [2], country signing certificates, e.g. downloaded from the ICAO PKD (Public Key Database), are needed for validation.

[CONDITIONAL] VAL-8.3.2-03: If an online status service to confirm the document's validity exists and is practically available, the process shall use this service to verify that the document is currently valid.

NOTE 4: Meaning not revoked, suspended, or reported as lost/stolen. Not all document issuers have available lookup services to check validity, and in some cases access to lookup services is restricted. Regarding current validity, note that there can be a delay in the order of days between the events of revoking a document and updating a status service.

NOTE 5: If digital identity documents from many different sources are accepted, online access (interactive or by API) to all the different status services can be impractical for documents that occur infrequently.

[CONDITIONAL] VAL-8.3.2-04X: If the digital identity document is required to be read from a chip embedded in a physical identity document, the identity proofing process shall protect against injection into the process, by the applicant or an external attacker, of a copy of a digital identity document that has previously been obtained and stored by the attacker.

NOTE 6: Fulfilment of this requirement can depend on the protocol supported by the chip; reliable fulfilment can be difficult if the chip does not support a protocol that supports cloning detection.

NOTE 7: Fulfilment of this requirement can rely on the applicant's use of software that is approved for the identity proofing process, e.g. mobile app functionality.

NOTE 8: Means for biometric injection attack detection, e.g. as per TS 18099 [5] can be used as a basis to also detect this type of injection attack.

[CONDITIONAL] VAL-8.3.2-04A: If the digital identity document is required to be read from a chip embedded in a physical identity document, in case of an interruption of the identity proofing process for any reason (e.g. loosing internet connection), if the identity proofing process is resumed, the identity document shall be reread from the chip.

VAL-8.3.2-05: Information obtained from the digital identity document shall be recorded as needed for binding to applicant and to evidence the identity proofing process.

NOTE 9: In addition to identity attributes, required information to be recorded is typically at least issuer, validity period, and the document's unique identification number.

VAL-8.3.2-06: The face photo contained in the digital identity document shall be extracted to enable binding to applicant.

8.3.3 Validation of physical identity document

[CONDITIONAL] If a physical identity document is used as authoritative evidence, the requirements in the present clause apply.

NOTE 1: A physical identity document can be used with the applicant's physical presence and remotely by the applicant presenting the document in front of a camera.

VAL-8.3.3-00: Successful validation of a physical identity document shall imply that the identity document as evidence is validated and that the identity attributes conveyed from the identity document are validated.

VAL-8.3.3-01: The process shall verify that the physical identity document presented is visually equal to the expected visual appearance of the document type.

[CONDITIONAL] VAL-8.3.3-02X: If a physical identity document is used as evidence in a remote identity proofing process, the process shall ensure that the applicant has the document in hand and presents the document in real-time in front of a camera.

NOTE 2: It is required that this happens at the time of the identity proofing; submission of a pre-recorded photo or video stream of an identity document is considered not to meet the requirements for identity proofing to Baseline or Extended LoIP. Means for biometric presentation attack detection, e.g. as specified by ISO/IEC 30107-1 [i.16] and 3 [3], can be used as a basis to detect a presentation attack using a pre-recorded or artificially generated video of an identity document. Means for biometric injection attack detection, e.g. as per TS 18099 [5] can be used as a basis to detect an injection attack using a pre-recorded or artificially generated video of an identity document.

NOTE 3: This can rely on the applicant's use of software approved for the identity proofing process, e.g. mobile app functionality.

VAL-8.3.3-03: The process shall ensure that the document presented by the applicant is a genuine, physical identity document that is not counterfeited or falsified/modified.

[CONDITIONAL] VAL-8.3.3-04X: If the physical identity document is used in a remote identity proofing process, the applicant's presentation of the identity document in front of a camera shall include recording at the time of the identity proofing of a video sequence to visualize the physical characteristics of the identity document and its security features. The recording shall cover each relevant side of the identity document presented by the applicant.

EXAMPLE 1: The applicant can be given instructions for the movement of the identity document, where the specific actions and/or their sequence are unpredictable to the applicant.

NOTE 4: With the current state of technology, the use of only a still photo of the identity document is not considered sufficient for Baseline or Extended LoIP.

EXAMPLE 2: Both the front and back sides of a national identity card will usually need to be presented.

[CONDITIONAL] VAL-8.3.3-04A: If the physical identity document is used in a remote identity proofing process, the video recording of the document shall use frame rate and resolution sufficient for the analysis of the document.

EXAMPLE 3: A frame rate of 25 frames per second and a resolution of 1280×720 pixels or 960×720 pixels (landscape) or 720×1280 pixels or 720×960 pixels (portrait).

[CONDITIONAL] VAL-8.3.3-04B: If the physical identity document is used in a remote identity proofing process, the process should capture from or integral to the video sequence one or more images of each relevant side of the identity document.

[CONDITIONAL] VAL-8.3.3-04C: If the physical identity document is used in a remote identity proofing process, and an image of the document is captured in the process, the image shall have sufficient resolution for the analysis of the document.

EXAMPLE 4: A resolution of 1280×720 pixels or 960×720 pixels (landscape) or 720×1280 pixels or 720×960 pixels (portrait).

[CONDITIONAL] VAL-8.3.3-05X: If the physical identity document is used in a remote identity proofing process, the process shall ensure that the video stream and any images captured are transmitted to an environment controlled by the actor responsible for the identity proofing process in a manner that ensures authenticity, integrity, and confidentiality of the video stream and images.

[CONDITIONAL] VAL-8.3.3-05A: If the physical identity document is used in a remote identity proofing process, the process shall protect against injection into the process, by the applicant or an external attacker, of a previously recorded or artificially generated video stream.

NOTE 5: Means for biometric injection attack detection, e.g. as per TS 18099 [5], can be used as a basis to also detect this type of injection attack.

[CONDITIONAL] VAL-8.3.3-05B: If the physical identity document is used in a remote identity proofing process, the process shall apply means that are reliably able to detect identity documents that are artificially generated or have been manipulated by an attacker with the relevant attack potential.

NOTE 6: See requirements OVR-5-07 and OVR-5-08 regarding attack potential.

[CONDITIONAL] VAL-8.3.3-05C: If the physical identity document is used in a remote identity proofing process, the useability (e.g. lighting conditions, reflections, sharpness) of video and any images captured in the same process or derived from the video sequence shall be assessed, and video and images shall be rejected if they are not useable, with instructions to the applicant to repeat the process under better conditions.

VAL-8.3.3-05D: There shall be an upper limit on the number of retries on the video capture before the process is aborted with failed result.

[CONDITIONAL] VAL-8.3.3-06: If the process is performed with manual validation of the physical identity document, the registration officer shall have access to authoritative sources of information on document appearance and document validation.

EXAMPLE 5: Public Register of Authentic Travel and Identity Documents Online (PRADO).

VAL-8.3.3-07X: A sufficient number of, and at least three, different security features of physical identity documents shall be reliably verified considering an attacker with the relevant attack potential.

EXAMPLE 6: Security elements can be watermarks, holograms, printing techniques, visual and ultraviolet light patterns, and see-through elements. The reliability of remote verification of different security elements can vary.

NOTE 7: PRADO has published an overview of security features [i.27] of identity documents.

[CONDITIONAL] VAL-8.3.3-07A: If the physical identity document is used in a remote identity proofing process, at least two of the security features verified shall be optically variable features.

NOTE 8: This implies that a document that has less than two optically variable features cannot be used in remote identity proofing processes.

VAL-8.3.3-07B: Selection of which variable security elements of physical identity documents to verify should have some randomness to hamper attackers targeting falsifying specific elements.

VAL-8.3.3-07C: The verification process for all security elements in scope of the IPSP's service shall be documented.

NOTE 9: Publication of the verification process information is not recommended. Internal documentation is assumed.

[CONDITIONAL] VAL-8.3.3-08: If the process is performed with the physical presentation of physical identity documents, the registration officer shall verify optical and haptic/tactile security features if any.

NOTE 10: Selection of security features to verify can depend on the tools that the registration officer has available, If no tool is available, only Level 1 security features can be verified. With tools such as magnifying glass or UV lamp, Level 2 security features can be verified.

[CONDITIONAL] VAL-8.3.3-09: If an online status service to confirm the physical identity document's validity exists and is practically available, the process shall use this service to verify that the document is currently valid.

NOTE 11: Meaning not revoked, suspended, or reported as lost/stolen. Not all document issuers have available lookup services to check validity, and in some cases access to lookup services is restricted. Regarding current validity, note that there can be a delay in the order of days between the events of revoking a document and updating a status service.

NOTE 12: If physical identity documents from many different sources are accepted, online access (interactive or by API) to all the different status services can be impractical for documents that occur infrequently.

VAL-8.3.3-10: Information printed on physical identity documents shall be recorded as needed for binding to applicant and to evidence the identity proofing process.

NOTE 13: Information can be extracted by manual transcription, automatically for example by optical scanning and OCR techniques, and in some cases by photo/photocopy of the document.

NOTE 14: In addition to identity attributes, required information to be recorded is typically at least issuer, validity period, and the document's unique identification number.

[CONDITIONAL] VAL-8.3.3-11: If face biometrics is applied to bind the physical identity document to the applicant, the face photo printed on the identity document shall be extracted.

[CONDITIONAL] VAL-8.3.3-12X: If the physical identity document is used in a remote identity proofing process, and the identity document has an Machine Readable Zone (MRZ), the information from the MRZ shall be extracted, validated, and compared with the information from the visible part of the identity document.

[CONDITIONAL] VAL-8.3.3-13: If the physical identity document is validated by manual procedures, the validation task should be assigned randomly among available registration officers.

[CONDITIONAL] VAL-8.3.3-14X: If validation of physical identity documents is done manually, the validation shall be carried out by a registration officer that has received appropriate training covering at least the following:

a) Fraud prevention and detection of forgery.

b) Data protection.

c) Communication training (when the registration officer is required to communicate with the applicant).

d) Training on software and equipment used.

e) Training on verification of documents and their security elements.

f) Training on detection of presentation and injection attacks.

[CONDITIONAL] VAL-8.3.3-14A: If validation of physical identity documents is done manually, the registration officer shall be allowed sufficient time for the validation and have working conditions that do not impair the registration officer's judgement.

[CONDITIONAL] VAL-8.3.3-15X: If validation of physical identity documents is done manually, the training of the registration officers shall be repeated or refreshed as required by threats intelligence, updates to procedures or tools, and at least annually.

[CONDITIONAL] VAL-8.3.3-16: If validation of physical identity documents is done manually, and the process is performed with the physical presentation of the document, the registration officer should have available tools to enhance the reliability of the validation.

EXAMPLE 7: Magnifying glass and ultraviolet lamp. Without tools, only Level 1 security features as defined by ICAO can be verified.

[CONDITIONAL] VAL-8.3.3-17: If validation of physical identity documents is done manually, and the document is used in a remote identity proofing process, the registration officer shall have available tools to enhance the reliability of the validation.

EXAMPLE 8: Computerized tool to zoom in on details of the document.

VAL-8.3.3-18: Automated means and machine-learning technology should be used to analyse the characteristics of physical identity documents against their expected appearance, including analysis of security elements of documents and potential manipulation of documents.

NOTE 15: This requirement implies that a purely manual process for validating a physical identity document is allowed both for physical presence and for remote identity proofing. However, the use of (additional) automated means is recommended.

NOTE 16: For unattended remote identity proofing, a purely manual validation process can only support the Baseline LoIP, see clause 9.2.3.2 of the present document.

NOTE 17: 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 18: Automated and manual analysis can be used in combination, e.g. with fall-back to manual analysis if the automated process yields an uncertain result, or by using automated analysis as a tool for a registration officer.

[CONDITIONAL] VAL-8.3.3-19X: If the physical identity document is used in a remote identity proofing process, the video stream and any image recorded shall be of sufficient quality for analysis by automated means and machine-learning technology and/or manual verification.

[CONDITIONAL] VAL-8.3.3-20: If automated means and machine-learning technology are used to analyse physical identity documents, the algorithms and technology shall be systematically tested against reference datasets and be kept updated to cope with changes in the threats and risk situation.

8.3.4 Validation of eID means

[CONDITIONAL] If authentication by use of an existing eID means is used as evidence, the requirements in the present clause apply.

VAL-8.3.4-01X: An authentication protocol that confirms at an assurance level similar to the LoA of the eID used that the holder of the eID means is successfully authenticated and that the eID means used is valid (not expired, suspended, or revoked) shall be executed.

VAL-8.3.4-02: Successful authentication shall imply that the eID means as evidence is validated and that the identity attributes conveyed from the eID means are validated and bound to the applicant.

NOTE 1: The eID means can represent a natural person, a legal person, or a natural person representing a legal person.

NOTE 2: The authentication protocol can include attributes conveyed from a European Digital Identity Wallet as specified by the amended eIDAS regulation [i.25] or similar eID means.

8.3.5 Validation of digital signature with certificate

[CONDITIONAL] If a digital signature with certificate is used as evidence, the requirements in the present clause apply.

VAL-8.3.5-00: Successful validation of the digital signature shall imply that the identity attributes conveyed from the certificate supporting the digital signature are validated and bound to the applicant.

NOTE 1: Usually, this means that the validation result is TOTAL-PASSED as defined by ETSI EN 319 102-1 [i.5].

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

VAL-8.3.5-01: The digital signature shall be created as part of the identity proofing process.

NOTE 3: This is to avoid threats from the use of documents previously signed by the applicant.

VAL-8.3.5-02X: The digital signature shall be validated and the signing certificate shall only be used as evidence for identity attributes if the signature is valid and confirmed to have been created as part of the identity proofing process.

VAL-8.3.5-03: VOID (moved to clauses C.2.3 and C.3.3).

8.3.6 Validation of trusted registers

NOTE 1: A trusted register can be an authentic source as defined by the amended eIDAS regulation [i.25].

[CONDITIONAL] If a trusted register is used as supplementary evidence in an identity proofing process, the requirements in the present clause apply.

VAL-8.3.6-00: Successful authentication of a trusted register and validation of authenticity and integrity of the communication with the trusted register shall imply that the statement of the trusted register on validity of identity attributes is trusted.

NOTE 2: A trusted register can be used in two ways: either the trusted register can be queried to convey identity attributes registered on the applicant, or previously collected attributes can be sent to the trusted register for validation. In the latter case, the response can be just a yes/no answer on validity of the attributes.

[CONDITIONAL] VAL-8.3.6-01: If the communication towards the trusted register is online, the communication channel shall be secured by using an up to date version of the TLS protocol or another protocol offering a comparable level of security.

[CONDITIONAL] VAL-8.3.6-02: If the communication towards the trusted register is online, the trusted register shall be authenticated.

EXAMPLE 1: By a website certificate.

[CONDITIONAL] VAL-8.3.6-03: If the communication towards the trusted register is message-based, all messages shall be authenticated and integrity protected.

EXAMPLE 2: By use of digital signatures. The identity proofing context can pose requirements that a digital signature is required to fulfil to be accepted.

[CONDITIONAL] VAL-8.3.6-04: If the communication towards the trusted register is message-based, all messages containing personal identity information shall be encrypted.

VAL-8.3.6-05X: The integrity and authenticity of identity attributes obtained from the trusted register shall be validated.

VAL-8.3.6-06X: The procedure to apply in case of discrepancies between the identity attributes obtained from trusted registers and information from other evidence shall be specified in the practice statement.

EXAMPLE 3: A trusted register can override identity attributes obtained from other evidence. The identity proofing context can pose requirements.

8.3.7 Validation of proof of access

[CONDITIONAL] If proof of access is used as supplementary evidence in an identity proofing process, the requirements in the present clause apply.

VAL-8.3.7-00: Successful validation of proof of access shall imply that the identity attributes conveyed from the proof of access are validated.

VAL-8.3.7-01: A proof of access protocol shall be executed to ensure that the applicant controls the item in question.

EXAMPLE 1: To confirm possession of mobile phone number, email address, or bank account.

VAL-8.3.7-02X: The identity attributes obtained shall be transferred or otherwise be made available for the identity proofing process in a way that ensures the authenticity of the source of information and integrity and confidentiality of the information.

VAL-8.3.7-03: The integrity and authenticity of the identity attributes obtained shall be validated.

EXAMPLE 2: Information from an existing customer record of a bank or a telecommunications service provider.

[CONDITIONAL] VAL-8.3.7-04: If proof of access to a bank account is used as supplementary evidence, the applicant's access to the bank account shall be reliably authenticated.

EXAMPLE 3: By use of eID means fulfilling requirements for EU Payment Services Directive (PSD2) Strong Customer Authentication (SCA) [i.2].

EXAMPLE 4: A payment made by the applicant to an account associated with the identity proofing process can be part of the proof of access protocol.

VAL-8.3.7-05X: The procedure to apply in case of discrepancies between the identity attributes obtained from proof of access and identity attributes from other evidence shall be specified in the practice statement.

EXAMPLE 5: The identity attributes obtained from proof of access can be regarded as authoritative and override other sources of attributes, or other evidence can be regarded as authoritative, or an arbitration procedure can be used. The identity proofing context can pose requirements.

8.3.8 Validation of documents and attestations

NOTE 1: Attestations can be (qualified) electronic attestation of attributes as defined by the amended eIDAS regulation [i.25].

[CONDITIONAL] If documents and attestations are used as supplementary evidence in an identity proofing process, the requirements in the present clause apply.

VAL-8.3.8-01: The identity proofing process shall verify that the document or attestation presented is of an accepted type and is issued by an actor trusted according to the identity proofing context.

VAL-8.3.8-02X: The identity of the issuer of the document or attestation, and the authenticity and integrity of the contained identity attributes, shall be verified while ensuring their confidentiality.

NOTE 2: For a digital document, this can imply validating a digital signature on the document or attestation. The identity proofing context can pose requirements that a digital signature is required to fulfil to be accepted.

NOTE 3: When attributes are conveyed from a European Digital Identity Wallet as specified by the amended eIDAS regulation [i.25] or similar eID means, the protocol used can guarantee authenticity, integrity and confidentiality.

NOTE 4: For a physical document, this can be by physical signatures or seals, logos and other visual elements, and by examining the document to detect falsification and tampering.

[CONDITIONAL] VAL-8.3.8-03: If a document or attestation is in physical form or digital form rendered for human validation, the identity proofing process shall verify that the document presented is visually equal to the expected visual appearance.

[CONDITIONAL] VAL-8.3.8-04: If a document or attestation is in physical form and the document type contains security elements, these security elements shall be verified to the extent required by the identity proofing context.

VAL-8.3.8-05X: The procedure to apply in case of discrepancies between the identity attributes obtained from documents and attestations and identity attributes from other evidence shall be specified in the practice statement.

EXAMPLE: The identity attributes obtained from documents and attestations can be regarded as authoritative and override other sources of identity attributes, or other evidence can be regarded as authoritative, or an arbitration procedure can be used. The identity proofing context can pose requirements.

8.4 Binding to applicant

8.4.1 General requirements

BIN-8.4.1-01X: The identity proofing process shall verify that the applicant is the legitimate holder of the authoritative evidence.

BIN-8.4.1-02X: The identity proofing process shall verify that the authoritative evidence is in the possession of the applicant.

NOTE 1: For the authoritative evidence types existing eID means and existing digital signature means, no specific binding requirements are needed since the validation of the evidence also verifies the binding. This is under the assumption that only the applicant can use the eID means or digital signature means.

NOTE 2: For the supplementary evidence types trusted register, proof of access, and documents and attestations, no specific binding requirements are needed. If the binding of the authoritative evidence (identity document, eID means, or digital signature means) to the applicant is successful, and the supplementary evidence is validated and identifies the same person, the supplementary evidence is considered bound to the applicant.

8.4.2 Capture of face image of the applicant

[CONDITIONAL] If the applicant is a natural person, and an identity document is used as evidence, and the identity proofing process is carried out remotely, the following requirements apply.

BIN-8.4.2-01: A video stream of the applicant's face shall be captured.

NOTE 1: The video stream and images extracted from the stream can be used for binding to applicant by both face biometrics and manual means.

BIN-8.4.2-01A: The video recording shall use frame rate and resolution of sufficient quality for the identity proofing process.

EXAMPLE 1: 25 frames per second and a resolution of 1280×720 pixels or 960×720 pixels (landscape) or 720×1280 pixels or 720×960 pixels (portrait).

BIN-8.4.2-02X: The video capture process shall apply presentation attack detection means to ensure that the video stream is of a live person present in front of the camera at the time of the identity proofing.

BIN-8.4.2-02A: The video capture process shall happen at the time of the identity proofing.

NOTE 2: Submission of a pre-recorded video stream is considered not to meet the requirements for identity proofing to Baseline or Extended LoIP.

NOTE 3: Active presentation attack detection, e.g. instructing the applicant to perform certain actions, where the specific actions or their sequence are unpredictable to the applicant, can be used for presentation attack detection.

NOTE 4: Passive presentation attack detection such as the capture of skin reflections or eye movements from the use of random light patterns can be used for presentation attack detection.

BIN-8.4.2-03X: The video stream capture shall apply means to detect artificially generated or manipulated face appearance.

NOTE 5: Such attacks are sometimes termed "deep fake" attacks.

[CONDITIONAL] BIN-8.4.2-04: If the video stream is captured on the applicant's device, the identity proofing process shall ensure that the video stream is transmitted to an environment controlled by the actor responsible for the identity proofing process in a manner that ensures authenticity, integrity, and confidentiality of the video stream.

BIN-8.4.2-04A: The identity proofing process shall apply biometric injection attack prevention and detection means to ensure that neither the applicant nor an external attacker can undetectably inject into the process a previously recorded or artificially generated video stream

NOTE 6: This can rely on the applicant's use of software approved for the identity proofing process, e.g. mobile app functionality.

[CONDITIONAL] BIN-8.4.2-04B: If the identity proofing targets Baseline LoIP, the biometric injection attack detection means shall be tested by an accredited laboratory according to TS 18099 [5] level Substantial (level 2) at the latest before the end of 2026.

[CONDITIONAL] BIN-8.4.2-04C: If the identity proofing targets Extended LoIP, the biometric injection attack detection means shall be tested by an accredited laboratory according to TS 18099 [5] level High (level 3) at the latest before the end of 2026.

BIN-8.4.2-04D: Evaluation of biometric injection detection means by an accredited laboratory according to TS 18099 [5] shall be repeated at least every second year.

NOTE 7: TS 18099 [5] poses requirements for external laboratory testing of injection attack detection means. Setting end of 2026 to enforce testing according to TS 18099 [5] is intended to provide IPSPs, laboratories, and accreditation authorities for laboratories sufficient time to prepare.

NOTE 8: Regardless of the evaluation according to TS 18099 [5], the IPSP is required to keep biometric injection attack detection means constantly updated according to the IPSP's risk intelligence procedures, see clause 5 of the present document.

[CONDITIONAL] BIN-8.4.2-05X: If face biometrics is used for binding to applicant, at least one image of sufficient quality for binding to applicant shall be captured integral to the video capturing or be extracted from the video stream.

[CONDITIONAL] BIN-8.4.2-05A: If face biometrics is used for binding to applicant, and a face image of the applicant is captured in the process, the face image shall have a resolution of sufficient quality for the identity proofing process.

EXAMPLE 2: A resolution of 1280×720 pixels or 960×720 pixels (landscape) or 720×1280 pixels or 720×960 pixels (portrait).

BIN-8.4.2-05B: The conditions (e.g. lighting conditions, reflections, sharpness) of video and images shall be assessed, and video and images shall be rejected if they are not suited for binding to applicant, with an instructions to the applicant to repeat the process under better conditions.

NOTE 9: The upcoming ISO/IEC 29794-5 [i.32] standard on biometric sample quality, face image data, can become a reference for image quality in future versions of the present document.

BIN-8.4.2-05C: There shall be an upper limit on the number of retries before the process is aborted with failed result.

BIN-8.4.2-05D: The IPSP shall in its practice statement state goals for APCER (attack presentation classification error rate) and BPCER (bona fide presentation classification error rate) values that are at least at the level of industry best practice and that the service shall aim to achieve.

BIN-8.4.2-05E: The IPSP shall keep its APCER and BPCER goals updated based on its threats intelligence procedure.

BIN-8.4.2-06X: The PAD means and APCER and BPCER rates shall be systematically tested in accordance with ISO/IEC 30107-3 [3] against updated reference data sets and against the goals set by the IPSP.

NOTE 10: Regarding ISO/IEC 30107-3 [3], the task of an IPSP will usually be a verification or identification process and metrics can be applied at data capture subsystem or full-system level depending on the design of the IPSP's system.

BIN-8.4.2-07X: The PAD means shall be evaluated by an accredited laboratory according to ISO/IEC 19989-3 [6] at the latest before the end of 2026.

BIN-8.4.2-07A: Evaluation of PAD means by an accredited laboratory according to ISO/IEC 19989-3 [6] shall be repeated at least every second year.

NOTE 11: ISO/IEC 19989-3 [6] specifies security evaluation of PAD by external laboratory testing applying Common Criteria (ISO/IEC 15408-1 [i.24]). Setting end of 2026 to enforce testing according to ISO/IEC 19989-3 [6] is intended to provide IPSPs, laboratories, and accreditation authorities for laboratories sufficient time to prepare.

NOTE 12: Regardless of the evaluation according to ISO/IEC 19989-3 [6], the IPSP is required to keep PAD means constantly updated according to the IPSP's risk intelligence procedures, see clause 5 of the present document.

NOTE 13: The upcoming CEN standard on "European requirements for biometric products" can be referenced from future versions of the present document to define the evaluation procedures, methodologies, parameters and tests for the functional and security evaluation of the video stream. The CEN standard will be based on ISO/IEC 19795-1 [4], ISO/IEC 19989-1 [i.30], ISO/IEC 19989-3 [6] and ISO/IEC 30107-3 [3].

BIN-8.4.2-08X: Test results for the PAD shall achieve an APCER as defined by ISO/IEC 30107-3 [3] in accordance with the goal stated in the practice statement.

NOTE 14: No specific number is specified for the APCER. Rapid technology improvement can lead to significant progress in industry best practice APCER performance even in the short term.

BIN-8.4.2-09X: Test results for the PAD should achieve BPCER as defined by ISO/IEC 30107-3 [3] in accordance with the goal stated in the practice statement.

NOTE 15: The BPCER has impact on user-friendliness and can thus indirectly have an impact on security.

BIN-8.4.2-10: VOID.

8.4.3 Binding to applicant by automated face biometrics

[CONDITIONAL] If binding to applicant is by automated face biometrics, the following requirements apply:

NOTE 1: Use of other biometric means than face biometrics is currently out of scope but can be a future possibility.

BIN-8.4.3-01X: The process shall provide a reliable, automated comparison between face image(s) extracted from the identity document presented by the applicant and face image(s) captured according to the requirements of clause 8.4.2 of the present document.

BIN-8.4.3-02X: Data capture and preliminary data quality assessment may be done in equipment controlled by the applicant.

BIN-8.4.3-03: Biometric signal processing, comparison, data storage, and decision shall be carried out in an environment controlled by the actor responsible for the identity proofing process.

EXAMPLE 1: To protect against threats to the biometric system as described in ISO/IEC 30107-1 [i.16], clause 5.1.

[CONDITIONAL] BIN-8.4.3-04: If biometric face recognition is used with the physical presence of the applicant, properly secured equipment shall be used to read the identity document presented by the applicant and obtain a face image of the applicant.

[CONDITIONAL] BIN-8.4.3-05: If biometric face recognition is used with the physical presence of the applicant, locally installed and properly secured equipment may be used for the biometric face recognition processing.

EXAMPLE 2: For fulfilment of the two requirements above, a biometric kiosk as commonly used at passport offices, or equipment similar to that used for automated border control, can be used.

BIN-8.4.3-05A: The IPSP shall in its practice statement state goals for False Acceptance Rate (FAR) and False Rejection Rate (FRR) values that are at least at the level of industry best practice and that the service shall aim to achieve.

BIN-8.4.3-05B: The IPSP shall keep its FAR and FRR goals updated based on its threats intelligence procedure.

NOTE 2: Rapid technology improvement can lead to significant progress in industry best practice FAR and FRR performance even in the short term.

NOTE 3: An example of industry best practice reference can be the one-to-one face matching results reported from the NIST Face Recognition Vendor Test.

NOTE 4: The upcoming CEN standards on "European requirements for biometric products" can in the future provide application profiles that can be used by the IPSP to define such goals.

BIN-8.4.3-06X: The biometric algorithms and technologies applied shall be systematically tested in accordance with ISO/IEC 19795-1 [4] against updated reference data sets and against the goals set by the IPSP.

NOTE 5: The applicable analysis in ISO/IEC 19795-1 [4] will usually be one-to-one matching.

BIN-8.4.3-07X: Test results for the biometric face recognition shall achieve FAR in accordance with the goal stated in the practice statement.

BIN-8.4.3-08X: Test results for the biometric face recognition should achieve False Rejection Rate (FRR) in accordance with the goal stated in the practice statement.

NOTE 6: False Rejection Rate has impact on user-friendliness, which can indirectly have an impact on security.

BIN-8.4.3-09X: The biometric face recognition should apply means to detect morphed photos in identity documents.

NOTE 7: 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 issuing 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 both by a registration officer and by face biometrics with a reliability above the applied threshold, meaning more than one person can use the identity document containing the morphed photo.

NOTE 8: Morphing detection means are best applied in the binding to applicant step of an identity proofing process when a new photo, known not to be morphed, of the applicant can be compared to the potentially morphed reference photo. The upcoming ISO/IEC 20059 [i.33] "Methodologies to evaluate the resistance of biometric recognition systems to morphing attacks" can in the future provide guidance.

8.4.4 Binding to applicant by manual face verification

[CONDITIONAL] If manual binding of the applicant to an identity document is used, the following requirements apply:

BIN-8.4.4-01X: The registration officer shall compare the face image obtained from the applicant's identity document with the applicant's physical appearance, either from the applicant's physical presence, from a video sequence captured according to the requirements of clause 8.4.2 of the present document, or from image(s) derived from or captured together with the video sequence.

BIN-8.4.4-02: The registration officer performing the binding to applicant shall receive training before being allowed to make any comparison, with training repeated or refreshed at least yearly.

EXAMPLE 1: See the FISWG Minimum Training Criteria for Assessors Using Facial Recognition Systems [i.22] or for more extensive description the ENFSI Best Practice Manual for Facial Image Comparison [i.23], Appendix A.

BIN-8.4.4-03: The registration officer shall perform a morphological analysis according to a defined feature list.

EXAMPLE 2: As recommended by the FISWG Facial Comparison Overview and Methodology Guidelines [i.20] and the corresponding checklist in [i.21].

BIN-8.4.4-04X: The registration officer shall be allowed to spend sufficient time for the face comparison and have working conditions that do not impede the registration officer's judgement.

NOTE 1: In general, an assessment according to the FISWG Facial Comparison Overview and Methodology Guidelines [i.20] can be sufficient, while a review according to the same document can be required at least for remote identity proofing.

BIN-8.4.4-05: The registration officer should have tools available to magnify images to view details.

NOTE 2: With physical presence and physical identity document, this can be a magnifying glass for the face image printed on the document. If face images are used, computerized tools are assumed.

[CONDITIONAL] BIN-8.4.4-06: If binding to applicant is done by comparing face images or video sequences, the registration officer should use computerized tools in the face comparison.

EXAMPLE 3: Tool for superimposition of images described by the FISWG Facial Comparison Overview and Methodology Guidelines [i.20].

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

[CONDITIONAL] If the applicant is a legal person or a natural person representing a legal person, the following requirements apply:

BIN-8.4.5-01: Validated evidence shall prove that the legal person exists and that the application to the trust service is a willful act carried out on behalf of the legal person.

[CONDITIONAL] BIN-8.4.5-02X: If the applicant is a natural person representing a legal person, the identity of the natural person shall be proven according to an applicable use case from clause 9 or Annex C of the present document.

[CONDITIONAL] BIN-8.4.5-03: If the applicant is a natural person representing a legal person, validated evidence shall prove the natural person's authorization to represent the legal person.

[CONDITIONAL] BIN-8.4.5-04X: If the applicant is a natural person representing a legal person, and the legal person is listed in a trusted register, the natural person's authorization to represent the legal person should be proven by information from that register.

NOTE 1: This implies that the natural person has one of the roles listed in the trusted register and that this role is authorized to represent the legal person in the identity proofing context.

NOTE 2: The trusted register can be an authentic source as defined by the amended eIDAS regulation [i.25] and the evidence can be conveyed as a qualified or non-qualified electronic attestation of attributes as defined by the same regulation.

8.5 Issuing of proof

8.5.1 Result of the identity proofing

ISS-8.5.1-01: The result of the identity proofing shall be delivered securely to the trust service provider, regarding the authenticity, integrity, and confidentiality of the result.

EXAMPLE 1: The result can be digitally signed and encrypted at the message level or be transmitted over a properly secured communication channel.

NOTE 1: The present document places no requirement on the format of the result of the identity proofing. Example formats can be a document (e.g. PDF), structured data (e.g. XML, JSON), an identity assertion (e.g. OIDC, SAML), or an electronic attestation of attributes.

NOTE 2: The result of the identity proofing process can convey the attributes that are verified and the LoIP, but can even be a simple 'success' or 'failure' statement meaning that identity attributes provided by the TSP at the start of the identity proofing process are verified (or not) against the applicant to the required LoIP.

NOTE 3: The present document makes no assumption on the attributes to convey, whether the applicant is a natural person, a legal person, or a natural person representing a legal person (roles or authorizations can be relevant in the latter case).

NOTE 4: The present document makes no assumptions on the information to convey for identity proofing processes that do not complete successfully.

ISS-8.5.1-02: The result of the identity proofing process shall convey the LoIP achieved by the identity proofing process for the identity attributes required for the unique identification of the applicant in the identity proofing context.

EXAMPLE 2: By referring to the Baseline or Extended LoIP defined by the present document.

[CONDITIONAL] ISS-8.5.1-03X: If the identity proofing process conveys identity attributes that are not required for unique identification in the identity proofing context, and whose assurance differ from the LoIP of the overall result of the identity proofing process, an indication of the differing assurance should be conveyed in the identity proofing result.

8.5.2 Evidence of the identity proofing process

NOTE 1: In this clause 8.5.2, the term "evidence" means audit information for the identity proofing process as such, and not authoritative or supplementary evidence as in other clauses of the document. See also clause 7.10 of the present document.

ISS-8.5.2-01: Evidence of the identity proofing process shall be gathered and retained in compliance with the identity proofing context.

NOTE 2: Evidence can be retained in digital or paper format.

NOTE 3: The need to retain evidence of identity proofing processes that did not complete successfully can be determined by the identity proofing context.

NOTE 4: Gathering and retention of evidence is required to comply with applicable data protection legislation, notably GDPR if the identity proofing process is carried out under the legislation of an EU Member State

ISS-8.5.2-02X: The evidence of the identity proofing process shall document the authoritative and supplementary evidence used in the identity proofing process and the issuer or source of that evidence.

EXAMPLE 1: An identity document can be identified by the issuer name and document number, or by retaining a copy of the document, possibly in the form of an image if a physical identity document is used. Retaining a copy can, depending on the identity proofing context, be required, allowed, or forbidden.

ISS-8.5.2-03: The evidence of the identity proofing process should completely document the identity proofing process.

EXAMPLE 2: Including images captured in a remote identity proofing process; however, retaining images of a human applicant can, depending on the identity proofing context, be required, allowed, forbidden, or limited in time.

ISS-8.5.2-04: Evidence of the identity proofing process shall be retained for the necessary retention time given by the identity proofing context.

EXAMPLE 3: A typical requirement from a TSP is to retain evidence of the identity proofing process as long as the applicant remains a subject/subscriber of the TSP plus some years after that time.

ISS-8.5.2-05: The evidence of the identity proofing process shall be stored in a tamper-proof way.

ISS-8.5.2-05A: The time of completion of the identity proofing process shall be part of the evidence.

NOTE 5: A (qualified) timestamp applied to the evidence can both prove the time and provide the tampering protection of the evidence.

ISS-8.5.2-06: The evidence of the identity proofing process shall be stored in a way that guarantees the confidentiality of the information.

ISS-8.5.2-07: The evidence of the identity proofing process shall be stored in a way that ensures the possibility to search, retrieve, and re-verify the identity proofing result.

NOTE 6: Offline storage or other means that will result in a prolonged response time are possible.

NOTE 7: If an identity document has been used in the identity proofing process, and no copy of that document has been retained, re-verification depends on the ability to obtain the document based on its identification.

ISS-8.5.2-08: At the end of the retention time defined by **ISS 8.5.2-04**, the evidence of the identity proofing process and all personal data on the applicant shall be deleted.

9 Use cases for identity proofing to Baseline and Extended LoIP

9.1 Introduction, compliance with the present document, general requirements for all use cases

USE-9.1-01X: To be compliant with the present document, an identity proofing process shall conform to at least one of the use cases in clause 9 or Annex C of the present document for Baseline LoIP or Extended LoIP.

USE-9.1-01A: Compliance with the claimed use cases and the claimed LoIP from the present document should be assessed by an independent, accredited conformity assessment body.

NOTE 1: Clause 9 of the present document specifies identity proofing use cases by combining requirements from clause 8 covering the five steps of an identity proofing process: initiation, attribute and evidence collection, attribute and evidence validation, binding to applicant, issuing of proof. Conformance to one or more of the use cases specified can be claimed.

NOTE 2: The identity proofing context can pose requirements that only certain use cases are applicable.

NOTE 3: The proposed use cases can be carried out in a synchronous process, meaning that all steps of the identity proofing process including issuing of proof are carried out in one continuous process, or an asynchronous process, where the validation and binding tasks and issuing of proof are done at a later time.

NOTE 4: See ETSI EN 319 403-1 [i.6] for guidance on the assessment of TSP processes and services.

USE-9.1-02X: The requirements in the following clauses of the present document shall apply to all use cases:

- clause 5 (operational risk assessment);
- clause 6 (policies and practices);
- clause 7 (identity proofing service management and operation);
- clause 8.1 (initiation);
- clause 8.2.1 (attribute and evidence collection general requirements);
- clause 8.3.1 (attribute and evidence validation general requirements);
- clause 8.4.1 (binding to applicant general requirements); and
- clause 8.5 (issuing of proof).

USE-9.1-03X: Other use cases than those in the present clause 9 may be specified by combining elements from clause 8 of the present document in different ways; for such use cases, the resulting use case's proper handling of the risks identified as relevant to the Baseline or Extended LoIP shall be demonstrated.

NOTE 5: Other means, and consequently other use cases, than those described in the present document can be used to reach Baseline LoIP or Extended LoIP. For example, the present document does not consider use cases where the applicant is a known subject, e.g. in cases where identity proofing is required to be repeated regularly, or use cases for continuous identity proofing where the behaviour of the subject over time can be used to determine the risk or the likelihood that the identity is correct.

9.2 Use cases for identity proofing of natural person

9.2.1 Use cases using an identity document with physical presence of the applicant

9.2.1.1 General requirements

[CONDITIONAL] If the identity proofing is based on the applicant's physical presence, the following requirements apply.

NOTE 1: For the physical presence use cases, the same requirements apply for both Baseline and Extended LoIP.

NOTE 2: The requirement for physical presence does not imply that the applicant has to be present during all the steps of the use case, e.g. an identity proofing process can be asynchronous with the result determined at a later time than the capturing of the information.

NOTE 3: The identity proofing context can mandate a manual operation use case, or an automated use case, or a hybrid use case, or leave the selection of use case open.

NOTE 4: While the normal case is that the applicant visits the physical location where the identity proofing takes place, a case where the registration officer visits the physical location where the applicant is present is also possible.

USE-9.2.1.1-01: Attribute collection shall be according to the requirements of clause 8.2.2.1 of the present document.

USE-9.2.1.1-02: At least one digital or physical identity document shall be used as authoritative evidence.

USE-9.2.1.1-03: Collection of evidence shall be according to the requirements in clause 8.2.3 of the present document.

USE-9.2.1.1-04: The identity proofing may use trusted registers and/or proof of access and/or documents and attestations as supplementary evidence.

USE-9.2.1.1-05: The identity proofing may use additional digital or physical identity documents as supplementary evidence.

USE-9.2.1.1-06: The identity proofing may use existing eID means as supplementary evidence.

USE-9.2.1.1-07: The identity proofing may use existing digital signature means as supplementary evidence.

NOTE 5: The identity proofing context can require the use of specific supplementary evidence, e.g. validation of the identity against a population register or identity document register.

9.2.1.2 Use case for manual operation

[CONDITIONAL] If the identity proofing is based on the applicant's physical presence, and validation of evidence is manual using a physical identity document, and binding to applicant is by manual face verification, then the following requirements apply.

NOTE: This is the most common use case for physical presence, where a registration officer manually validates a physical identity document and manually performs binding to applicant. The hybrid and automated use cases cover use of digital identity documents.

USE-9.2.1.2-01: The registration officer shall guide the applicant and carry out the identity proofing process according to a defined process description.

USE-9.2.1.2-02: The identity proofing process shall specify how the registration officer shall handle deviations from expected results or expected behaviour of the applicant, including the conditions where the identity proofing process shall be aborted, and the information to convey to the applicant when an identity proofing process is aborted.

EXAMPLE: The applicant can be informed only that the process has failed with no further information, or be informed of the specific reason why the process failed.

USE-9.2.1.2-03X: At least one physical identity document shall be used as authoritative evidence.

USE-9.2.1.2-04X: Evidence validation shall be according to the requirements in clause 8.3.3 of the present document, including requirements that are marked CONDITIONAL, where the condition is on physical presentation of the identity document or on manual validation of the identity document.

USE-9.2.1.2-05: Binding to applicant shall be according to requirements in clause 8.4.4 of the present document.

9.2.1.3 Use case for hybrid manual and automated operation

[CONDITIONAL] If the identity proofing is based on the applicant's physical presence, validation of evidence is automated using a digital identity document, and binding to applicant is by manual face verification, then the following requirements apply.

NOTE 1: This use case resembles manual border control with a digital identity document obtained from the chip of a passport or national identity card. The identity document content, including face photo, is displayed on a screen to the registration officer that manually compares to the applicant's appearance.

USE-9.2.1.3-01: The registration officer shall guide the applicant and carry out the identity proofing process according to a defined process description.

USE-9.2.1.3-02: The identity proofing process shall specify how the registration officer shall handle deviations from expected results or expected behaviour of the applicant, including the conditions where the identity proofing process shall be aborted, and the information to convey to the applicant when an identity proofing process is aborted.

EXAMPLE: The applicant can be informed only that the process has failed with no further information, or be informed of the specific reason why the process failed.

USE-9.2.1.3-03X: At least one digital identity document shall be used as authoritative evidence.

NOTE 2: The use of a physical identity document is not considered common practice for the hybrid use case of physical presence. This would require on-site equipment to scan and analyse the physical identity document. When the digital identity document is read from a chip embedded in a physical identity document, the physical identity document can however be used as supplementary evidence.

USE-9.2.1.3-04: Evidence validation shall be according to the requirements in clause 8.3.2 of the present document.

USE-9.2.1.3-04A: A face image of the applicant should be captured.

[CONDITIONAL] USE-9.2.1.3-04B: If a face image is captured according to **USE-9.2.1.3-04A**, unless the face image is captured by specialized equipment in a controlled environment, the capture of the face image of the applicant shall be according to the requirements in clause 8.4.2 of the present document

NOTE 3: Manual binding to applicant can be done by comparing the face image from the identity document to the applicant's physical appearance, although comparing against a face image is recommended.

NOTE 4: See note 3 in clause 9.2.1.4 below regarding "specialized equipment".

USE-9.2.1.3-05: Binding to applicant shall be according to the requirements in clause 8.4.4 of the present document.

9.2.1.4 Use case for automated operation

[CONDITIONAL] If the identity proofing is based on the physical presence of the applicant, validation of evidence is automated using digital identity document, and binding to applicant is by automated face biometrics, then the following requirements apply.

NOTE 1: This use case requires equipment that can read and validate a digital identity document, obtain a face photo of the applicant, and perform binding to applicant by face biometrics. The use case resembles automated border control.

USE-9.2.1.4-01: At least one registration officer shall be present at the physical location of the identity proofing.

USE-9.2.1.4-02: The applicant shall receive guidance on the process either by automated means or by the registration officer.

USE-9.2.1.4-03: The registration officer shall be alerted in case of deviations from expected results or expected behaviour of the applicant.

USE-9.2.1.4-04: The identity proofing process shall specify how the registration officer shall handle deviations from expected results or expected behaviour of the applicant, including the conditions where the identity proofing process shall be aborted, and the information to convey to the applicant when an identity proofing process is aborted.

EXAMPLE: The applicant can be informed only that the process has failed with no further information or be informed of the specific reason why the process failed.

USE-9.2.1.4-05X: At least one digital identity document shall be used as authoritative evidence.

NOTE 2: A fully automated procedure to Baseline or Extended LoIP requires the use of a digital identity document.

USE-9.2.1.4-06: Evidence validation shall be according to the requirements in clause 8.3.2 of the present document.

USE-9.2.1.4-07: A face image of the applicant shall be captured.

[CONDITIONAL] USE-9.2.1.4-08X: Unless the face image is captured by specialized equipment in a controlled environment, the capture of the face image of the applicant shall be according to the requirements in clause 8.4.2 of the present document.

NOTE 3: Specialized equipment can be similar to automated border control or a biometric kiosk in a controlled environment. When the applicant is physically present, the requirements in clause 8.4.2, e.g. to capture a video sequence, are not necessarily relevant under such conditions.

USE-9.2.1.4-09: Binding to applicant shall be according to the requirements in clause 8.4.3 of the present document.

9.2.2 Use cases using an identity document for attended remote identity proofing

9.2.2.1 General requirements

[CONDITIONAL] If the identity proofing is based on the remote presence of the applicant with online communication with a registration officer, the following requirements apply.

NOTE 1: For the attended remote use cases, the requirements for Baseline LoIP and Extended LoIP differ in that manual validation of a physical identity document can be used for Baseline LoIP but not for Extended LoIP. In addition, the risk assessment for the two levels, especially concerning attack potential to consider, will be different and can lead to differences in implementation.

NOTE 2: The identity proofing context can mandate a manual operation use case, or a hybrid use case, or leave the selection of use case open. As attended remote identity proofing requires the presence of a registration officer, fully automated identity proofing is considered not relevant.

USE-9.2.2.1-01: The registration officer shall guide the applicant and carry out the identity proofing process according to a defined process description.

USE-9.2.2.1-02: The identity proofing process shall specify how the registration officer shall handle deviations from expected results or expected behaviour of the applicant, including the conditions where the identity proofing process shall be aborted, and the information to convey to the applicant when an identity proofing process is aborted.

EXAMPLE: The applicant can be informed only that the process has failed with no further information or be informed of the specific reason why the process failed.

USE-9.2.2.1-03: Attribute collection shall be according to the requirements of clause 8.2.2.1 of the present document.

USE-9.2.2.1-04: At least one digital or physical identity document shall be used as authoritative evidence.

USE-9.2.2.1-05: Collection of evidence shall be according to the requirements in clause 8.2.3 of the present document.

USE-9.2.2.1-06: VOID.

USE-9.2.2.1-07: The identity proofing may use trusted registers and/or proof of access and/or documents and attestations as supplementary evidence.

USE-9.2.2.1-08: The identity proofing may use additional digital or physical identity documents as supplementary evidence.

USE-9.2.2.1-09: The identity proofing may use existing eID means as supplementary evidence.

USE-9.2.2.1-10: The identity proofing may use existing digital signature means as supplementary evidence.

NOTE 3: The identity proofing context can require use of the specific supplementary evidence, e.g. validation of the identity against a population register or identity document register.

9.2.2.2 Use case for manual operation (Baseline LoIP only)

[CONDITIONAL] If the identity proofing is based on the remote presence of the applicant with online communication with a registration officer, and validation of evidence is manual using a physical identity document, and binding to applicant is by manual face verification, then the following requirements apply.

NOTE 1: This use case is similar to the physical appearance with manual operation case in clause 9.2.1.2 of the present document. Validation of the physical identity document and binding to applicant are more difficult than with physical presence, but the use case is acceptable for Baseline LoIP provided that the difficulty is compensated by the specialist skills of the registration officer and the availability of tools to the registration officer. The hybrid use case in clause 9.2.2.3 is strongly recommended above the manual use case.

USE-9.2.2.2-01X: At least one physical identity document shall be used as authoritative evidence.

USE-9.2.2.2-02X: Evidence validation shall be according to the requirements in clause 8.3.3 of the present document, including requirements that are marked CONDITIONAL, where the condition is on remote presentation of the identity document or on manual validation of the identity document.

USE-9.2.2.2-02A: A face image of the applicant should be captured according to the requirements in clause 8.4.2 of the present document

NOTE 2: Manual binding to applicant can be done by comparing the face image from the identity document to the applicant's online appearance, although comparing against a face image is recommended.

USE-9.2.2.2-03: Binding to applicant shall be according to the requirements in clause 8.4.4 of the present document.

9.2.2.3 Use case for hybrid manual and automated operation

[CONDITIONAL] If the identity proofing is based on remote presence of the applicant with online communication with a registration officer, and validation of evidence is either automated using a digital identity document or combined automated and manual for a physical identity document, and binding to applicant is either by manual face verification or a combination of manual face verification and face biometrics, then the following requirements apply.

NOTE 1: This hybrid use case can use either digital or physical identity document, where automated means for evidence validation is required even for a physical identity document. While manual binding to applicant is allowed as per the manual use case in clause 9.2.2.2, combined manual and face biometric binding to applicant is highly recommended.

[CONDITIONAL] USE-9.2.2.3-01X: If a digital identity document is used as authoritative evidence, evidence validation shall be according to the requirements in clause 8.3.2 of the present document.

NOTE 2: A digital identity document will yield more reliable evidence validation than a physical identity document.

[CONDITIONAL] USE-9.2.2.3-02X: If a physical identity document is used as authoritative evidence, evidence validation shall be according to the requirements in clause 8.3.3 of the present document, including requirements that are marked CONDITIONAL, where the condition is on remote presentation of the identity document or on manual validation of the identity document**.**

[CONDITIONAL] USE-9.2.2.3-03X: If a physical identity document is used as authoritative evidence, requirements **VAL-8.3.3-18**, **VAL-8.3.3-19**, and **VAL-8.3.3-20** of the present document shall apply as additional to manual validation of the identity document.

NOTE 3: Meaning that automated analysis and machine learning technology is mandatory for validation of the physical identity document, combined with manual validation.

[CONDITIONAL] USE-9.2.2.3-03A: If face biometrics is used for binding to applicant, a face image of the applicant shall be captured according to the requirements in clause 8.4.2 of the present document.

[CONDITIONAL] USE-9.2.2.3-03B: If only manual binding to applicant is used, a face image of the applicant should be captured according to the requirements in clause 8.4.2 of the present document.

NOTE 4: Manual binding to applicant can be done by comparing the face image from the identity document to the applicant's online appearance, although comparing against a face image is recommended.

USE-9.2.2.3-04: Binding to applicant shall be according to one of the following alternatives:

a) by applying both manual binding to applicant (clause 8.4.4) and face biometrics (clause 8.4.3) in parallel; or

b) by applying face biometrics (clause 8.4.3) with fallback to manual binding (clause 8.4.4), where the outcome of the face biometrics does not yield a reliable match; or

c) by applying only manual binding to applicant (clause 8.4.4).

[CONDITIONAL] USE-9.2.2.3-05X: If binding to applicant is by applying manual face verification and automated face biometrics in parallel, and the two binding methods yield different results, the identity proofing process shall be aborted.

9.2.3 Use cases using an identity document for unattended remote identity proofing

9.2.3.1 General requirements

[CONDITIONAL] If the identity proofing is based on the remote presence of the applicant with unattended online communication, the following requirements apply.

NOTE 1: For the unattended remote use cases, manual operation, whether it is manual validation of a physical identity document or manual binding to applicant or both, is considered to only be able to reach Baseline LoIP. Hybrid manual and automated operation and automated operation can reach Extended LoIP; automated operation requires use of a digital identity document.

NOTE 2: While the user dialogue of the identity proofing is automated, subsequent validation of evidence and binding to applicant can still be manual as for the attended remote use case but only to reach Baseline LoIP. Hybrid automated and manual validation of evidence and binding to applicant and fully automated operation are more relevant use cases. The identity proofing context can mandate an automated use case, or a hybrid use case, or a manual use case, or leave the selection of use case open.

USE-9.2.3.1-01: The applicant shall receive automated guidance throughout the identity proofing process.

USE-9.2.3.1-02: The automated process' handling of deviations from expected results or expected behaviour of the applicant shall be specified, including the conditions where the identity proofing process shall be aborted, and the information to convey to the applicant when an identity proofing process is aborted.

EXAMPLE: The applicant can be informed only that the process has failed with no further information or be informed of the specific reason why the process failed.

USE-9.2.3.1-03: Attribute collection shall be according to the requirements of clause 8.2.2.1 of the present document.

USE-9.2.3.1-04: The process shall use at least one digital or physical identity document as authoritative evidence.

USE-9.2.3.1-05: Collection of evidence shall be according to the requirements in clause 8.2.3 of the present document.

USE-9.2.3.1-06: The capture of the face image of the applicant shall be according to the requirements in clause 8.4.2 of the present document.

USE-9.2.3.1-07: The identity proofing may use trusted registers and/or proof of access and/or documents and attestations as supplementary evidence.

USE-9.2.3.1-08: The identity proofing may use additional digital or physical identity documents as supplementary evidence.

USE-9.2.3.1-09: The identity proofing may use existing eID means as supplementary evidence.

USE-9.2.3.1-10: The identity proofing may use existing digital signature means as supplementary evidence.

NOTE 3: The identity proofing context can require the use of specific supplementary evidence, e.g. validation of the identity against a population register or identity document register.

9.2.3.2 Use case for manual operation (Baseline LoIP only)

[CONDITIONAL] If the identity proofing is based on the remote presence of the applicant with unattended online communication, and validation of evidence is manual using a physical identity document, and binding to applicant is by manual face verification, then the following requirements apply.

NOTE 1: The hybrid use case in clause 9.2.3.3 is strongly recommended above the manual use case.

USE-9.2.3.2-01: The identity proofing process shall specify how the registration officer shall handle deviations from expected results or expected behaviour of the applicant, including the conditions where the identity proofing process shall be aborted, and the information to convey to the applicant when an identity proofing process is aborted.

NOTE 2: Deviations can be detected both by automated means during the online communication with the applicant and by the registration officer during the manual validation of evidence and manual binding to applicant.

USE-9.2.3.2-03X: At least one physical identity document shall be used as authoritative evidence.

USE-9.2.3.2-04X: Evidence validation shall be according to the requirements in clause 8.3.3 of the present document, including requirements that are marked CONDITIONAL, where the condition is on remote presentation of the identity document or on manual validation of the identity document.

USE-9.2.3.2-05: Binding to applicant shall be according to the requirements in clause 8.4.4 of the present document.

9.2.3.3 Use case for hybrid manual and automated operation

[CONDITIONAL] If the identity proofing is based on the remote presence of the applicant with unattended online communication, and validation of evidence is either automated using a digital identity document or combined automated and manual for physical identity document, and binding to applicant is either by manual face verification or a combination of manual face verification and face biometrics, then the following requirements apply.

NOTE 1: This hybrid use case can use a digital or physical identity document; automated means for evidence validation is required even for a physical identity document.

USE-9.2.3.3-01: The identity proofing process shall specify how the registration officer shall handle deviations from expected results or expected behaviour of the applicant, including the conditions where the identity proofing process shall be aborted, and the information to convey to the applicant when an identity proofing process is aborted.

NOTE 2: Deviations can be detected by automated means during the online communication with the applicant, by automated means during subsequent automated evidence validation and binding to applicant, and by the registration officer during manual validation of evidence and manual binding to applicant.

[CONDITIONAL] USE-9.2.3.3-02X: If a digital identity document is used as authoritative evidence, evidence validation shall be according to the requirements in clause 8.3.2 of the present document.

NOTE 3: A digital identity document will yield more reliable evidence validation than a physical identity document.

[CONDITIONAL] USE-9.2.3.3-03X: If physical identity document is used as authoritative evidence, evidence validation shall be according to the requirements in clause 8.3.3 of the present document, including requirements that are marked CONDITIONAL, where the condition is on remote presentation of the identity document or on manual validation of the identity document.

[CONDITIONAL] USE-9.2.3.3-04X: If a physical identity document is used as authoritative evidence, requirements **VAL-8.3.3-18**, **VAL-8.3.3-19**, and **VAL-8.3.3-20** of the present document shall apply as additional to manual validation of the identity document.

NOTE 4: Meaning that automated analysis and machine learning technology is mandatory for validation of the physical identity document, combined with manual validation.

USE-9.2.3.3-05X: Binding to applicant shall be according to one of the following alternatives:

a) by applying both manual binding to applicant (clause 8.4.4) and face biometrics (clause 8.4.3) in parallel; or

b) by applying face biometrics (clause 8.4.3) with fallback to manual binding (clause 8.4.4) where the outcome of the face biometrics does not yield a reliable match; or

c) by applying only manual binding to applicant (clause 8.4.4); this alternative can only be used for Baseline LoIP.

[CONDITIONAL] USE-9.2.3.3-06X: If binding to applicant is achieved by applying manual face verification and automated face biometrics in parallel, and the two binding methods yield different results, the identity proofing process shall be aborted.

9.2.3.4 Use case for automated operation

[CONDITIONAL] If the identity proofing is based on the remote presence of the applicant with automated online communication, and validation of evidence is automated using a digital identity document, and binding to applicant is by automated face biometrics, then the following requirements apply.

NOTE: A fully automated process requires the use of a digital identity document.

USE-9.2.3.4-01X: At least one digital identity document shall be used as authoritative evidence.

USE-9.2.3.4-02: Evidence validation shall be according to the requirements in clause 8.3.2 of the present document.

USE-9.2.3.4-03: Binding to applicant shall be according to the requirements in clause 8.4.3 of the present document.

9.2.4 Use case for identity proofing by authentication using eID means

[CONDITIONAL] If the identity proofing is based on authentication using eID means, the following requirements apply.

USE-9.2.4-01: Attribute collection shall be according to the requirements of clause 8.2.2.1 of the present document.

USE-9.2.4-02: Collection of evidence shall be according to the requirements in clause 8.2.4 of the present document.

[CONDITIONAL] USE-9.2.4-02A: If Baseline LoIP is targeted, requirement **COL-8.2.4-02X** shall apply.

[CONDITIONAL] USE-9.2.4-02B: If Extended LoIP is targeted, requirement **COL-8.2.4-02A** shall apply.

USE-9.2.4-03: Validation of evidence shall be according to the requirements in clause 8.3.4 of the present document.

USE-9.2.4-04: The identity proofing may use trusted registers and/or proof of access and/or documents and attestations as supplementary evidence.

USE-9.2.4-05: The identity proofing may use digital or physical identity documents as supplementary evidence.

USE-9.2.4-06: The identity proofing may use another eID means as supplementary evidence.

USE-9.2.4-07: The identity proofing may use existing digital signature means as supplementary evidence.

NOTE: The identity proofing context can require the use of specific supplementary evidence, e.g. validation of the identity against a population register.

9.2.5 Use case for identity proofing using digital signature with certificate

[CONDITIONAL] If the identity proofing is based on the use of a digital signature with a certificate, the following requirements apply.

USE-9.2.5-01: Attribute collection shall be according to the requirements of clause 8.2.2.1 of the present document.

USE-9.2.5-02: Collection of evidence shall be according to the requirements in clause 8.2.5 of the present document.

[CONDITIONAL] USE-9.2.4-02A: If Baseline LoIP is targeted, requirement **COL-8.2.5-03X** shall apply.

[CONDITIONAL] USE-9.2.4-02B: If Extended LoIP is targeted, requirement **COL-8.2.5-03A** shall apply.

USE-9.2.5-03: Validation of evidence shall be according to the requirements in clause 8.3.5 of the present document.

USE-9.2.5-04: The identity proofing may use trusted registers and/or proof of access and/or documents and attestations as supplementary evidence.

USE-9.2.5-05: The identity proofing may use digital or physical identity documents as supplementary evidence.

USE-9.2.5-06: The identity proofing may use eID means as supplementary evidence.

USE-9.2.5-07: The identity proofing may use an additional digital signature using a different certificate as supplementary evidence.

NOTE: The identity proofing context can require the use of specific supplementary evidence, e.g. validation of the identity against a population register.

9.3 Use case for identity proofing of legal person

[CONDITIONAL] If identity proofing is of a legal person, the following requirements apply.

NOTE 1: The same requirements apply for both Baseline and Extended LoIP.

NOTE 2: The present clause does not assume the involvement of an authorized natural person representing the legal person, but in reality some human involvement is needed in the process.

NOTE 3: The use of identity document and proof of access as evidence is considered out of scope for a legal person.

USE-9.3-01: The identity proofing shall collect attributes according to the requirements in clause 8.2.2.2 of the present document.

USE-9.3-02X: The identity proofing shall use documents and attestations as authoritative evidence witnessing the purpose of the identity proofing according to the requirements in clauses 8.2.8 and 8.3.8 of the present document.

NOTE 4: Attestations can be in the form of qualified or non-qualified electronic attestation of attributes as defined by the amended eIDAS regulation [i.25].

[CONDITIONAL] USE-9.3-03X: If the legal person is registered in a trusted register, the requirements in clauses 8.2.6 and 8.3.6 of the present document shall apply.

NOTE 5: The trusted register can be an authentic source as defined by the amended eIDAS regulation [i.25].

NOTE 6: The identity proofing context can require the use of specific documents and attestations or trusted registers as evidence.

[CONDITIONAL] USE-9.3-03A: If the legal person is not registered in any trusted register, the attributes that would otherwise be collected and validated from a trusted register shall be collected and validated by other means providing the same confidence as a trusted register would do.

EXAMPLE: In some countries, public sector bodies are not registered in official legal person registers.

USE-9.3-04X: The identity proofing may use authentication by eID means as evidence according to the requirements in clauses 8.2.4 and 8.3.4 of the present document; requirement **VAL-8.2.4-02X** or **VAL-8.2.4-02A** apply dependent on whether the desired LoIP is Baseline or Extended.

NOTE 7: While eID means authenticating a legal person exists in the market, such solutions are not common.

USE-9.3-05X: The identity proofing may use a digital signature with a certificate as evidence according to the requirements in clauses 8.2.5 and 8.3.5 of the present document; requirement **VAL-8.2.5-03X** or **VAL-8.2.5-03A** apply dependent on whether the desired LoIP is Baseline of Extended.

NOTE 8: A digital signature for a legal person is termed an 'electronic seal' by the amended eIDAS regulation [i.25].

NOTE 9: Digital signatures for legal persons (electronic seals) are used for different purposes. It is, in general, difficult to assess that identity proofing of the legal person is a legitimate use of the digital signature and certificate. The amended eIDAS regulation [i.25] Article 35 assigns to a qualified electronic seal only the presumption of integrity of the data sealed and correctness of the origin of the data.

USE-9.3-06: The identity proofing may, in addition to documents and attestations and trusted register as covered by requirements **USE-9.3-02X** and **USE-9.3-03X**, use additional trusted registers and/or proof of access and/or additional documents and attestations as supplementary evidence.

9.4 Use case for identity proofing of natural person representing legal person

[CONDITIONAL] If identity proofing is of a natural person representing a legal person, the following requirements apply.

[CONDITIONAL] USE-9.4-01X: If Baseline LoIP is targeted, the identity proofing for the natural person shall be done according to at least the requirements for one of the use cases for Baseline LoIP in clause 9.2 of the present document.

[CONDITIONAL] USE-9.4-01A: If Extended LoIP is targeted, the identity proofing of the natural person shall be done according to the requirements for one of the use cases for Extended LoIP in clause 9.2 of the present document.

NOTE 1: The identity proofing context can specify that only certain use cases are allowed.

USE-9.4-01B: Attribute collection shall be according to the requirements of clause 8.2.2.3 of the present document.

USE-9.4-02X: Evidence collection shall be according to the requirements in clause 8.2.9 of the present document.

USE-9.4-03X: Evidence validation for the legal person shall be according to the relevant clauses 8.3.2 to 8.3.8 of the present document.

[CONDITIONAL] USE-9.4-04: If the legal person is registered in a trusted register, the requirements in clauses 8.2.6 and 8.3.6 of the present document apply.

NOTE 2: The trusted register can be an authentic source as defined by the amended eIDAS regulation [i.25].

[CONDITIONAL] USE-9.4-05: If the legal person is not registered in any trusted register, or the required attributes to validate the role of the natural person concerning the legal person are not present in the register, the required attributes for the legal person, including the natural person's authorization to represent the legal person, shall be validated by other means providing the same confidence as a trusted register would do.

EXAMPLE: In some countries, public sector bodies are not registered in official legal person registers.

USE-9.4-06: The identity proofing may, in addition to trusted register as covered by requirement **USE-9.4-04**, use additional trusted registers and/or proof of access and/or documents and attestations as supplementary evidence.

9.5 Use cases for additional identity proofing to enhance an identity proven by use of an eID from Baseline LoIP to Extended LoIP

9.5.1 General requirements

[CONDITIONAL] If the applicant is a natural person, including a natural person representing a legal person, and the identity of the applicant has been proven to Baseline LoIP by means of authentication using an eID, and an enhancement to Extended LoIP is required, the following requirements apply.

NOTE 1: Enhancing identity proofing for a legal person is out of scope of the present clause 9.5.

EXAMPLE: The purpose of the identity proofing process can be to issue a qualified certificate for electronic signature according to the amended eIDAS regulation [i.25] where the applicant is in possession of an eID at LoA substantial. This eID can be used to reach Baseline LoIP with enhancement according to one of the use cases in the present clause 9.5 in order to reach Extended LoIP.

USE-9.5.1-01: The identity proofing to Baseline LoIP shall be done by use of an eID according to the use case in clause 9.2.4 of the present document.

USE-9.5.1-02: The evidence used to enhance identity proofing from Baseline LoIP to Extended LoIP shall prove the same identity as the identity obtained from the identity proofing to Baseline LoIP.

NOTE 2: Note requirements in clause 8.3.1 of the present document for handling deviations in identity attributes between different evidence.

USE-9.5.1-03: The eID used for identity proofing to Baseline LoIP shall have been issued based on a separate identity proofing process from the identity proofing process to enhance to Extended LoIP.

NOTE 3: The eID can be issued based on evidence that is also used to enhance the identity proofing, but not in the same process.

USE-9.5.1-04: The identity proofing may use trusted registers and/or proof of access and/or documents and attestations as supplementary evidence.

USE-9.5.1-05: The identity proofing may use digital or physical identity documents as supplementary evidence.

USE-9.5.1-06: The identity proofing may use additional eID means as supplementary evidence.

USE-9.5.1-07: The identity proofing may use existing digital signature means as supplementary evidence.

9.5.2 Use case for enhancing identity proofing to Extended LoIP by a full identity proofing using an identity document

[CONDITIONAL] If the applicant is a natural person, including a natural person representing a legal person, and the identity of the applicant has been proven to Baseline LoIP by means of authentication using an eID, and an enhancement to Extended LoIP is done by use of identity proofing using an identity document and capture of face image of the applicant, the following requirements apply.

NOTE: One application of this use case can be to capture a reference face image and identity attributes bound to that face image that can later be used together with the eID to enhance identity proofing from Baseline to Extended LoIP according to clause 9.5.3 of the present document.

USE-9.5.2-01: The identity proofing to enhance from Baseline to Extended LoIP shall be according to the requirements for Extended LoIP from one of the use cases described in clauses 9.2.1, 9.2.2, or 9.2.3 of the present document.

9.5.3 Use case for enhancing identity proofing to Extended LoIP by use of a previously captured reference face image

[CONDITIONAL] If the applicant is a natural person, including a natural person representing a legal person, and the identity of the applicant has been proven to Baseline LoIP by means of authentication using an eID, and an enhancement to Extended LoIP is done by capturing a face image of the applicant and binding this image to a previously captured reference face image bound previously to the applicant's identity, the following requirements apply.

NOTE 1: For this use case, a face image and identity attributes bound to this face image are firstly captured for the applicant by a separate identity proofing process fulfilling requirements for Extended LoIP. The enhancement is done by using an eID to reach Baseline LoIP, and then in the same process capturing another face image according to the requirements for Extended LoIP and binding (comparing) this face image to the previously captured (reference) face image, and comparing the identity attributes bound to this (reference) face image to the identity attributes obtained from the eID. If these identity attributes match, an enhancement is obtained.

USE-9.5.3-01: An identity proofing process fulfilling the requirements for Extended LoIP from one of the use cases described in clauses 9.2.1, 9.2.2, or 9.2.3 of the present document shall be used to capture a reference face image and to bind the necessary identity attributes to this reference face image.

USE-9.5.3-02: All storage and transmission of the reference face image, the identity attributes bound to this reference face image, and the link between them shall be protected with respect to authenticity, integrity and confidentiality according to the identity proofing context.

NOTE 2: E.g. according to GDPR when the legislation of an EU Member State applies. The storage can be the responsibility of the IPSP, the TSP or another actor requesting the enhancement of the identity proofing, or another actor trusted by the IPSP to reliably store the reference face image and the identity attributes bound to this reference face image.

NOTE 3: The record of the reference face image and the identity attributes bound to this reference face image will be used as an authoritative source of identity information.

USE-9.5.3-03: The reference face image should be stored as a biometric template.

USE-9.5.3-04: Capturing a face image to be used to enhance to Extended LoIP shall be done according to the requirements for Extended LoIP in clause 8.4.2 of the present document.

USE-9.5.3-05: Binding of the face image used to enhance to Extended LoIP to the reference face image and the identity attributes bound to this reference face image shall be done either by automated face biometrics according to the requirements of clause 8.4.3 of the present document, or by a combination of automated face biometric according to the requirements of clause 8.4.3 of the present document and manual binding according to the requirements of clause 8.4.4 of the present document.

USE-9.5.3-06: A reference face image and the identity attributes bound to this reference face image shall have a determined maximum validity period, which shall be stated by the IPSP in its practice statement.

EXAMPLE 1: An updated reference face image and updated identity attributes can be required every 2-5 years.

USE-9.5.3-07: The IPSP shall in its practice statement state any rules the IPSP applies for obsoleting a reference face image and the identity attributes bound to this reference face image.

EXAMPLE 2: A reference face image can be deemed useful only as long as the identity document used in the identity proofing process to capture the reference face image and the identity attributes is valid.

Annex A (informative): Void

Annex B (informative): Threats to identity proofing

The list of threats below is compiled by ENISA in the report "Remote ID proofing - Analysis of methods to carry out identity proofing remotely" [i.15]. The list is compiled from the replies received by ENISA from their stakeholders' questionnaire and considering various other literature on identity proofing as referenced by the ENISA report. It is a non-exhaustive list of threats, as all such lists will be not least due to the rapidly changing threat landscape in the identity proofing area. The threats are at a relatively coarse level that can be detailed in further versions of the present document. Such detailing can be based on further work by ENISA.

Threats are described relatively to the process tasks described in clause 4.2 of the present document but with no specific threats for the issuing of proof task.

The following threats are described for the initiation task.

Table B.1: Example threats to the initiation task of identity proofing

Initiation threats	Coverage by ETSI TS 119 461 (the present document)
[T_POLICY_FLAW] Policy flaw. A remote identification proofing process has to take into account a large number of different contexts and when some are not correctly understood when defining the policy, this can lead to several vulnerabilities.	Identity proofing is required to identify the applicable identity proofing context and fulfil the constraints and requirements found by this context. Requirements to this effect are posed throughout clause 8.
[T_PHISHING] User accepts process initiation from attacker. Some remote identity proofing may be exposed to phishing attacks. This is for example the case in processes with interruptions and reconnections using SMS or email.	Full protection against phishing is not possible only by the TSP (or IPSP) since, if the applicant is tricked into visiting a phishing site, the TSP/IPSP will not even be aware of the situation. However, requirements in clauses 8.3.2 and 8.3.3 aim to ensure that even if an attacker uses a phishing site to trick the victim into a purported identity proofing process using identity documents, the attacker cannot later reuse the captured information to gain an identity proofing in the identity of the victim. Clauses 8.3.4 and 8.4.5 pose requirements for validation of eID means and digital signature means. Even when notified at eIDAS level substantial or high, some such means can be vulnerable to phishing attacks, which is out of control of the TSP/IPSP.

The following threats are described for the attribute and evidence collection and validation tasks.

Table B.2: Example threats to the attribute and evidence collection task of identity proofing

Attribute and evidence collection and validation threats	Coverage by ETSI TS 119 461 (the present document)
[T_DOC_WEAK] Insufficiently secured Identity document. Some identity documents which are still valid in Europe do not have remotely verifiable security features strong enough to achieve the expected level of assurance.	The starting point is that only passports and national identity cards are accepted. The identity proofing context will specify which documents to accept and can deny the use of documents that are of insufficient quality, like some old types of national identity cards. The identity proofing context can also accept other document types that have security to passports and national identity cards.

Attribute and evidence collection and validation threats	Coverage by ETSI TS 119 461 (the present document)
[T_DOC_IMPRECISE] Insufficiently precise Identity document. Some identity documents which are still valid in Europe do not include all the information necessary to uniquely and positively identify the applicant. Some do not have a unique identifier of the person and the information mentioned is not sufficient to avoid duplicates. For example, on the French identity card in force at the date of writing of this report, only the surname, first name, sex, date and name of the commune of birth appear. Cases of perfect duplicates on these elements are obviously common.	Attributes collected are required to uniquely identify the person in the identity proofing context. When necessary attributes are not available from a single evidence, supplementary evidence can be used to prove the remaining attributes. This includes additional attributes for electronic attestations of attributes.
[T_DOC_STOLEN] Stolen or revoked identity document. This case refers to an attacker using a stolen authentic document. This is a common identity theft scenario, most often combined with a presentation attack on the verification stage to deceive the software or the person who is going to verify that the picture on the identity document matches the person presenting it.	If the stolen document is genuine and belongs to another person, the situation can be detected during the binding to applicant task. For identity documents, revocation checking is covered by VAL-8.3.2-04X and VAL-8.3.3-09, stating that if an online status service exists for the document, this is required to be used if practically possible. In many cases, online checking may not be provided, or access may be limited. Implementing access may be infeasible for documents that are seldomly encountered if many different documents are accepted. For eID means a proper authentication protocol will not accept the use of a revoked eID. For digital signature means, revocation checking is an integral part of signature and certificate validation.
[T_DOC_FAKE] Counterfeited or forged identity document. A counterfeited document is a complete reproduction of an identity document while a forged document is an original document on which an attacker has modified one or more elements. In some cases, it may also be a stolen blank document personalized by the attacker. The imperfections of a counterfeited or forged document may be easier to conceal in the case of remote verification. See T_QUALITY_ALTERATION.	Verification of security elements of a physical identity document is required to ensure that the document is not counterfeit and not tampered with. For remote identity proofing, video capture of the presentation of the document is required since a picture will not enable the same level of checking of security elements. Hybrid processing with both manual and automated, machine-learning technology for validation is recommended, while a manual process is allowed, but only for Baseline LoIP. See also the response to T_DOC_FANTASY below. For a digital identity document, validation of the signature on the information is required, also checking that the issuer is trusted according to the identity proofing context.
[T_DOC_FANTASY] Fantasy or non-recognized identity document. A fantasy document is a document created from scratch without reference to an existing type of document. It is generally of a fairly coarse quality, although there are some relatively likely production channels for fancy documents. Identity documents issued by non-recognized states or by states that no longer exist can be classified in the same category.	The registration officer is required to have access to authoritative sources of information on document appearance and validation, such as PRADO. This is needed to ensure that the document exists and has the expected appearance and to obtain knowledge of security elements that can be checked (also for T_DOC_FAKE above).
[T_DOC_HUMAN_CAPABILITIES] Lack of operator capability or knowledge about [some] accepted identity documents. If an operator is involved in the data validation or verification phase, he may not have the capability or competence to perform this task satisfactorily. For example, he may be unfamiliar with the document or data source presented to him. An attacker will seek to produce a forged document relating to a type rarely encountered by operators to take advantage of their lack of expertise.	If the identity proofing context allows the use of many different documents, the measures mentioned for T_DOC_FAKE and T_DOC_FANTASY above are crucial. Requirements for training of registration officers are posed to ensure competence.

Attribute and evidence collection and validation threats	Coverage by ETSI TS 119 461 (the present document)
[T_DOC_HUMAN_ERROR] Non-handled human error. If an operator is involved in the data validation or verification phase, he may make an error.	Clear procedures are required to handle deviations, see requirements for the use cases in clause 9.2. Training is important, where requirements are posed both in VAL-8.3.3-13 for manual validation of a physical identity document and in clause 8.4.4 on binding to applicant by manual face verification. A hybrid use case combining automated and manual validation and binding to applicant is recommended, especially when physical identity documents are used, although manual processing is allowed. Still human errors cannot 100 % be eliminated. A fully automated process is possible when digital identity documents are used, removing the human error possibility. The same applies to use of eID means or digital signature means where validation is assumed to be fully automated.
[T_DOC_SOFTWARE_PERFORMANCE] Software capability to authenticate identity documents not at the required level. If a software component is involved in the data validation or verification phase, it may not be able to validate or verify adequately the identity document it is presented. Indeed, there are hundreds (or even thousands if one takes into account every single model variation) of valid identity document in use around the world. Software could support documents in an uneven way. An attacker will seek to produce a forged document relating to a more permissive document type.	This threat is relevant only when physical identity documents are used. VAL-8.3.3-20 states that if automated means and machine-learning technology are used to analyse physical identity documents, the algorithms and technology are required to be systematically tested against reference datasets and be kept updated to cope with changes in the threats and risk situation.
[T_DOC_CHIP_READING_NOT ALLOWED] Chip reading not allowed. Reading the chip of an eMRTD (electronic Machine-Readable Travel Document); most passports are compliant with ICAO 9303 Part 10 [2] if done carefully is a good way to recover identity attributes with a high level of assurance. However, this operation, while technically possible in accordance with ICAO 9303 Part 10 [2], is not always legally possible in some EU countries such as France.	This is an applicable threat with some national identity cards, like France as mentioned, and the restriction may only concern the face photo of the eMRTD and not the entire eMRTD. Additionally, not all existing national identity cards, and not all passports, have a chip with eMRTD. In all cases where a passport has eMRTD support, the eMRTD will expose a face photo. If the identity proofing context requires a digital identity document, then a passport or national identity card without eMRTD, or a national identity card where a face photo is unavailable with the eMRTD, cannot be used alone. The present document requires that an authoritative identity document includes a face photo since this is needed for binding to applicant. An eMRTD document that cannot expose a face photo can, however, be used in two ways: 1) As supplementary evidence of identity information, where binding to applicant is done by use of other evidence (another document, eID, digital signature). 2) As an eID, covered by the requirements for use of eID means in the present document, if the eMRTD document can be used in an authentication protocol. For example, the latter is the case for the German nPA eID building on eMRTD technology and the associated "eIDAS token" specification. The physical identity card containing the eMRTD can always be used as physical identity card, if this is allowed.

Attribute and evidence collection and validation threats	Coverage by ETSI TS 119 461 (the present document)
[T_QUALITY_ALTERATION] Artificial image or video quality alteration. When data collection is performed remotely, transmitted identity document image or video is altered in such a way as to degrade its quality to the point of making it difficult or even impossible to detect a forged or counterfeit document or to identify with confidence the applicant. This can be exploited by acting on the quality of the transmission, for example by artificially limiting the bandwidth, or by acting on the capture conditions, for example by reducing lighting. This is usually exploited in combination with one or more of the following to increase the likelihood of success.	Clause 8.3.3 poses requirement for quality of the video stream and any images captured when a physical identity document is used remotely.
[T_DOC_IMAGE] Image presented instead of genuine document. The attacker may attempt to mislead the system by using photos instead of legitimate document. This type of attack is particularly common on fully automatic systems that require a picture of the identity document. For example, the attacker will present a photo of a forged identity document. For this type of attack, a screen is usually placed in front of the camera in the place of the applicant.	Photo of identity document is not accepted. Video is required.
T_DOC_VIDEO] Video presented instead of genuine document. The attacker may attempt to mislead the system by using a video instead of legitimate document. This type of attack is particularly common on fully automatic systems that require a dynamic capture of the id document. For example, the attacker will present a video of a forged identity document including simulated OVD (Optically Variable Device are security features which show different information depending on the viewing angle and/or lightning conditions such as holograms, iridescent ink, etc.). For this type of attack, a screen is usually placed in front of the camera in the place of the applicant.	VAL-8.3.3-02 requires that a real document is presented in front of the camera. Fully automated process is not allowed for remote identity proofing with physical identity documents; hybrid using combination of automated and manual validation is preferred, while a manual process is accepted. Measures for biometric presentation attack and injection attack prevention and detection as specified in clause 8.4.2 of the present document can be used to protect against also presentation and injection attacks for remote use of physical identity documents.
[T_DOC_AI] AI generated video presented instead of genuine document. The attacker may attempt to mislead the system by altering the signal using a video manipulating technology in order to make it look like a genuine document. For instance, an AI-based software can generate data corresponding to an original identity document (for instance by including all artifacts produced by OVDs). This attack can be prepared in advance when the scenario is predictable or generated on the fly. It can use a screen or projector placed in front of the camera or directly replace the video stream generated by the camera. The possibilities of applying AI in the field of presentation attacks are significant and rapidly evolving.	The video capture process is required to ensure that a real document is presented in front of the camera. Security elements of the document are required to be checked. Fully automated process is not allowed for remote identity proofing with physical identity documents; hybrid automated manual (preferred) or manual are required. Use of a deep fake video requires that the video is presented or injected into the identity proofing process. Measures for biometric presentation attack and injection attack prevention and detection as specified in clause 8.4.2 of the present document can be used to protect against also presentation and injection attacks for remote use of physical identity documents.
T_DATA_INJECTION] Data injection. When a data capture system is set up, the possibility for the attacker to inject data directly by bypassing the capture system makes it possible to avoid the validation treatments that could be carried out on the applicant's equipment and to industrialise replay or AI-based presentation attacks.	VAL-8.3.2-04X and VAL-8.3.3-02X cover protection against this type of attack for identity documents. Clause 8.4.2 poses requirements for protection against injection attacks for capture of face image of applicant.
[T_DATA_ALTERATION] Data alteration before it is sent to the system. It may allow an attacker to modify the captured data. This vulnerability is particularly severe when part of the validation operations is carried out on the applicant's equipment.	VAL-8.3.2-02 covers this threat for digital identity document, VAL-8.3.3-04X for physical identity document. Clause 8.4.2 poses requirements for capture of face image of applicant.

Attribute and evidence collection and validation threats	Coverage by ETSI TS 119 461 (the present document)
[T_REPLAY] Interception and replay of captured data. This can allow an attacker to carry out a replay attack. A loophole allows the attacker to capture data collected when verifying the identity of a legitimate applicant. Possibly through a Man In The Middle. The replay attack consists of using the captured data by presenting it again to the system, thus impersonating the legitimate applicant.	VAL-8.3.2-04X and VAL-8.3.3-02X cover protection against this type of attack for identity documents. Clause 8.4.2 covers this for capture of face image of the applicant.

The following threats are described for the binding to applicant task.

NOTE: For the social engineering, bribery, and insider threats, dual control (two persons) could be considered. This is not normal practice, and the present document does not include requirements for dual control.

Table B.3: Example threats to the binding to applicant task of identity proofing

Binding to applicant threats	Coverage by ETSI TS 119 461 (the present document)
[T_FACE_IMAGE] Image presented instead of applicant's face. The attacker may attempt to mislead the system by using photos instead of the genuine face of the legitimate applicant. This type of attack is particularly common on fully automatic systems that require a picture of the applicant for binding with the presented identity document. For example, the attacker will present a photo of the legitimate applicant. For this type of attack, a screen or a printed photo can be placed in front of the camera in the place of the applicant's face. Several photos can be used to mislead systems that require some actions to be performed by the applicant (such as smile, close an eye, etc.).	Requirements in clause 8.4.2 require presentation attack detection measures to protect against this threat.
[T_FACE_VIDEO] Video presented instead of applicant's face. The attacker may attempt to mislead the system by using a video instead of genuine face of the legitimate applicant. This type of attack is particularly common on fully automatic systems that require a dynamic capture of the applicant's face for binding with the presented id document. For example, the attacker will present an edited video of the legitimate applicant performing the actions sequence requested by the system. For this type of attack, a screen is usually placed in front of the camera in the place of the applicant.	Requirements in clause 8.4.2 require presentation attack detection measures to protect against this threat.
[T_FACE_MASK] Mask. The attacker uses a mask usually to impersonate a person whose identity has been provided with a stolen identity document [T_DOC_STOLEN]. There is a wide variety of techniques easily available to produce a mask to match a person, ranging from a simple cut-out photo to a more realistic latex or silicone mask.	Requirements in clause 8.4.2 require presentation attack detection measures to protect against this threat. This also protects against an attack using makeup and not mask.
[T_FACE_AI] AI generated video presented instead of applicant's face. An AI-based software can generate in real time a video of the legitimate applicant mimicking the behaviour of the attacker. This attack can be prepared in advance when the scenario is predictable or generated on the fly. It can use a screen or projector placed in front of the camera or directly replace the video stream generated by the camera. The possibilities of applying AI in the field of presentation attacks are significant and rapidly evolving.	Requirements for presentation and injection attack prevention and detection are posed in clause 8.4.2 to protect against this threat. In addition, BIN-8.4.2-03X requires measures to detect deep fake attacks.

Binding to applicant threats	Coverage by ETSI TS 119 461 (the present document)
[T_FACE_HUMAN_CAPABILITIES] Lack of operator's abilities to identify a person. If an operator is involved in the binding and verification step, he may not have the capabilities or competence to perform this task satisfactorily. For example, he may not have the ability to reliably identify a person from another ethnic group. This situation may be exploited by an attacker.	Requirements are posed in clause 8.4.4 on how to do binding to applicant by manual face verification; this can be seen as an important addition by the present document. Clause 8.4.4 also poses requirements on training of the registration officer.
[T_FACE_LOOKALIKE] Similar looking person. Solutions using biometrics to perform the binding step are vulnerable when people with strong similarities to the legitimate applicant attempt to mislead the system. This is the case, for example, with twins or even members of the same family when the identity documents used as a reference are a little old.	Clause 8.4.3 poses requirement on the FAR when biometrics are used. For manual binding to applicant, the requirements in clause 8.4.4 are intended to protect against erroneous binding to applicant as far as reasonably possible.
[T_FACE_OLD_REFERENCE] Old identity document. Even if it is not a good practice, identity documents can be valid during a long period (up to 15 years in France at the time this report is written for example). As a result, the time lapse between the date on which the photo on the identity document is taken and the date on which the verification is carried out may be significant and the appearance of the applicant may have changed significantly, especially for young people.	COL-8.2.1-07 allows the identity proofing context to pose freshness requirements on identity information, which includes pictures and the evidence as such. With face biometrics, clause 8.4.3 poses requirements for FAR and FRR. With an old reference photo, both false rejection and false acceptance can be more likely, but the FAR requirement still applies. For manual face verification, clause 8.4.4 has requirements and an important measure is that the registration officer can rely on procedures where "no" is a justified answer, see requirements for all manual and hybrid use cases in clause 9.2.
[T_FACE_POOR_QUALITY_REFERENCE] Poor quality photo on the identity document. Photographs on identity documents can be small, of poor quality, sometimes in shades of grey. This can be exploited for a "lookalike" attack.	The requirements cited for T_FACE_OLD_REFERENCE above, except the freshness requirement, apply in this case as well. This is one reason why an automated, biometric procedure using physical identity documents cannot be expected to yield sufficiently reliable results.
[T_FACE_SOFTWARE_PERFORMANCE] Performance of facial recognition software not at the expected level. When facial recognition is done or assisted by software, possible lack of performance of the software is a vulnerability. Indeed, the context (reference photo from an identity document and possibly a relatively old one) may lead to favouring the FRR (False Rejection Rate, i.e. the proportion of people who should have been accepted but were unduly rejected) rather than the FAR (False Acceptance Rate, i.e. the rate of people who should have been rejected but who nevertheless broke into the system).	Clause 8.4.3 poses requirements for FAR and FRR for biometrics, that the stated goals for these parameters are fulfilled, and that means are required to be systematically tested against reference datasets and kept updated to cope with changes in the threats and risk situation.
[T_DATA_INCONSISTENCY_INACCURACY] Inconsistency or inaccuracy of reference data. When reference data is used to validate or verify an identity, it is possible in some configurations to find cases of inconsistent or incomplete reference data, for example, differences in transliteration, homonyms, etc. For instance, during the remote identity proofing for a legal person, identification of a legal representative is key and it may occur that the person being the legal representative is not uniquely defined by the registered identity attributes thus allowing legal person impersonation by anyone sharing the common set of registered identity attributes. The management policy (automatic or manual) of these cases can constitute a loophole that can be exploited by an attacker.	Requirements in clause 8.3.1 demand clear procedures to resolve conflicts between name representation from different sources/evidence: Encoding (character representation, transcription, lack of diacritics), differences in representation of names (initials versus full name, missing middle names change of name not reflected in evidence, truncation etc.). When supplementary evidence is used, VAL-8.3.6-06, VAL-8.3.7-05, and VAL-8.3.8-05 requires that the procedure to apply in case of discrepancies in attributes obtained from the supplementary evidence and from other evidence is defined; meaning which evidence is authoritative regarding the attribute values.

Binding to applicant threats	Coverage by ETSI TS 119 461 (the present document)
[T_SOCIAL ENGINEERING] Social engineering. If an operator is involved in the data validation or verification phase and interaction with the applicant is part of the process, it is possible for an attacker to convince the operator to improperly validate an identity verification operation, for instance by appealing to his sensitivity.	Requirements for thorough procedures that are required to be followed, as posed for all manual and hybrid use cases in clause 9.2. Additionally, the training requirements cited earlier for registration officers contribute to counter this threat.
[T_BRIBERY] Bribery of an operator. If an operator is involved in the data validation or verification phase and interaction with the applicant is part of the process, it is possible for an attacker to convince the operator to improperly validate an identity verification operation by bribing him.	ETSI EN 319 401 [1] has requirements for screening of personnel. If several registration officers are available, VAL-8.3.3-13 requires tasks to be allocated randomly between them.
[T_INSIDER] Insider. If an operator is involved in the data validation or verification phase and interaction with the applicant is part of the process, it is possible for an attacker to have the remote identity proofing service provider hire a malicious operator who will validate identities that should normally have been rejected.	ETSI EN 319 401 [1] has requirements for screening of personnel. If several registration officers are available, VAL-8.3.3-13 requires tasks to be allocated randomly between them.
[T_REVOKED_CERTIFICATE] Revoked certificate. Use of revoked certificate as a proof of identity without checking its status.	For all cases where certificates are used, requirements are posed to check their validity, which includes revocation checking. This applies when digital signature means are used (clause 8.3.5) as well as for use of digitally signed material with other evidence (e.g. signed eMRTD digital document, signed documents and attestations).
[T_EMRTD_WEAK_IMPLEMENTATION] eMRTD weak implementation. Security of eMRTD relies on the country or organization certificate. There is no complete official master list of these certificates. Using an unsecure list of certificates or not using that security make the system vulnerable to forged eMRTD. A poor implementation of security mechanisms ensuring data integrity and chip presence makes the solution vulnerable to various attacks such as Man in the middle, eMRTD cloning, etc.	COL-8.2.3-03 requires that for each identity proofing context supported, a list of the documents accepted is required to be identified by the identity proofing practice statement, and VAL-8.3.2-02 requires that a digital identity document is accepted only if the issuer's digital signature is successfully validated.
[T_BLACKBOX] Blackbox. eID, IdP, or any other digital proof of identity related threats should be handled as a blackbox threat. Any vulnerability on these systems may lead to a vulnerability on the remote identity proofing system.	Quality requirements are posed on digital identity document, eID, digital signature and supplementary evidence. No evidence can be used unless its quality is assessed. The identity proofing context can decide for example that an eID alone is not sufficient, due to the risk that an attacker controls the victims eID or the risk of a social engineering attack, supplementary evidence can be required.

The following general threats that are not specific to any task of the identity proofing process, are described.

Table B.4: Example general threats to identity proofing

General threats	Coverage by ETSI TS 119 461 (the present document)
[T_CONSTRAINT] Applicant under constraint. During remote identity proofing, the applicant may be threatened and perform this operation under constraint. This vulnerability, which also exists in face-to-face interviews, is made easier to exploit in the context of a remote verification.	The requirements in clause 8.4.2 on video provides better protection against this type of attack than use of merely photo.
[T_PROCESS_FLAW] Process flaw. Generally speaking, any flaw/inaccuracy in the remote identity verification process can constitute a loophole that can be exploited by an attacker.	The present document does not pose requirements on processes but describes use cases in clause 9 and Annex C that are recommended, and strict requirements in clause 8 for the tasks of an identity proofing process. Processes are recommended to be audited and approved/supervised when identity proofing is done for a (qualified) trust service.
[T_DELEGATION] Delegated operator. Delegation of responsibilities could weaken the process. If the remote identity proofing is delegated to another organization (e.g. a bank asking an identity provider to do so, or a parent company with respect to a more specialized subsidiary), it is possible that some ambiguity in this outsourcing arises as soon as organizational boundaries are crossed. This could loosen the security of the entire process.	If identity proofing is outsourced from a TSP to a specialized IPSP, the IPSP is required to adhere to the requirements of the present document and be audited accordingly. A TSP is clearly responsible for identity proofing for its services and is required to manage subcontracting accordingly. The identity proofing context is required to be identified, and its requirements obeyed.

Annex C (normative): Use cases for identity proofing for EU qualified trust services

C.1 Introduction

This annex specifies requirements for identity proofing targeted explicitly to fulfil requirements of the original eIDAS regulation [i.1] and the amended eIDAS regulation [i.25]. Requirements for identity proofing are posed in Article 24.1 of the original eIDAS regulation [i.1] for issuing of qualified certificates, in Article 24.1, 24.1a, and 24.1b of the amended eIDAS regulation [i.25] for issuing of qualified certificates and qualified electronic attestation of attributes, and in Article 44 (same requirements for both the original [i.1] and the amended [i.25] eIDAS regulation) for identification of senders and addressees of Qualified Electronic Registered Delivery Services (QERDS). For other qualified trust services, neither the original nor the amended eIDAS regulation [i.25] pose specific requirements for identity proofing.

Article 24.1 of the original eIDAS regulation [i.1] is superseded by Article 24.1, 24.1a, and 24.1b of the amended eIDAS regulation [i.25] but the amended eIDAS regulation [i.25] Article 51.2b specifies a transitional measure where a qualified trust service provider that is granted the qualified status before entry into force of the amended eIDAS regulation [i.25] is allowed to continue to rely on the methods set out in Article 24.1 of the original eIDAS regulation [i.1] until 24 months after the entry into force of the amended eIDAS regulation [i.25]. Hence, the present document includes use cases to fulfil the requirements of Article 24.1 of the original eIDAS regulation [i.1] in clause C.2.

Regarding qualified electronic attestation of attributes, Annex VI of the amended eIDAS regulation [i.25] specifies a minimum list of attributes for which EU Member States are required to provide means for verification against authentic sources. Many of these attributes cannot be expected to be provided by authoritative evidence as defined by the present document, meaning supplementary evidence is required for these attributes. The amended eIDAS regulation [i.25] however has no requirement for a qualified electronic attestation of attributes to be based (solely) on authentic sources; other supplementary evidence can be used. Qualified electronic attestations of attributes can include other attributes than those defined by Annex VI of the amended eIDAS regulation [i.25].

C.2 Use cases for issuing of qualified certificate according to Article 24.1 of the original eIDAS regulation

C.2.1 Use case for identity proofing by physical presence of the applicant

[CONDITIONAL] If identity proofing is done for the purpose of issuing qualified certificate according to Article 24.1 of the original eIDAS regulation [i.1], and identity proofing is done by physical presence according to letter a of this Article, the following requirements apply.

QTS-C.2.1-01: The requirements of clause 9.2.1.1 of the present document shall apply.

QTS-C.2.1-02: The requirements of either clause 9.2.1.2 or clause 9.2.1.3 or clause 9.2.1.4 of the present document shall apply.

C.2.2 Use case for identity proofing by authentication using eID means

[CONDITIONAL] If identity proofing is done for the purpose of issuing qualified certificate according to Article 24.1 of the original eIDAS regulation [i.1], and identity proofing is done by authentication using eID means according to letter b of this Article, the following requirements apply.

QTS-C.2.2-01: The requirements for Baseline LoIP of clause 9.2.4 of the present document shall apply.

QTS-C.2.2-02: The eID means shall be eIDAS substantial eID or eIDAS high eID.

QTS-C.2.2-03: The eID means shall have been issued based on physical presence of the natural person or an authorized representative of the legal person.

C.2.3 Use case for identity proofing by certificate of qualified electronic signature or qualified electronic seal

[CONDITIONAL] If identity proofing is done for the purpose of issuing qualified certificate according to Article 24.1 of the original eIDAS regulation [i.1], and identity proofing is done by the certificate of a qualified electronic signature or qualified electronic seal according to letter c of this Article, the following requirements apply.

QTS-C.2.3-01: The requirements of clause 9.2.5 of the present document shall apply.

[CONDITIONAL] QTS-C.2.3-02: If the applicant is a natural person or a natural person representing a legal person, the digital signature shall be a qualified electronic signature.

[CONDITIONAL] QTS-C.2.3-03: If the applicant is a legal person, the digital signature shall be a qualified electronic seal or a qualified electronic signature.

QTS-C.2.3-04: The qualified certificate shall have been issued based on identity proofing either by a prior physical presence of the natural person or of an authorized representative of the legal person, or by an eIDAS substantial eID or an eIDAS high eID that is in turn based on identity proofing by the physical presence of the natural person or an authorized representative of the legal person.

QTS-C.2.3-05: The signature shall be validated by eIDAS signature validation.

NOTE: Conformant to eIDAS Article 32, which has identical text in both the original and the amended eIDAS regulation [i.25].

QTS-C.2.3-06: The signature should be validated according to ETSI TS 119 172-4 [7].

C.2.4 Use case for identity proofing by other identification means

[CONDITIONAL] If identity proofing is done for the purpose of issuing qualified certificate according to Article 24.1 of the original eIDAS regulation [i.1], and identity proofing is done by other identification means according to letter d of this Article, the following requirements apply.

NOTE: Baseline LoIP is considered sufficient for identity proofing under the requirements of the original eIDAS regulation [i.1].

[CONDITIONAL] QTS-C.2.4-01: If attended remote identity proofing using physical or digital identity document as authoritative evidence is used, the requirements of clause 9.2.2.1 of the present document shall apply.

[CONDITIONAL] QTS-C.2.4-02: If attended remote identity proofing using physical or digital identity document as authoritative evidence is used, the requirements of either clause 9.2.2.2 or 9.2.2.3 of the present document shall apply.

[CONDITIONAL] QTS-C.2.4-03: If unattended remote identity proofing using physical or digital identity document as authoritative evidence is used, the requirements of clause 9.2.3.1 of the present document shall apply.

[CONDITIONAL] QTS-C.2.4-04: If unattended remote identity proofing using physical or digital identity document as authoritative evidence is used, the requirements of either clause 9.2.3.2 or 9.2.3.3 or 9.2.3.4 of the present document shall apply.

QTS-C.2.4-05: The identity proofing method shall be recognized at national level by the EU Member State in which the qualified trust service provider is registered.

QTS-C.2.4-06: The identity proofing method shall in terms of reliability provide equivalent assurance of the identity proofing to physical presence as determined at national level by the EU Member State in which the qualified trust service provider is registered.

QTS-C.2.4-07: The fulfilment of requirement **QTS-C.2.4-06** shall be confirmed by a conformity assessment body.

C.2.5 Use case for identity proofing of legal person

[CONDITIONAL] If identity proofing is done for the purpose of issuing qualified certificate according to Article 24.1 of the original eIDAS regulation [i.1], and identity proofing is of a legal person, the following requirements apply.

QTS-C.2.5-01: The requirements of clause 9.3 of the present document shall apply.

[CONDITIONAL] QTS-C.2.5-02: Where applicable, the legal person registration number as stated in the appropriate official, trusted register shall be collected and validated.

NOTE: According to Annex III of the original eIDAS regulation [i.1]. Some legal persons, e.g. public sector bodies in some EU Member States, can be exempted from registration in official registers.

C.2.6 Use case for identity proofing of natural person representing legal person

[CONDITIONAL] If identity proofing is done for the purpose of issuing qualified certificate according to Article 24.1 of the original eIDAS regulation [i.1], and identity proofing is of a natural person representing a legal person, the following requirements apply**.**

QTS-C.2.6-01: The requirements of clause 9.4 of the present document for Baseline LoIP or Extended LoIP shall apply.

QTS-C.2.6-02: The identity of the natural person shall be proven according to the requirements of clause C.2.1, or C.2.2, or C.2.3, or C.2.4 of the present document.

[CONDITIONAL] QTS-C.2.6-03: Where applicable, the legal person registration number as stated in the appropriate official, trusted register shall be collected and validated.

NOTE: According to Annex III of the original eIDAS regulation [i.1]. Some legal persons, e.g. public sector bodies in some EU Member States, can be exempted from registration in official registers.

C.3 Use cases for issuing of qualified certificate or qualified electronic attestation of attributes according to Article 24.1, 24.1a, and 24.1b of the amended eIDAS regulation

C.3.1 Use case for identity proofing by physical presence of the applicant

[CONDITIONAL] If identity proofing is done for the purpose of issuing qualified certificate or qualified electronic attestation of attributes according to Article 24.1, 24.1a, or 24.1b of the amended eIDAS regulation [i.25], and identity proofing is done by physical presence according to letter d of Article 24.1a and/or letter e of Article 24.1b, the following requirements apply.

QTS-C.3.1-01: The requirements for Extended LoIP of clause 9.2.1.1 of the present document shall apply.

QTS-C.3.1-02: The requirements for Extended LoIP of either clause 9.2.1.2 or 9.2.1.3 or 9.2.1.4 of the present document shall apply.

QTS-C.3.1-03: The procedure for physical presence shall be in accordance with national law in the EU Member State where the qualified trust service provider is registered.

QTS-C.3.1-04: Identity proofing for any further attributes additional to the unique identity of the person shall be either according to the requirements of one of the clauses C.3.1, C.3.2, C.3.3, or C.3.4 of the present document, or by means of qualified electronic attestation of attributes, or by means of supplementary evidence that according to the identity proofing context is regarded as authoritative evidence according to the requirements of clauses 8.2.6 and 8.3.6 (trusted register), and/or clauses 8.2.7 and 8.3.7 (proof of access), and/or clauses 8.2.8 and 8.3.8 (documents and attestations) of the present document.

NOTE: This requirement answers Article 24.1b of the amended eIDAS regulation [i.25] when identity proofing of the applicant's unique identity is by physical presence according to clause C.3.1 of the present document.

C.3.2 Use case for identity proofing by authentication using eID means

[CONDITIONAL] If identity proofing is done for the purpose of issuing qualified certificate or qualified electronic attestation of attributes according to Article 24.1, 24.1a, or 24.1b of the amended eIDAS regulation [i.25], and identity proofing is done by authentication using eID means according to letter a of Article 24.1a and/or letter a of Article 24.1b, the following requirements apply.

QTS-C.3.2-01: The requirements for Extended LoIP of clause 9.2.4 of the present document shall apply.

QTS-C.3.2-02: The eID means shall conform to eIDAS high eID.

QTS-C.3.2-03: The eID means shall be eIDAS notified eID.

NOTE 1: All European Digital Identity Wallets will fulfil requirements QTS-C.3.2-02 and C.3.2-03.

QTS-C.3.2-04: Identity proofing for any further attributes additional to the unique identity of the person shall be either according to the requirements of one of the clauses C.3.1, C.3.2, C.3.3, or C.3.4 of the present document, or by means of qualified electronic attestation of attributes, or by means of supplementary evidence that according to the identity proofing context is regarded as authoritative evidence according to the requirements of clauses 8.2.6 and 8.3.6 (trusted register), and/or clauses 8.2.7 and 8.3.7 (proof of access), and/or clauses 8.2.8 and 8.3.8 (documents and attestations) of the present document.

NOTE 2: This requirement answers Article 24.1b of the amended eIDAS regulation [i.25] when identity proofing of the applicant's unique identity is by authentication using eID means according to clause C.3.2 of the present document.

C.3.3 Use case for identity proofing by certificate of qualified electronic signature or qualified electronic seal

[CONDITIONAL] If identity proofing is done for the purpose of issuing qualified certificate or qualified electronic attestation of attributes according to Article 24.1, 24.1a, or 24.1b of the amended eIDAS regulation [i.25], and identity proofing is done by the certificate of a qualified electronic signature or qualified electronic seal according to letter b of Article 24.1a and/or letter b of Article 24.1b, the following requirements apply.

QTS-C.3.3-01: The requirements for Extended LoIP of clause 9.2.5 of the present document shall apply.

[CONDITIONAL] QTS-C.3.3-02: If the applicant is a natural person or a natural person representing a legal person, the digital signature shall be a qualified electronic signature.

[CONDITIONAL] QTS-C.3.3-03: If the applicant is a legal person, the digital signature shall be a qualified electronic seal or a qualified electronic signature.

QTS-C.3.3-04: The qualified certificate used for the identity proofing shall have been issued based on identity proofing by one of the following alternatives

a) physical presence according to clause C.3.1 or C.2.1 of the present document;

b) eID means according to clause C.3.2 of the present document;

c) eID means according to clause C.2.2 of the present document when the eID is both an eIDAS high eID and an eIDAS notified eID;

d) Other identification means according to clause C.3.4 of the present document.

NOTE 1: This excludes use of qualified certificates issued under the original eIDAS regulation [i.1], except when these certificates are issued based on physical presence, where the requirements are at same level as in the amended eIDAS regulation [i.25], or are issued based on an eID that fulfils the requirements set by both the original eIDAS regulation [i.1] and the amended eIDAS regulation [i.25].

NOTE 2: Specification of a certificate extension to mediate the identity proofing method used to issue a certificate is ongoing in ETSI TC ESI.

QTS-C.3.3-05: Identity proofing for any further attributes additional to the unique identity of the person shall be either according to the requirements of one of the clauses C.3.1, C.3.2, C.3.3, or C.3.4 of the present document, or by means of qualified electronic attestation of attributes, or by means of supplementary evidence that according to the identity proofing context is regarded as authoritative evidence according to the requirements of clauses 8.2.6 and 8.3.6 (trusted register), and/or clauses 8.2.7 and 8.3.7 (proof of access), and/or clauses 8.2.8 and 8.3.8 (documents and attestations) of the present document.

NOTE 3: This requirement answers Article 24.1b of the amended eIDAS regulation [i.25] when identity proofing of the applicant's unique identity is by certificate of qualified electronic signature or qualified electronic seal according to clause C.3.3 of the present document.

QTS-C.3.3-06: The signature shall be validated according to eIDAS signature validation.

NOTE 4: Conformant to eIDAS Article 32, which has identical text in both the original and the amended eIDAS regulation [i.25].

QTS-C.3.3-07: The signature should be validated according to ETSI TS 119 172-4 [7].

C.3.4 Use case for identity proofing by other identification means

[CONDITIONAL] If identity proofing is done for the purpose of issuing qualified certificate or qualified electronic attestation of attributes according to Article 24.1, 24.1a, or 24.1b of the amended eIDAS regulation [i.25], and identity proofing is done by other identification means according to letter c of Article 24.1a and/or letter d of Article 24.1b, the following requirements apply.

[CONDITIONAL] QTS-C.3.4-01: If attended remote identity proofing using physical or digital identity document as authoritative evidence is used, the requirements for Extended LoIP of clause 9.2.2.1 of the present document shall apply.

[CONDITIONAL] QTS-C.3.4-02: If attended remote identity proofing using physical or digital identity document as authoritative evidence is used, the requirements for Extended LoIP of clause 9.2.2.3 of the present document shall apply.

NOTE 1: Manual operation as described in clause 9.2.2.2 is not considered to support Extended LoIP and hence not issuing of qualified certificates or qualified electronic attestations of attributes according to the amended eIDAS regulation [i.25].

[CONDITIONAL] QTS-C.3.4-03: If unattended remote identity proofing using physical or digital identity document as authoritative evidence is used, the requirements for Extended LoIP of clause 9.2.3.1 of the present document shall apply.

[CONDITIONAL] QTS-C.3.4-04: If unattended remote identity proofing using physical or digital identity document as authoritative evidence is used, the requirements for Extended LoIP of either clause 9.2.3.3 or clause 9.2.3.4 of the present document shall apply.

NOTE 2: Manual operation as described in clause 9.2.3.2 is not considered to support Extended LoIP and hence not issuing of qualified certificates or qualified electronic attestations of attributes according to the amended eIDAS regulation [i.25].

[CONDITIONAL] QTS-C.3.4-05: If identity proofing is done by enhancing an identity proofing for Baseline LoIP using eID as authoritative evidence, the requirements of clause 9.5 of the present document shall apply.

[CONDITIONAL] QTS-C.3.4-06: If identity proofing is done by enhancing an identity proofing for Baseline LoIP using eID as authoritative evidence, the eID used as authoritative evidence shall be an eIDAS substantial eID or eIDAS high eID and either:

a) be an eIDAS notified eID; or

b) be an eIDAS certified eID; or

c) have been assessed by an independent conformity assessment body to fulfil the requirements for an eIDAS substantial eID or eIDAS high eID.

NOTE 3: Notified according to Article 9 of the amended eIDAS regulation [i.25], or certified according to Article 12a of the amended eIDAS regulation [i.25], or assessed by independent conformity assessment.

QTS-C.3.4-07: Identity proofing for any further attributes additional to the unique identity of the person shall be either according to the requirements of one of the clauses C.3.1, C.3.2, C.3.3, or C.3.4 of the present document, or by means of qualified electronic attestation of attributes, or by means of supplementary evidence that according to the identity proofing context is regarded as authoritative evidence according to the requirements of clauses 8.2.6 and 8.3.6 (trusted register), and/or clauses 8.2.7 and 8.3.7 (proof of access), and/or clauses 8.2.8 and 8.3.8 (documents and attestations) of the present document.

NOTE 4: This requirement answers Article 24.1b of the amended eIDAS regulation [i.25] when identity proofing of the applicant's unique identity is by other identification means according to clause C.3.4 of the present document.

QTS-C.3.4-08: The conformity of the identity proofing method with the requirements of this clause C.3.4 of the present document shall be confirmed by a conformity assessment body.

NOTE 5: The requirement of letter c of Article 24.1a of the amended eIDAS regulation [i.25] is for the conformity assessment to confirm that the identification method ensures the identification of a natural person with a high level of confidence. The use cases referred by requirements QTS-C.3.4-01 to QTS-C.3.4-05 are all presumed to provide identity proofing with a high level of confidence. The requirement of letter d of Article 24.1b of the amended eIDAS regulation [i.25] is for the conformity assessment to confirm that the verification of attributes is done with a high level of confidence. Requirement QTS-C.3.4-07 is intended to ensure such high level of confidence.

C.3.5 Use case for identity proofing of legal person

[CONDITIONAL] If identity proofing is done for the purpose of issuing qualified certificate or qualified electronic attestation of attributes according to Article 24.1, 24.1a, or 24.1b of the amended eIDAS regulation [i.25], and identity proofing is of a legal person, the following requirements apply.

QTS-C.3.5-01: Identity proofing for the unique identity of the legal person shall be according to the requirements for Extended LoIP of clause 9.3 of the present document.

QTS-C.3.5-02: Identity proofing for any further attributes additional to the unique identity of the legal person shall be either according to the requirements for Extended LoIP of clause 9.3 of the present document or by means of qualified electronic attestation of attributes.

NOTE 1: Clause 9.3 of the present document covers use of all of the means authentication by eID, certificate of digital signature or seal, trusted register, proof of access, and documents and attestations for identity proofing of further attributes of a legal person.

[CONDITIONAL] QTS-C.3.5-03: Where applicable, the legal person registration number as stated in the appropriate official, trusted register shall be collected and validated.

NOTE 2: According to Annex III of the amended eIDAS regulation [i.25]. Some legal persons, e.g. public sector bodies in some EU Member States, can be exempted from registration in official registers.

C.3.6 Use case for identity proofing of natural person representing legal person

[CONDITIONAL] If identity proofing is done for the purpose of issuing qualified certificate or qualified electronic attestation of attributes according to Article 24.1, 24.1a, or 24.1b of the amended eIDAS regulation [i.25], and identity proofing is of a natural person representing a legal person, the following requirements apply.

QTS-C.3.6-01: The requirements for Extended LoIP of clause 9.4 of the present document shall apply.

QTS-C.3.6-02: The identity of the natural person shall be proven according to the requirements of clause C.3.1, or C.3.2, or C.3.3, or C.3.4 of the present document.

QTS-C.3.6-03: Identity proofing for any further attributes additional to the unique identity of the legal person and/or the natural person shall be either according to the requirements for Extended LoIP of clause 9.4 of the present document or by means of qualified electronic attestation of attributes.

NOTE 1: Clause 9.4 of the present document covers use of trusted register, proof of access, and documents and attestations for identity proofing of further attributes of a natural person, legal person, and the relationship between the natural and the legal person.

[CONDITIONAL] QTS-C.3.6-04: Where applicable, the legal person registration number as stated in the appropriate official, trusted register shall be collected and validated.

NOTE 2: According to Annex III of the amended eIDAS regulation [i.25]. Some legal persons, e.g. public sector bodies in some EU Member States, can be exempted from registration in official registers.

C.4 Use case for qualified electronic registered delivery services according to Article 44 of the amended eIDAS regulation

NOTE: Requirements for identification of senders and addressees of Qualified Electronic Registered Delivery Services (QERDS) are not changed from the original to the amended eIDAS regulation [i.25]. In line with current practice for deployed QERDSs, the requirement for identity proofing is set to Baseline LoIP according to clause C.2 of the present document. Preamble (52) to the amended eIDAS regulation [i.25] can be read as requiring a higher level of identity proofing. This is reflected in conditional requirements for Extended LoIP where authenticity and/or confidentiality of the information delivered is critical.

QTS-C.4-01: Identity proofing for senders and addressees of a QERDS shall at a minimum be done by application of the relevant use case from clause C.2 of the present document.

[CONDITIONAL] QTS-C.4-02: If the QERDS supports deliveries where the authenticity of the information is critical, identity proofing for the relevant senders of the QERDS should be done by application of the relevant use case from clause C.3 of the present document.

[CONDITIONAL] QTS-C.4-03: If the QERDS supports deliveries where the confidentiality of the information is critical, identity proofing for the relevant addressees of the QERDS should be done by application of the relevant use case from clause C.3 of the present document.

Annex D (informative): Mapping to applicable requirements of the amended eIDAS regulation

Identity proofing is not in itself a trust service, but a trust service component. Table D.1 below covers the requirements from the amended eIDAS regulation [i.25] that explicitly apply to identity proofing. When a QTSP subcontracts an IPSP for identity proofing, the IPSP will need to fulfil certain eIDAS requirements especially regarding risk management and security. These aspects are not covered in the table below because fulfilment of eIDAS requirements will be part of the contract between the QTSP and the IPSP and responsibilities can be divided between them in different ways. The present document aids in fulfilment of relevant eIDAS requirements by requiring an IPSP to handle service management and operations according to the relevant requirements from ETSI EN 319 401 [1] and to manage risks related to identity proofing in accordance with ETSI EN 319 401 [1] and clause 5 of the present document.

The amended eIDAS regulation [i.25] Article 51.2b specifies a transitional measure where a QTSP that is granted the qualified status before entry into force of the amended eIDAS regulation [i.25] is allowed to continue to rely on the methods set out in Article 24.1 of the original eIDAS regulation [i.1] until 24 months after the entry into force of the amended eIDAS regulation [i.25]. The table below only considers the requirements of the amended eIDAS regulation [i.25].

Table D.1: Mapping of eIDAS requirements to requirements of the present document

Regulation Article 5 Pseudonyms in electronic transaction	**ETSI TS 119 461**
(1) Without prejudice to specific rules of Union or national law requiring users to identify themselves or to the legal effect given to pseudonyms under national law, the use of pseudonyms that are chosen by the user shall not be prohibited.	COL-8.2.2.1-02A and note.
Regulation Article 15 Accessibility for persons with disabilities and special needs	**ETSI TS 119 461**
The provision of electronic identification means, trust services and end-user products that are used in the provision of those services shall be made available in plain and intelligible language, in accordance with the United Nations Convention on the Rights of Persons with Disabilities and with the accessibility requirements of Directive (EU) 2019/882, thus also benefiting persons who experience functional limitations, such as elderly people, and persons with limited access to digital technologies.	INI-8.1-04 and note.

Regulation Article 24 Requirements for qualified trust service providers	ETSI TS 119 461 reference
(1) When issuing a qualified certificate or a qualified electronic attestation of attributes, a qualified trust service provider shall verify the identity and, if applicable, any specific attributes of the natural or legal person to whom the qualified certificate or the qualified electronic attestation of attributes is to be issued.	Clause C.3.
(1a) The verification of the identity referred to in paragraph 1 shall be performed, by appropriate means, by the qualified trust service provider, either directly or by means of a third party, on the basis of one of the following methods or, when needed, on a combination thereof in accordance with the implementing acts referred to in paragraph 1c:	Regarding combination, QTS-C.3.4-05 and QTS-C.3.4-06 cover use of an eID at LoA 'substantial' plus additional means. Note the possibility to use trusted registers (e.g. authentic sources), attributes and attestations (e.g. (Q)EAA), and proof of access in combination with the methods (a)-(d) below.
(a) by means of the European Digital Identity Wallet or a notified electronic identification means which meets the requirements set out in Article 8 with regard to assurance level high;	Clause C.3.2. In addition, clause C.3.5 for legal person. In addition, clause C.3.6 for natural person representing legal person.
(b) by means of a certificate of a qualified electronic signature or of a qualified electronic seal, issued in compliance with point (a), (c) or (d);	Clause C.3.3. In addition, clause C.3.5 for legal person. In addition, clause C.3.6 for natural person representing legal person.
(c) by using other identification methods which ensure the identification of the person with a high level of confidence, the conformity of which shall be confirmed by a conformity assessment body;	Clause C.3.4. In addition, clause C.3.5 for legal person. In addition, clause C.3.6 for natural person representing legal person.
(d) through the physical presence of the natural person or of an authorised representative of the legal person, by means of appropriate evidence and procedures, in accordance with national law.	Clause C.3.1. In addition, clause C.3.5 for legal person. In addition, clause C.3.6 for natural person representing legal person.
(1b) The verification of the attributes referred to in paragraph 1 shall be performed, by appropriate means, by the qualified trust service provider, either directly or by means of a third party, on the basis of one of the following methods or, where necessary, on a combination thereof, in accordance with the implementing acts referred to in paragraph 1c:	Combinations are implicitly allowed from the requirements below. The requirements cited are for all use cases, where unique identity is proven by one means, additional attributes can be proven by any other applicable means.
(a) by means of the European Digital Identity Wallet or a notified electronic identification means which meets the requirements set out in Article 8 with regard to assurance level high;	QTS-C3.1-04, QTS-C.3.2-04, QTS-C-3-3-05, QTS-C.3.4-07. In addition, QTS-C.3.5-02 for legal person. In addition, QTS-C.3.6-03 for natural person representing legal person.
(b) by means of a certificate of a qualified electronic signature or of a qualified electronic seal, issued in accordance with paragraph 1a, point (a), (c) or (d);	QTS-C3.1-04, QTS-C.3.2-04, QTS-C-3-3-05, QTS-C.3.4-07. In addition, QTS-C.3.5-02 for legal person. In addition, QTS-C.3.6-03 for natural person representing legal person.
(c) by means of a qualified electronic attestation of attributes;	QTS-C3.1-04, QTS-C.3.2-04, QTS-C-3-3-05, QTS-C.3.4-07. In addition, QTS-C.3.5-02 for legal person. In addition, QTS-C.3.6-03 for natural person representing legal person.
(d) by using other methods, which ensure the verification of the attributes with a high level of confidence, the conformity of which shall be confirmed by a conformity assessment body;	QTS-C3.1-04, QTS-C.3.2-04, QTS-C-3-3-05, QTS-C.3.4-07. In addition, QTS-C.3.5-02 for legal person. In addition, QTS-C.3.6-03 for natural person representing legal person.
(e) by means of the physical presence of the natural person or of an authorised representative of the legal person, by means of appropriate evidence and procedures, in accordance with national law.	QTS-C3.1-04, QTS-C.3.2-04, QTS-C-3-3-05, QTS-C.3.4-07. In addition, QTS-C.3.5-02 for legal person. In addition, QTS-C.3.6-03 for natural person representing legal person.
Regulation Article 44 Requirements for qualified electronic registered delivery services	**ETSI TS 119 461**
(1) Qualified electronic registered delivery services shall fulfil the following requirements: *(c) they ensure with a high level of confidence the identification of the sender;* *(d) they ensure the identification of the addressee before delivery of the data;*	Clause C.4

History

Document history		
V1.1.1	July 2021	Publication
V2.1.1	February 2025	Publication