ETSI TS 119 461 V1.1.1 (2021-07)

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

Reference

DTS/ESI-0019461

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

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

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 Web server (https://ipr.etsi.org/).

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™** and **LTE™** 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 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 Regulation (EU) No 910/2014 [i.1].

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

1 Scope

The scope of the present document is 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 present document provides requirements for a Baseline Level of Identity Proofing (LoIP) aimed to support issuing of certificates at the NCP policy level as specified in ETSI EN 319 411-1 [i.7] as well as the QCP policy level as specified in ETSI EN 319 411-2 [i.8]. The Baseline LoIP also aims to support identity proofing for other ETSI trust services standards such as ETSI TS 119 431-1 [i.10] and ETSI EN 319 521 [i.12]. Annex A indicates how to use the present document in conjunction with these standards.

NOTE 1: The present document has the potential to have wider applicability than the defined scope, but any application for other purposes than enrolment to trust services is out of scope.

The present document aims at supporting identity proofing in European and other regulatory frameworks. Specifically, but not exclusively, the present document aims to support issuing of qualified certificates as defined in Regulation (EU) No 910/2014 [i.1] (the eIDAS Regulation) Article 24.1. The present document aims to meet the requirements of Article 24.1 as follows: 24.1 (a) by clause 9.2.1, 24.1 (b) by clause 9.2.4, 24.1 (c) by clause 9.2.5, 24.1 (d) by clauses 9.2.2 and/or 9.2.3 depending on the decision of the competent national authority.

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

NOTE 2: See ETSI EN 319 403-1 [i.6] for guidance on the assessment of TSP processes and services.

2 References

2.1 Normative references

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

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

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

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

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

[2] 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 30107-3:2017: "Information technology -- Biometric presentation attack detection -- Part 3: Testing and reporting".

2.2 Informative references

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

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

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

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

[i.2] Commission 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 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] ETSI TS 119 431-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev".

[i.11] EN 419 241-1: "Trustworthy systems supporting server signing - Part 1: General system security requirements" (produced by CEN).

[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] 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".

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

[i.16] ISO/IEC 30107-1:2016: "Information technology - Biometric presentation attack detection - Part 1: Framework".

[i.17] ISO/IEC 19795-1:2021: "Information technology - Biometric performance testing and reporting - Part 1: Principles and framework".

[i.18] ISO/IEC 19989-3:2020: "Information security - Criteria and methodology for security evaluation of biometric systems - Part 3: Presentation attack detection".

[i.19] ISO/IEC TS 29003:2018: "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 15408-1:2009: "Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model".

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:

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

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

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].

(identity) attribute: quality or characteristic ascribed to a person

baseline LoIP: Level of Identity Proofing (LoIP) reaching a high level of confidence based on the fulfilment of general good practice requirements for the identity proofing process and considered suitable for the trust services policies currently defined by ETSI standards

NOTE: This level aims to protect against typical attacks as described in Annex B of the present document.

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

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

NOTE: Source Regulation (EU) 910/2014 [i.1].

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

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

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

NOTE: Source ISO/IEC 19795-1 [i.17].

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

NOTE: Source ISO/IEC 19795-1 [i.17].

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

identity document: physical or digital 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 the resulting restrictions on the selection of attributes and evidence and on the identity proofing process itself

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

identity proofing 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

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.

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].

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

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.

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 trusted 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.

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:

APCER	Attack Presentation Classification Error Rate
BPCER	Bona fide Presentation Classification Error Rate
eID	electronic Identification
eMRTD	electronic Machine Readable Travel Document
FAR	False Acceptance Rate
FRR	False Rejection Rate
GDPR	General Data Protection Regulation

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
PAD	Presentation Attack Detection
QCP	Qualified Certificate Policy
TLS	Transport Layer Security
TSP	Trust Service Provider

3.4 Notations

The requirements identified in the present document include:

a) requirements applicable to any TSP 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

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

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

4 General concepts

4.1 Identity proofing actors

Regulation (EU) 910/2014 [i.1] of the European Parliament and of the Council (the eIDAS Regulation) does not 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. 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 the Baseline LoIP.

The applicant is identified by a set of identity attributes, and evidence is provided by the applicant to link these attributes to the applicant. The identity proofing process can be carried out automated, by a human 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 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.

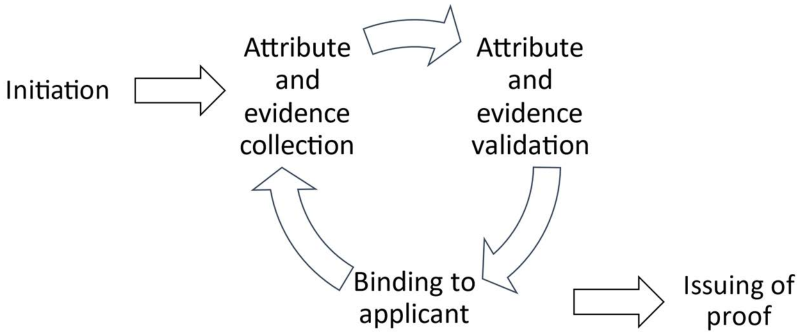
Initiation
Attribute and evidence collection
Attribute and evidence validation
Binding to applicant
Issuing of proof

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 8 is structured into sub-clauses 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 information.
- Clause 8.3 states requirements for validation of attributes against the provided evidence and requirements to ensure that evidence in itself is genuine and valid.
- Clause 8.4 states requirements for binding to applicant, meaning ensuring that the applicant presenting the evidence really is the person identified by the evidence. Binding to applicant can be done manually by a registration officer, or automated, notably by biometrics for natural persons, or by a combination of manual and automated.
- 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 LoIP. Requirements are specified for five use cases and sub-cases when the applicant is a natural person:

1) Physical presence:
    a) Manual operation.
    b) Hybrid manual and automated operation.
    c) Automated operation.
2) Attended remote, where the applicant communicates in real-time with a registration officer:
    a) Manual operation.
    b) Hybrid manual and automated operation.
3) Unattended remote, where the communication with the applicant is automated:
    a) Manual operation.

    b) Hybrid manual and automated operation.

    c) Automated operation.

4) Use of eID means.

5) Use of digital signature with certificate.

Automated operation is considered not relevant to the attended remote case since a registration officer is anyway needed for communication with the applicant. While remote identity proofing with manual operation can be applied, the use of hybrid manual and automated operation is strongly encouraged. Fully automated operation 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 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 requirements, whether the physical identity document is used with physical presence, remote with automated validation, or remote with manual validation.

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 subject to the requirements of the eIDAS Regulation [i.1] and 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 of the identity proofing, assumed to be Baseline 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.

- 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.

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 digital signature supported by certificate. Use of these evidence types as authoritative evidence requires fulfilment of the relevant requirements of the present document.

NOTE 1: 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, proof of access (in particular of a bank account), and documents and attestations.

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

EXAMPLE 1: A national population register can be considered as authoritative evidence 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.

NOTE 2: An exception is the identity proofing use cases for a legal person in clause 9.3 of the present document. 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.

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.

The evidence listed as authoritative evidence above can be used in simplified ways as supplementary evidence, but this is out of the scope of the present document.

EXAMPLE 3: An eID is used as authoritative evidence, and a still photo of a physical identity document is used as supplementary evidence; a still photo of a physical identity document is not sufficient to accept the document as authoritative evidence but can be sufficient for the use of the document as supplementary evidence.

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, which 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 and the related countermeasures specified by the present document.

		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(*)** 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

More detailed examples of threats are provided in Annex B 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 CABs 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 LoIP Baseline may use in its documentation the following specific OID:

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

5 Operational risk assessment

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

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.

6.2 Terms and Conditions

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

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.

7.9 Incident management

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

7.10 Collection of evidence

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

7.11 Business continuity management

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

7.12 Termination and termination plans

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

7.13 Compliance

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

8 Identity proofing service requirements

8.1 Initiation

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

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

INI-8.1-03: 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 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).

8.2 Attribute and evidence collection

8.2.1 General requirements

COL-8.2.1-01: The identity attributes required for the identity proofing context shall be defined and collected.

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

COL-8.2.1-03: The identity attributes shall be validated by use of one or more authoritative 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-8.2.1-06: A list of the identity proofing use cases supported, the evidence that can be trusted, and, as far as possible, the identity proofing contexts supported shall be published.

NOTE 4: Identification of use cases can be by reference to clause 9 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 information 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 information conveyed from an evidence does 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

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

COL-8.2.2.1-01: For each identity proofing context supported, the means used to collect identity attributes for a natural person shall be documented and published.

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

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 1: 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 2: 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 3: 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 4: 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.

NOTE 5: 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, official 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 6: 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.

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

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

COL-8.2.2.2-01: For each identity proofing context supported, the means used to collect identity attributes for a legal person shall be documented and published.

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, or by manual input in the course of the identity proofing process.

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 LEI (Legal Entity Identifier).

8.2.2.3 Attribute collection for natural person representing legal person

[CONDITONAL] 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.

8.2.3 Use of physical and digital identity document as evidence

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

COL-8.2.3-01: An identity document used as evidence may 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-8.2.3-02: The document used as authoritative evidence shall contain a face photo and/or other information that can be 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 supplementary documents without a face photo or similar information.

NOTE 4: The present document only specifies requirements for binding to applicant using face biometrics and/or manual face verification. Requirement COL-8.2.3-02 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-8.2.3-03: For each identity proofing context supported, a list of the identity documents that are accepted shall be documented and published.

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-8.2.3-04: If physical identity documents are used as evidence, only passports, national identity cards and other official identity documents that according to the identity proofing context offer comparable 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-8.2.3-05: If physical identity documents are used as evidence, the documents shall be presented in their 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, photo, or scan.

[CONDITIONAL] COL-8.2.3-06: If digital identity documents are used as 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 comparable 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.

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

8.2.4 Use of existing eID means as evidence

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

COL-8.2.4-01: 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 documented and published.

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 is 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 eIDAS Regulation [i.1] Article 9 can be used.

COL-8.2.4-02: The eID shall conform to eIDAS LoA substantial or high or conform to an LoA defined by another assurance level framework and offering comparable assurance to the relevant eIDAS LoA level.

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 eIDAS Regulation [i.1] 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-8.2.4-03: If required attributes to be collected cannot be confirmed by the authentication using the eID means, these attributes shall be collected from other sources and validated by use of other evidence 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.

[CONDITIONAL] COL-8.2.4-04: If the eID means is used for an identity proofing process supporting an EU qualified trust service, the eID shall conform to eIDAS LoA substantial or high.

NOTE 6: When the qualified trust service is the issuance of a qualified certificate, eIDAS Article 24.1 (b) states that the eID means is required to be issued based on a prior physical presence of the natural person or an authorized representative of the legal person.

8.2.5 Use of existing digital signature means as evidence

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

COL-8.2.5-01: For each identity proofing context supported, the conditions under which digital signatures and certificates are accepted shall be documented and published.

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 information included in the certificate and the semantics of this information.

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 eIDAS regulation, 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.

[CONDITONAL] 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.

COL-8.2.5-03: The certificate shall at least conform to the NCP policy level as defined by ETSI EN 319 411-1 [i.7].

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-8.2.5-04: If required attributes to be collected are not present in the certificate, these attributes shall be collected from other sources and validated by the use of other evidence in accordance with the identity proofing context.

[CONDITIONAL] COL-8.2.5-05: If the digital signature with certificate is used for an identity proofing process supporting an EU qualified trust service, the digital signature shall be a qualified electronic signature as defined by the eIDAS Regulation if the applicant is a natural person or a natural person representing a legal person, or a qualified electronic seal as defined by the eIDAS Regulation if the applicant is a legal person.

NOTE 6: When the qualified trust service is the issuance of a qualified certificate, eIDAS Article 24.1 (c) states that the qualified certificate is required to be 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 eID means conforming to eIDAS substantial or high that is in turn based on identity proofing by the physical presence of the natural person or an authorized representative of the legal person.

8.2.6 Use of trusted register as supplementary evidence

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

COL-8.2.6-01: 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 documented and published.

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

EXAMPLE 2: Depending on the identity proofing context, information sources such as existing customer databases of TSPs or other service providers can be defined as trusted registers.

[CONDITIONAL] COL-8.2.6-03: If the applicant is a legal person, the attributes collected for the legal person shall be verified against an authoritative business register to the extent that the legal person is registered and that the required attributes are present in the register.

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

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

COL-8.2.7-01: 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 or validated from these mechanisms shall be documented and published.

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

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

EXAMPLE 2: Proof of access to a mobile phone with identity information 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-8.2.7-03: The reliability of attributes obtained from proof of access mechanisms shall be evaluated with all cases of attributes considered to have lower reliability than the outcome of the general identity proofing process documented and published.

EXAMPLE 4: The general outcome of an identity proofing process is Baseline, 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

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

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

EXAMPLE 1: For a natural person, in some countries, utility bills or similar can be required as evidence of address.

EXAMPLE 2: 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.

[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-8.2.8-03: The reliability of attributes obtained from documents and attestations shall be evaluated with all cases of attributes considered to have lower reliability than the outcome of the general identity proofing process documented and published.

EXAMPLE 3: The general outcome of an identity proofing process is Baseline, 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.

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-8.2.9-03: 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 documented and published.

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

COL-8.2.9-04: For each identity proofing context supported, the positions, roles, or other relationships accepted for a natural person to represent a legal person shall be documented and published.

EXAMPLE 2: Directors, executives, board members, or a natural person with authorization duly delegated from another natural person in an authorized role.

COL-8.2.9-05: 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 documented and published.

COL-8.2.9-06: If the legal person is listed in an authoritative business register, the role of the natural person concerning the legal person shall be collected from or validated against this business register to the extent that the required attributes are present in the register.

NOTE 1: Practices for registration vary between countries. As one example, public sector entities are not registered in business registers in all countries.

COL-8.2.9-07: The role of the natural person concerning the legal person may be collected from or verified against other information sources than authoritative business registers.

NOTE 2: This, in particular, applies to legal persons that are not present in such business registers.

EXAMPLE 3: Information source can be public notaries, other registers than business registers, the official web site of the legal person, 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-8.3.1-01: All necessary identity attributes shall be validated to the required reliability by the presented evidence.

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-8.3.1-03: The handling of differences in encoding of identity attributes between collected attributes and attributes from evidence, and between different evidence, shall be described.

EXAMPLE 1: Typical sources of differences are transcription between alphabets 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-8.3.1-04: The handling of differences in name attributes between collected attributes and attributes from evidence, and between different evidence, shall be described.

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-8.3.1-06: The identity proofing process shall verify that the evidence is issued by an authoritative source that is trusted according to the identity proofing context.

[CONDITONAL] 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-8.3.1-08: The identity proofing process shall verify 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: The authenticity and integrity of the evidence shall be verified.

[CONDITIONAL] VAL-8.3.1-10: If the evidence has explicit security features/elements, these elements shall be verified.

NOTE 2: This need not be all security elements of, e.g. a physical identity document. A selection of elements sufficient for assessing that the evidence is genuine can be applied.

VAL-8.3.1-11: The identity proofing process shall as far as 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.

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

8.3.2 Validation of digital identity document

[CONDITONAL] If digital identity documents are used as evidence, the requirements in the present clause apply.

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

NOTE 2: 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 3: 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 4: 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-8.3.2-04: If the digital identity document is required to be read from a chip embedded in a physical identity document, the identity proofing process shall ensure that neither the applicant nor an external attacker can inject into the process a copy of a digital identity document that has previously been obtained and stored by the attacker.

NOTE 5: 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 6: 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.

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 7: 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

[CONDITONAL] If a physical identity document is used as 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-8.3.3-01: The process shall verify that the physical identity document presented is visually equal to the expected visual appearance of the document type.

[CONDITONAL] VAL-8.3.3-02: If a physical identity document is used as evidence in a remote validation 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 LoIP.

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-8.3.3-04: 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 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 a still photo of the identity document is not considered sufficient for Baseline LoIP. This can change in the future with the development of image analysis technology.

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

[CONDITIONAL] VAL-8.3.3-05: If the physical identity document is used in a remote identity proofing process, the 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.

NOTE 5: In particular, to protect against replay attack with the injection of another video stream in the process.

[CONDITONAL] 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 3: PRADO (Public Register of Authentic Travel and Identity Documents Online) for the EU and the EEA countries.

VAL-8.3.3-07: Security elements of physical identity documents shall be verified to the extent needed to obtain sufficient reliability in the genuineness of the document; the verification process shall be documented.

EXAMPLE 4: Security elements can be watermarks, holograms, printing techniques, visual and infrared light patterns, and see-through elements.

[CONDITONAL] 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.

[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 6: 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 7: 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 8: 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 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.

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

[CONDITONAL] VAL-8.3.3-12: If the physical identity document is used in a remote identity proofing process, and the identity document has an MRZ (machine readable zone), the information from the MRZ should be extracted and validated.

[CONDITONAL] 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.

[CONDITONAL] VAL-8.3.3-14: 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.

[CONDITONAL] VAL-8.3.3-15: If validation of physical identity documents is done manually, the training of the registration officers shall be repeated or refreshed at least annually.

[CONDITONAL] 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 5: Magnifying glass and an ultraviolet lamp.

[CONDITONAL] 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 6: 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 10: 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 11: 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 12: 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 human registration officer.

[CONDITONAL] VAL-8.3.3-19: If automated means and machine-learning technology are used to analyse physical identity documents, the video stream recorded according to requirement **VAL-8.3.3.-04** shall be of sufficient quality for the analysis.

[CONDITONAL] 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

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

VAL-8.3.4-01: An authentication protocol that confirms 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.

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

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

8.3.5 Validation of digital signature with certificate

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

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

NOTE 1: This is to avoid threats from the use of documents previously signed by the applicant.

VAL-8.3.5-02: The digital signature shall be validated and the signing certificate shall only be used as evidence for identity attributes if the signature is valid.

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

NOTE 3: If the digital signature is valid, the information obtained from the certificate supporting the digital signature can be considered valid and bound to the applicant.

NOTE 4: The certificate can represent a natural person, a legal person, or a natural person representing a legal person.

[CONDITIONAL] VAL-8.3.5-03: If the identity proofing context requires a digital signature supported by a qualified certificate according to the eIDAS Regulation, the signature should be validated according to ETSI TS 119 172-4 [i.14].

8.3.6 Validation of information obtained from trusted registers

[CONDITONAL] If trusted registers are used in an identity proofing process, the requirements in the present clause apply.

[CONDITONAL] 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.

[CONDITONAL] 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.

[CONDITONAL] 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.

[CONDITONAL] 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-8.3.6-05: The integrity and authenticity of the information obtained from the trusted register shall be validated.

VAL-8.3.6-06: The procedure to apply in case of discrepancies between the information obtained from trusted registers and information from other evidence shall be documented.

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

8.3.7 Validation of proof of access

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

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-8.3.7-02: The identity information 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 PSD2 (EU Payment Services Directive) SCA (Strong Customer Authentication) [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-8.3.7-05: 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 documented.

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

8.3.8 Validation of documents and attestations

[CONDITONAL] If documents and attestations are used 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-8.3.8-02: The identity of the issuer of the document or attestation, and the authenticity and integrity of the contained information, shall be verified.

NOTE 1: 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 2: 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-8.3.8-05: 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 documented.

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

8.4 Binding to applicant

8.4.1 General requirements

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

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

NOTE 1: For the 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

[CONDITONAL] 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-8.4.2-02: The video capture process shall apply liveness detection measures to ensure that the video stream is of a live person present in front of the camera at the time of the identity proofing.

NOTE 2: It is required that this happens at the time of the identity proofing; submission of a pre-recorded video stream is considered not to meet the requirements for identity proofing to Baseline LoIP. A part of liveness detection can be instructing the applicant to perform certain actions, where the specific actions or their sequence are unpredictable to the applicant.

BIN-8.4.2-03: The video stream capture should apply measures to detect artificially generated or manipulated face appearance.

NOTE 3: 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.

NOTE 4: In particular to protect against replay attack with an injection of another video stream in the process.

NOTE 5: This can rely on the applicant's use of software approved for the identity proofing process, e.g. mobile app functionality.

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

BIN-8.4.2-06: The video stream capture shall apply PAD measures in compliance with ISO/IEC 30107-3 [3].

BIN-8.4.2-07: The PAD should be evaluated according to ISO/IEC 19989-3 [i.18].

NOTE 6: ISO/IEC 19989-3 [i.18] specifies security evaluation of PAD applying Common Criteria (ISO/IEC 15408 [i.24]).

BIN-8.4.2-08: Test results for the PAD shall achieve an APCER (attack presentation classification error rate) as defined by ISO/IEC 30107-3 [3] at the level of industry best practice.

NOTE 7: 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-8.4.2-09: Test results for the PAD should achieve BPCER (bona fide presentation classification error rate) as defined by ISO/IEC 30107-3 [3] at the level of industry best practice.

NOTE 8: The BPCER has no impact on security but on user-friendliness.

BIN-8.4.2-10: The PAD measures and APCER and BPCER rates shall be kept up to date concerning advances in the threat landscape and available technology.

8.4.3 Binding to applicant by automated face biometrics

[CONDITONAL] 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-8.4.3-01 The process shall provide a reliable, automated comparison between the face image extracted from the identity document presented by the applicant and a face image captured according to the requirements of clause 8.4.2 of the present document.

BIN-8.4.3-02: Only data capture and preliminary data quality assessment shall 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 clause 5.1 in ISO/IEC 30107-1 [i.16].

[CONDITONAL] 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.

[CONDITONAL] 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-8.4.3-06: The biometric algorithms and technologies applied shall be systematically tested against reference datasets and kept updated to cope with changes in the threats and risk situation.

NOTE 2: See for example, clauses for face biometrics in ISO/IEC 19795-1 [i.17].

BIN-8.4.3-07: Test results for the biometric face recognition shall show a FAR (false acceptance rate) at the level of industry best practice.

NOTE 3: No specific number is specified for FAR. Rapid technology improvement can lead to significant progress in industry best practice FAR performance even in the short term.

NOTE 4: An example of industry best practice reference can be the one-to-one face matching results reported from the NIST Face Recognition Vendor Test.

BIN-8.4.3-08: Test results for the biometric face recognition should show a FRR (false rejection rate) at the level of industry best practice.

NOTE 5: False rejection rate has no impact on security but on user-friendliness.

BIN-8.4.3-09: The biometric face recognition may apply measures to detect morphed photos in identity documents.

NOTE 6: 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 human 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 7: 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.

8.4.4 Binding to applicant by manual face verification

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

BIN-8.4.4-01: The registration officer shall compare the face photo obtained from the applicant's identity document with the applicant's physical appearance, either from the applicant's the physical presence or from a 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-8.4.4-04: The registration officer shall be allowed to spend sufficient time for the face comparison.

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 shall 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

[CONDITONAL] 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-8.4.5-02: If the applicant is a natural person representing a legal person, the identity of the natural person shall be proven according to the requirements 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-8.4.5-04: If the applicant is a natural person representing a legal person, and the legal person is listed in an authoritative business register, the natural person's authorization to represent the legal person should be proven by information from that register.

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

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), or an identity assertion (e.g. OIDC, SAML).

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 LoIP defined by the present document.

ISS-8.5.1-03: The result of the identity proofing process may convey LoIP separately for individual identity attributes that are not required for unique identification in the identity proofing context and where these LoIPs differ from the overall result of the identity proofing process.

8.5.2 Evidence of the identity proofing process

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

NOTE 1: Evidence can be retained in digital or paper format.

NOTE 2: The need to retain evidence of identity proofing processes that did not complete successfully can be determined by the identity proofing context.

NOTE 3: 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-8.5.2-02: The evidence of the identity proofing process shall document the identity 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 a video sequence or 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 video sequences used in a remote identity proofing process; however, retaining video sequences or images of a human applicant can, depending on the identity proofing context, be required, allowed, or forbidden.

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 several of 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-8.5.2-06: 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 4: Offline storage or other means that will result in a prolonged response time are acceptable.

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 LoIP

9.1 Introduction

USE-9.1-01: The identity proofing process should conform to at least one of the use cases in the present clause 9 for the LoIP Baseline.

NOTE 1: Clause 9 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.

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

- 8.1 (initiation);
- 8.2.1 (attribute and evidence collection general requirements);
- 8.3.1 (attribute and evidence validation general requirements);
- 8.4.1 (binding to applicant general requirements); and
- 8.5 (issuing of proof).

USE-9.1-03: 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 LoIP shall be demonstrated.

9.2 Use cases for identity proofing of natural person

9.2.1 Use cases 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, and the Baseline LoIP is targeted, then the following requirements apply.

NOTE 1: 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 2: 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 3: 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 4: The identity proofing context can require the use of specific supplementary evidence.

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

USE-9.2.1.2-04: Evidence validation shall be according to the requirements in clause 8.3.3 of the present document, including the following conditional requirements: 8.3.3-06, 8.3.3-08, 8.3.3-13, 8.3.3-14, 8.3.3-15.

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-9.2.1.3-03: At least one digital identity document shall be used as 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-9.2.1.3-05: 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-9.2.1.4-05: At least one digital identity document shall be used as evidence.

NOTE 2: A fully automated procedure to Baseline 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.

USE-9.2.1.4-08: The capture of the face image of the applicant should be according to the requirements in clause 8.4.2 of the present document.

NOTE 3: Since the face image can be captured by specialized equipment and the applicant is physically present, not all requirements in clause 8.4.2 are necessarily relevant.

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 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 human registration officer, and the Baseline LoIP is targeted, then the following requirements apply.

NOTE 1: 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 human 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: The capture of the face image of the applicant shall be according to the requirements in clause 8.4.3 of the present document.

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 2: The identity proofing context can require use of the specific supplementary evidence.

9.2.2.2 Use case for manual operation

[CONDITIONAL] If the identity proofing is based on the remote presence of the applicant with online communication with a human 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: This use case is similar to the physical appearance with manual operation case in clause 9.2.1.2 of the present document. Even though validation of the physical identity document and binding to applicant are more difficult than with physical presence, the use case is acceptable 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-9.2.2.2-01: At least one physical identity document shall be used as evidence.

USE-9.2.2.2-02: Evidence validation shall be according to the requirements in clause 8.3.3 of the present document, including the following conditional requirements:

- 8.3.3-02;
- 8.3.3-04;
- 8.3.3-05;
- 8.3.3-06;
- 8.3.3-14;
- 8.3.3-15.

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 human 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-9.2.2.3-01: If a digital identity document is used as 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-9.2.2.3-02: If a physical identity document is used as evidence, evidence validation shall be according to the requirements in clause 8.3.3 of the present document, including the following conditional requirements:

- 8.3.3-02;
- 8.3.3-04;
- 8.3.3-05;
- 8.3.3-06;
- 8.3.3-14;
- 8.3.3-15.

[CONDITIONAL] USE-9.2.2.3-03: If a physical identity document is used as evidence, requirements **COL-8.3.3-18** and **COL-8.3.3-19** 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.

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.

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.

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

USE-9.2.2.3-05: If binding to applicant is by a combination of manual face verification and automated face biometrics, and the two binding methods yield different results, either the result of the manual face verification shall prevail, or the identity proofing process shall be aborted.

9.2.3 Use cases 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, and the Baseline LoIP is targeted, then the following requirements apply.

NOTE 1: 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 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 2: The identity proofing context can require the use of specific supplementary evidence.

9.2.3.2 Use case for manual operation

[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 use case where the session with the applicant is automated but validation and binding to applicant is done later by purely manual operation is allowed, as it provides the same reliability as the similar case for remote attended identity proofing in clause 9.2.2.2. 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-9.2.3.2-03: At least one physical identity document shall be used as evidence.

USE-9.2.3.2-04: Evidence validation shall be according to the requirements in clause 8.3.3 of the present document, including the following conditional requirements:

- 8.3.3-02;
- 8.3.3-04;
- 8.3.3-05;
- 8.3.3-06;
- 8.3.3-14;
- 8.3.3-15.

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. While manual binding to applicant is allowed as per the manual use case in clause 9.2.3.2, combined manual and face biometrics binding to applicant is highly recommended.

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-9.2.3.3-02: If a digital identity document is used as 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-9.2.3.3-03: If physical identity document is used as evidence, evidence validation shall be according to the requirements in clause 8.3.3 of the present document, including the following conditional requirements:

- 8.3.3-02;
- 8.3.3-04;
- 8.3.3-05;
- 8.3.3-06;
- 8.3.3-14;
- 8.3.3-15.

[CONDITIONAL] USE-9.2.3.3-04: If a physical identity document is used as evidence, requirements **COL-8.3.3-18** and **COL-8.3.3-19** 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-9.2.3.3-05: 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.

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.

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

USE-9.2.3.3-06: If binding to applicant is achieved by a combination of manual face verification and automated face biometrics, and the two binding methods yield different results, either the result of the manual face verification shall prevail, or 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-9.2.3.4-01: At least one digital identity document shall be used as 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, and the Baseline LoIP is targeted, then 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.

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.

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, and the Baseline LoIP is targeted, then 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.

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.

9.3 Use case for identity proofing of legal person

[CONDITIONAL] If identity proofing is of a legal person, and the Baseline LoIP is targeted, then the following requirements apply.

NOTE 1: The present clause does not assume the involvement of a natural person representing the legal person.

NOTE 2: 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-9.3-02: The identity proofing shall use documents and attestations as 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.

USE-9.3-03: The identity proofing should collect and validate evidence from an authoritative trusted register according to the requirements in clauses 8.2.6 and 8.3.6 of the present document.

NOTE 3: The identity proofing context can require the use of specific documents and attestations or trusted registers as evidence.

USE-9.3-04: 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.

NOTE 4: While eID means authenticating a legal person exists in the market, such solutions are not common.

USE-9.3-05: 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.

NOTE 5: A digital signature for a legal person is termed an 'electronic seal' by the eIDAS Regulation.

NOTE 6: 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 eIDAS Regulation 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.

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, and the Baseline LoIP is targeted, the following requirements apply.

USE-9.4-01: Identity proofing for the natural person shall be done according to the requirements for one of the use cases for Baseline LoIP in clause 9.2 of the present document.

NOTE: The identity proofing context can specify that only certain use cases are allowed.

USE-9.4-02: Evidence collection for a natural person representing a legal person shall be done according to the requirements in clause 8.2.9 of the present document.

USE-9.4-03: The evidence collected for the legal person and for the natural person's authorization to represent the legal person shall be validated according to requirements in the relevant parts of clause 8 of the present document.

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

A.1 Introduction

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

- ETSI EN 319 411-1 [i.7] and ETSI EN 319 411-2 [i.8] for issuance of certificates;
- ETSI EN 319 521 [i.12] for electronic registered delivery services;
- ETSI TS 119 431-1 [i.10] for remote electronic signing services that in turn refers to EN 419 241-1 [i.11].

A.2 Application for issuance of NCP certificates as specified in ETSI EN 319 411-1

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

> ***[QUOTE]***
>
> ***REG-6.2.2-02: The TSP shall collect either direct evidence or an attestation from an appropriate and authorized source, of the identity (e.g. name) and if applicable, any specific attributes of subjects to whom a certificate is issued. Submitted evidence may be in the form of either paper or electronic documentation (in both cases the RA shall validate their authenticity). Verification of the subject's identity shall be at time of registration by appropriate means.***
>
> ***When the subject is a natural person (i.e. physical person as opposed to legal person):***
>
> ***REG-6.2.2-05 [NCP] [CONDITIONAL]: If the subject is a natural person (i.e. physical person as opposed to legal person), evidence of the subject's identity (e.g. name) shall be checked against this natural person either directly by physical presence of the person (the subject shall be witnessed in person unless a duly mandated subscriber represents the subject), or shall have been checked indirectly using means which provides equivalent assurance to physical presence.***
>
> ***NOTE 1: An example of the required indirect evidence of identity is one or more registration documents electronically signed by a person trusted to have checked the person's identity in line with the requirements of this clause.***
>
> ***[end QUOTE]***

The requirements of the present document are intended to fulfil the above requirements as follows:

Referring to the above requirement **REG-6.2.2-05** from ETSI EN 319 411-1 [i.7], the requirement for identity proofing "by the physical presence of the natural person" can be met by the application of clause 9.2.1 of the present document: "Use cases with physical presence of the applicant".

Referring to the above requirement **REG-6.2.2-05** from ETSI EN 319 411-1 [i.7], the requirement for identity proofing "*by methods which provide equivalent assurance … to the physical presence*" can be met through application of the following clauses of the present document: clause 9.2.2 "Use cases for attended remote identity proofing", clause 9.2.3 "Use cases for unattended remote identity proofing", clause 9.2.4 "Use case for identity proofing by authentication using eID means", or clause 9.2.5 "Use case for identity proofing using digital signature with certificate".

Referring to the above requirement **REG-6.2.2-02** from ETSI EN 319 411-1 [i.7], the requirement to collect evidence from an appropriate and authorized source is covered by clause 8.2 of the present document.

> ***[QUOTE]***
>
> ***When the subject is a natural person who is identified in association with a legal person (e.g. the subscriber):***
>
> ***REG-6.2.2-08 [NCP] [CONDITIONAL]: If the subject is a natural person who is identified in association with a legal person (e.g. the subscriber), evidence of the identity, in particular the ones listed in REG-6.2.2-09, shall be checked against a natural person either directly by physical presence of the person (the subject shall be witnessed in person unless a duly mandated subscriber represents the subject), or shall have been checked indirectly using means which provides equivalent assurance to physical presence.***
>
> ***[end QUOTE]***

Requirement **REG-6.2.2-08** from ETSI EN 319 411-1 [i.7] can be met through application of clause 9.4 of the present document: "Use case for identity proofing of natural person representing legal person".

> ***[QUOTE]***
>
> ***When the subject is a legal person, or other organizational entity identified in association with a legal person:***
>
> ***REG-6.2.2-10 [NCP] except [EVCP] [CONDITIONAL]: If the subject is a legal person, or other organizational entity identified in association with a legal person, evidence of the identity, in particular the ones listed in REG-6.2.2-12, shall be checked against a duly mandated subscriber either directly, by physical presence of a person allowed to represent the legal person, or shall have been checked indirectly using means which provides equivalent assurance to physical presence.***
>
> ***[end QUOTE]***

Requirement **REG-6.2.2-10** from ETSI EN 319 411-1 [i.7] can be met through application of clause 9.3 of the present document: "Use case for identity proofing of legal person".

> ***[QUOTE]***
>
> ***REG-6.2.2-09 [CONDITIONAL]: If the subject is a natural person who is identified in association with a legal person (e.g. the subscriber), evidence shall be provided of:***
>
> ***[…]***
>
> ***e) affiliation of the natural person to the legal person consistent with national or other applicable identification practices;***
>
> ***[…]***
>
> ***[end QUOTE]***

Requirement **REG-6.2.2-09** from ETSI EN 319 411-1 [i.7] can be met through application of clause 9.4 of the present document: "Use case for identity proofing of natural person representing legal person".

A.3 Application for issuance of QCP certificates as specified in ETSI EN 319 411-2

ETSI EN 319 411-2 [i.8] specifies requirements for a QTSP issuing qualified certificate as defined in the eIDAS Regulation (EU) No 910/2014 (eIDAS) [i.1], Article 24.1. To do so, ETSI EN 319 411-2 [i.8] integrates the requirements for issuing NCP certificates (see clause A.2) and further specifies the following requirements for the issuance of a qualified certificate, **QCP certificate**, as quoted from ETSI EN 319 411-2 [i.8]:

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

The requirements of the present document are intended to fulfil requirements for issuance of a QCP certificate as follows:

The above requirement **REG-6.2.2-05** from ETSI EN 319 411-1 [i.7] and **REG-6.2.2-02 a** from ETSI EN 319 411-2 [i.8] for identity proofing "*by the physical presence of the natural person*" can be met by the application of the following clauses of the present document: clause 9.2.1 "Use cases with physical presence of the applicant" when the applicant is a natural person, clause 9.3 "Use cases for identity proofing of legal person" when the applicant is a legal persons, and clause 9.4 "Use cases for identity proofing of natural person representing legal person" when the applicant is a natural person representing a legal person.

The above requirement **REG-6.2.2-05** from ETSI EN 319 411-1 [i.7] and **REG-6.2.2-02 b** from ETSI EN 319 411-2 [i.8] for identity proofing "*by methods which provide equivalent assurance … to the physical presence*" can be met by the application of one of the following clauses of the present document: clause 9.2.2 "Use cases for attended remote identity proofing", clause 9.2.3 "Use cases for unattended remote identity proofing", clause 9.2.4 "Use case for identity proofing by authentication using eID means", or clause 9.2.5 "Use case for identity proofing using digital signature with certificate". As demonstrated in Annex B of the present document, the level of confidence in the identity achieved by the use cases of these clauses is equivalent to the level of confidence on the identity as specified in clause 9.2.1 of the present document: "Use cases with physical presence of the applicant", i.e. a high level of confidence in the identity for all use-cases.

As indicated by ETSI EN 319 411-2 [i.8] **REG-6.2.2-02 b**, the proof of equivalence can be done according to Regulation (EU) No 910/2014 [i.1].

In particular, Article 24.1 (d) of Regulation (EU) No 910/2014 [i.1] states: "*by using other identification methods recognized at national level which provide equivalent assurance in terms of reliability to physical presence. The equivalent assurance shall be confirmed by a conformity assessment body*" can be met by the application of any of the clauses referred above for **REG-6.2.2-05** from ETSI EN 319 411-1 [i.7] and **REG-6.2.2-02 b** from ETSI EN 319 411-2 [i.8], for ways equivalent in terms of reliability to physical presence. Since eIDAS Article 24.1 (d) refers to "methods recognized at national level", it is clear that approval by a national authority is needed.

NOTE 1: The referred requirements above consider remote identity proofing with liveness detection and other presentation attack detection methods equivalent to physical presence.

NOTE 2: To cover *"the impersonation risks inherent to remote applications. In particular, an uninterrupted chain of subsequent remote registrations can increase such risks, because the person can never be actually seen for years, and/or because the traceability with the initial face to face is weakened"*, the present document indicates measurable quality thresholds on the evidence to be used, independent of the fact that such evidence was issued remotely or in the presence of the applicant. E.g. the quality of a certificate supporting a qualified signature is ensured by the fact that the issuing TSP is duly supervised. The quality of a notified eIDAS eID means is ensured by the review done for the eID means notification process. By requiring such quality benchmark on evidence, the present document does not require the quality of such evidence itself to be assessed (in particular, whether such evidence was issued remotely or not). It pushes this responsibility to the evidence producer (e.g. a QTSP issuing certificate, a government issuing an eIDAS eID means, etc.).

The same reasoning applies "mutatis mutendis" to the issuance of a QCP to a legal person by reference to the requirements defined for issuing of an NCP certificate (see clause A.2).

A.4 Application of the present document to ETSI EN 319 521

The current requirement in ETSI EN 319 521 [i.12] states requirements for a Qualified Electronic Registered Delivery Service (QERDS) as quoted:

[QUOTE]

REQ-QERDS-5.2.1.1-01 The QERDSP shall verify the identity of the sender and the recipient either directly or by relying on a third party:

a) by the physical presence of the natural person or of an authorized representative of the legal person; or

b) remotely, using electronic identification means, for which a physical presence of the natural person or of an authorized representative of the legal person was ensured and which meets the requirements set out in Article 8 of the Regulation (EU) N° 910/2014 with regard to the assurance levels 'substantial' or 'high'; or

c) by means of a certificate of an advanced electronic signature or of an advanced electronic seal; or

d) by using other identification methods recognized at national level which provide equivalent assurance in terms of reliability to physical presence. The equivalence of the assurance level shall be confirmed by a conformity assessment body.

NOTE: The third party verifying the identity of the sender and the recipient can be another QERDSP in the case that the sender or the recipient or both are subscribed to another QERDSP.

[end QUOTE]

The requirements of the present document are intended to fulfil requirements for verification of entity (natural person) as requested above as follows:

Referring to the above requirement **REQ-QERDS-5.2.1.1-01 a)** from ETSI EN 319 521 [i.12], the requirement for "*by the physical presence of the natural person*" can be met by the application of the means specified in clauses A.2 and A.3 of the present document to cover **REG-6.2.2-05** from ETSI EN 319 411-1 [i.7].

Referring to the above requirement **REQ-QERDS-5.2.1.1-01 b)** from ETSI EN 319 521 [i.12], the requirement for *"using electronic identification means"* can be met by the application of clause 9.2.4 of the present document: "Use case for identity proofing by authentication using eID means".

Referring to the above requirement **REQ-QERDS-5.2.1.1-01 c)** from ETSI EN 319 521 [i.12], the reqirement for *"by means of a certificate of an advanced electronic signature or of an advanced electronic seal"* can be met by application of clause 9.2.5 of the present document: "Use case for identity proofing using digital signature with certificate".

Referring to the above requirement **REQ-QERDS-5.2.1.1-01 d)** from ETSI EN 319 521 [i.12], the requirement for "*by methods which provide equivalent assurance … to the physical presence"* can be met by the application of any of the means specified in clauses A.1 and A.2 of the present document to cover **REG-6.2.2-05** from ETSI EN 319 411-1 [i.7].

A.5 Application of the present document to ETSI TS 119 431-1 and EN 419 241-1

ETSI TS 119 431-1 [i.10] specifies the by-default policy referring to EN 419 241-1 [i.11] as follows:

[QUOTE]

> ***LNK-6.2.2-01: Clause SRC_SA.1.1 of CEN EN 419 241-1, specifying enrolment shall apply.***
>
> ***I.e. SRC_SA.1.1 The enrolment of the signer SHALL be as specified in Annex A, A.1, for assurance level low or higher.***

[end QUOTE]

ETSI TS 119 431-1 [i.10] further specifies the normalized policy as follows:

[QUOTE]

> ***LNK-6.2.2-02 [NSCP] [CONDITIONAL]: If the signer is a natural person, clause SRA_SAP.1.1 of CEN EN 419 241-1, specifying enrolment shall apply.***
>
> ***I.e. SRA_SAP.1.1 The enrolment of the signer SHALL be as specified in Annex A, subclause A.1, for assurance level substantial or higher.***

[end QUOTE]

Annex A, subclause A.1, of EN 419 241-1 referred above provides requirements equivalent to the ones specified in the Annex to CIR (EU) 2015/1502 [i.3], clauses 2.1, 2.2.1 and 2.3.1 for assurance levels low, substantial, and high. The present document can fulfil these requirements as indicated in table A.1.

Table A.1

A.1.1 Application and registration **(for all levels)**	**Coverage by present document**
1. *Ensure the applicant is aware of the terms and conditions related to the use of the electronic identification means.*	Clause 6.2
2. *Ensure the applicant is aware of recommended security precautions related to the electronic identification means.*	Clause 6.2
3. *Collect the relevant identity data required for identity proofing and verification.*	Clause 8.2
A.1.2 Identity proofing and verification (natural person) **(for all levels)**	
1. *The person can be assumed to be in possession of evidence recognized by the Member State in which the application for the electronic identity means is being made and representing the claimed identity.*	Clause 8.4
2. *The evidence can be assumed to be genuine, or to exist according to an authoritative source and the evidence appears to be valid.*	Clause 8.3
3. *It is known by an authoritative source that the claimed identity exists and it may be assumed that the person claiming the identity is one and the same.*	Clause 8 and in particular requirement COL-8.2.1-03
IN ADDITION for level Substantial	
The person has been verified to be in possession of evidence recognized by the Member State in which the application for the electronic identity means is being made and representing the claimed identity; *and* *the evidence is checked to determine that it is genuine; or, according to an authoritative source, it is known to exist and relates to a real person;* *and* *steps have been taken to minimize the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired evidence;*	Clause 9.2 Clause 8.3 Clauses 8.3, 8.4 and 9.2
OR	
An identity document is presented during a registration process in the Member State where the document was issued and the document appears to relate to the person presenting it; *and* *steps have been taken to minimize the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired documents;*	Clause 9.2
OR	
Where procedures used previously by a public or private entity in the ***same Member*** *State for a purpose other than the issuance of electronic identification means provide for an equivalent assurance to those set out in section A.1.2 for the assurance level substantial, then the entity responsible for registration need not to repeat those earlier procedures, provided that such equivalent assurance is confirmed by a conformity assessment body compliant with the applicable regulatory requirements (see note) or by an equivalent body;*	Generally not applicable to the present document but clause 8.3.7 (proof of access) can be used if the requirement is fulfilled by the source of the information.
OR	
Where electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level substantial or high, and taking into account the risks of a change in the person identification data, it is not required to repeat the identity proofing and verification processes. Where the electronic identification means serving as the basis has not been notified, the assurance level substantial or high must be confirmed by a conformity assessment body compliant with the applicable regulatory requirements (see note) or by an equivalent body.	Clause 9.2.4

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

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 tricks the victim into a purported identity proofing process using identity documents, the attacker cannot be able to use the obtained 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

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 comparable security to passports and national identity cards.
[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.
[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-8.3.2-04 and VAL-8.3.3-07, 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 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. This cannot completely guarantee that a fake or forged document is accepted if the attacker has high competence and resources. 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. 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).

Attribute and evidence collection and validation threats	Coverage by ETSI TS 119 461 (the present document)
[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.
[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, but they can be expected to be infrequent enough that an attacker cannot expect an error to occur given several retries. 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 of 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.

Attribute and evidence collection and validation threats	Coverage by ETSI TS 119 461 (the present document)
[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, 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.
[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.	VAL-8.3.3-18 poses requirement for quality of the video stream if automated analysis of a physical identity document is used. For manual validation of a physical identity document is used, no similar requirement is posed, but VAL-8.3.3-16 requires that a registration officer has available tools. Requirements for the manual and hybrid use cases in clause 9.2 state that the identity proofing process is required to specify handling of deviations and conditions for aborting the process.
[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.

Attribute and evidence collection and validation threats	Coverage by ETSI TS 119 461 (the present document)
[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.
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-8.3.2-05 and VAL-8.3.3-02 cover protection against this type of attack for identity documents. Same for requirements in clause 8.4.2 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-8.3.3-05 for physical identity document, and BIN-8.4.2-04 for capture of face image of applicant.
[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-8.3.2-05 and VAL-8.3.3-02 cover protection against this type of attack for identity documents. BIN-8.4.2-02 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

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.)	Photo is not sufficient. A video recording of the applicant's face is required.

Binding to applicant threats	Coverage by ETSI TS 119 461 (the present document)
[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.	BIN-8.4.2-02 and other requirements in clause 8.4.2 require liveness detection and 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 for liveness detection and presentation attack detection are posed to protect against this threat.
[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 liveness detection and presentation attack detection are posed in clause 8.4.2 to protect against this threat. In addition, BIN-8.4.2-03 recommends measures to protect against deep fake attacks.
[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.	BIN-8.4.3-07 poses a strict requirement on the FAR (false acceptance rate) 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 identity information, which includes pictures and the evidence as such. With face biometrics, BIN-8.4.3-07 poses the FAR requirement that always apply, and BIN-8.4.3-08 has a recommendation for FRR (False Rejection Rate). 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.

Binding to applicant threats	Coverage by ETSI TS 119 461 (the present document)
[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).	BIN-8.4.3-07 poses the requirement for FAR for biometrics; FRR is not security relevant but is a user convenience, hence BIN-8.4.3-08 is only a recommendation. BIN-8.4.3-06 states that biometric algorithms and technologies applied 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.
[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-8.3.3-12 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-8.3.3-12 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 documented and published, and VAL-8.3.2-03 requires that a digital identity document is accepted only if the issuer's digital signature is successfully validated.

Binding to applicant threats	Coverage by ETSI TS 119 461 (the present document)
[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

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 that are recommended, and strict requirements in clause 8 for the tasks of an identity proofing process. Processes should 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 should 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.

History

Document history		
V1.1.1	July 2021	Publication