![ETSI logo] The Standards People

Standards for Identity proofing
ETSI TR 119 460 / TS 119 461

Presented by: **Sylvie Lacroix**   For: **Training on ETSI Standards for trust services**

01.06.2021

STF 588 - rationale

- The current European standards published by ETSI on trust services specify identity proofing only by generic requirements like "physical presence" or "*means which provide equivalent assurance as physical presence*" derived from eIDAS art. 24.1.

  - Physical presence as a benchmark is not well-defined as no requirements are posed neither for the quality of physical identity documents nor for the competence or procedures to be carried out by the person performing the check.

  - What constitutes "equivalent assurance" as physical presence is up to subjective judgement.

  - Guidelines for remote identity proofing are needed to avoid cumbersome and expensive physical presence procedures when possible.

- TSPs tend to outsource identity-proofing processes to dedicated service providers

- These needs become even more pressing under the options to review the eIDAS Regulation

ETSI STF 588 deliverables

ETSI TR 119 460 Electronic Signature and Infrastructures (ESI); Survey of technologies and regulatory requirements for identity proofing for trust service subjects.

This document surveys the technologies, legislations, specifications, guidelines and standards related to or used for identity proofing. Information has been gathered from stakeholders such as national agencies developing requirements, product and service vendors, research and academic environments, and relevant existing specifications.

TR 119 460 finalised - published

ETSI TS 119 461 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for identity proofing of trust service subjects.

This document aims to specify policy and security requirements for a trust service component providing identity proofing of trust service subjects. It can be used for conformity assessment of a trust service provider which includes this service component as part of its service or can be used for conformity assessment of a specialized provider of identity proofing supporting other trust service providers.

The document specifies practices for security supporting different technological approaches, and use-cases using these technologies offering a consistent 'baseline' outcome level.

TS 119 461 - Work in progress

Policy and security requirements for trust service components providing identity proofing of trust service subjects

- Identity proofing is not an eIDAS trust service by itself, but a trust service component. An identity proofing service component may be used by many different trust services

  - ETSI EN 319 403-1 auditable -> one audit that can be reused for different purposes

- Security and policy requirements

  - Based on ETSI EN 319 401 – common requirements for all trust services

  - Specific requirements for identity proofing
    - Specify best practice requirements on how to **use selected means** to implement the three tasks of attribute and evidence collection, attribute and evidence validation, and binding to applicant + initiation and result.
    - Specify how identity proofing processes can be constructed **by combining means** (use-cases) to meet the desired baseline outcome of the identity proofing process.

  - Support and relation with EN 319 411-1 / -2 clauses 6.2,

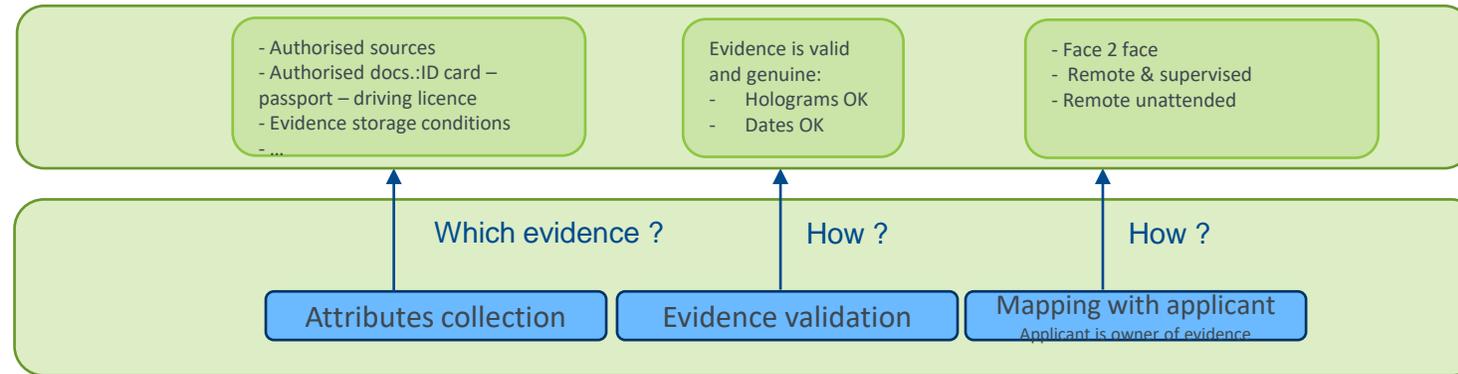 - Specific requirements to support qualified trust services (does not mean the ID Proofing is a (Q)TS)

- Security requirements are provided to cover commonly faced risks falling in two main categories

  - **Falsified evidence** : An applicant claims an incorrect identity using forged evidence.

  - **Identity theft** : An applicant uses valid evidence associated with another person.

  - Also considered : **operational risks** and **social risks (e.g. constraint)**

Identity proofing is part of the broader identity management lifecycle and must be considered 'in context'

ETSI
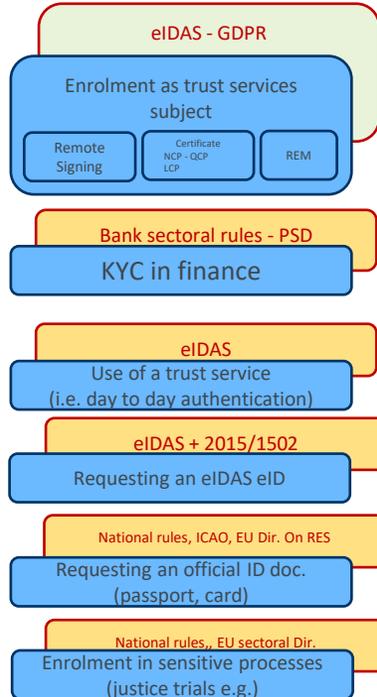
Depends on:
- Who is id-proved
- Purpose (context&outputs)

- Authorised sources
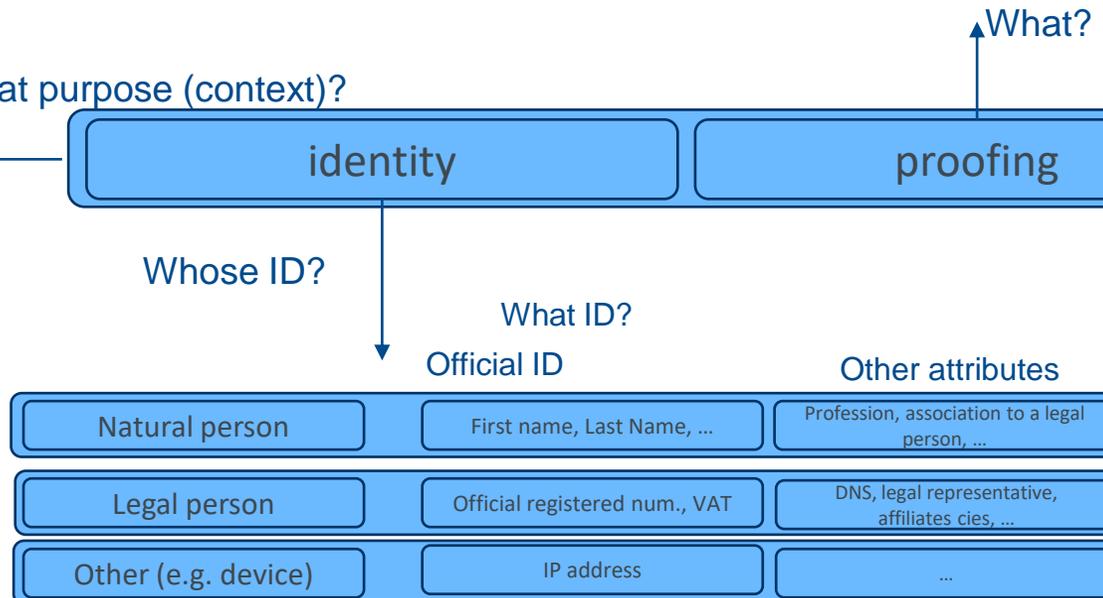- Authorised docs.:ID card – passport – driving licence
- Evidence storage conditions
- ...

Evidence is valid and genuine:
- Holograms OK
- Dates OK

- Face 2 face
- Remote & supervised
- Remote unattended

Process

Which evidence ?   How ?   How ?

Driving requirements behind purposes

eIDAS - GDPR
Enrolment as trust services subject
Remote Signing | Certificate NCP - QCP LCP | REM

Attributes collection   Evidence validation   Mapping with applicant
                                                             Applicant is owner of evidence

Can also be an input ...

Bank sectoral rules - PSD
KYC in finance

For what purpose (context)?

What?

eIDAS
Use of a trust service (i.e. day to day authentication)

| identity | proofing |

enrolment

Provision of credential for accessing service

Use-case e.g.
Issue a Natural person certificate for AdES, level NCP

eIDAS + 2015/1502
Requesting an eIDAS eID

Whose ID?

Typical outputs

Provision of official (e)ID means

National rules, ICAO, EU Dir. On RES
Requesting an official ID doc. (passport, card)

What ID?

Official ID   Other attributes

National rules,, EU sectoral Dir.
Enrolment in sensitive processes (justice trials e.g.)

Natural person	First name, Last Name, ...	Profession, association to a legal person, ...
Legal person	Official registered num., VAT	DNS, legal representative, affiliates cies, ...
Other (e.g. device)	IP address	...

TR 119 460 - information collection

ETSI TR 119 460 V1.1.1 (2021-02)

TECHNICAL REPORT

Electronic Signatures and Infrastructures (ESI);
Survey of technologies and regulatory requirements
for identity proofing for trust service subjects

- ⱱ 53 sources of information analysed in depth (collection of relevant documents by ESI, eMails (to ESI and eSignature News mailing list), found by STF experts while analysing received info.).

- ⱱ Direct contacts with stakeholders – spontaneous inputs

- ⱱ Liaison with ENISA Remote ID proofing report group

- ⱱ Questionnaires: in-depth responses to questionnaires from 5 QTSPs and 9 vendors

- ⱱ eIDAS up-date consultation

TR 119 460 - methodology for analysis
Reading Sheets based on ID proofing process components

The reading sheets offers **a common window to look at the information,** to compare heterogenous and numerous information and derive trends for each component:

- Short description (purpose, context, type of ID, …)

- Attribute & evidence collection

- Attribute & evidence validation

- Mapping ID attributes with applicant (binding)

- Requirements of the use case/scenario (incl. security requirements)
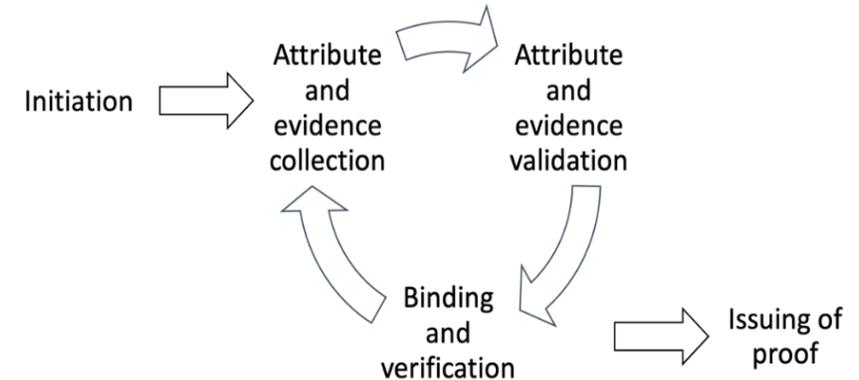
This is completed and "confronted" with the feedback from the questionnaires to vendors and TSPs.

The conclusions identify relevant information for the TS.
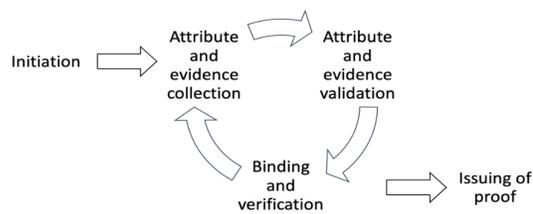
7

- **Data subjects : individuals, legal entities, individuals acting on behalf of legal entities**

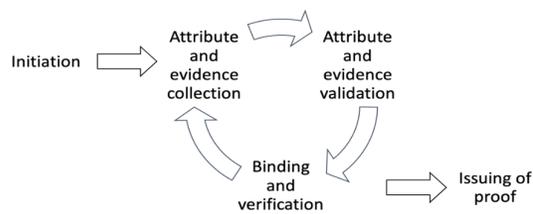- **Evidence that can be presented**

  - Identity documents (e.g. a passport) – eligible for 'authoritative evidence' status
  - eIDs – eligible for 'authoritative evidence' status
  - Digital certificate supporting an electronic signature – eligible for 'authoritative evidence' status
  - Trusted registers, proof of access information, other documents and attestations – eligible for 'supplementary evidence' status

- **Attribute presentation modes**

  - Collected as digital representation of an identity document (e.g. scan or photo of identity card or passport)
    - Captured remotely
    - Captured on site
  - Digitally extracted from an ID document (e.g. through (remote) access to the identity document chip)
  - Transmitted in purely digital form as an eID or a digital certificate;

- **Communication channels**

  - In the event of remote collection, e.g.
    - Security measures deployed to protect the integrity of the attribute transmission (e.g. end-to-end encryption);
    - ID attributes remotely presented by the applicant or obtained from a third party independent of the applicant (a "trust " service)
  - Constraints to be observed in case of on-site presentation (e.g. on the personnel)
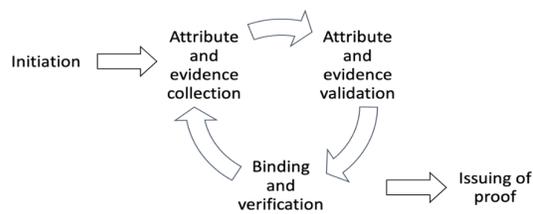
⩔ Determination that the evidence is genuine (issued by recognised independent/authoritative sources)

⩔ Determination that the ID attributes are valid (not expired, not revoked)

The following aspects are specified:

⩔ Description of customary security checks implemented, and security features verified in relation to attributes collected as digital representation of an ID document;

⩔ Description of customary security checks implemented in relation to 'purely digital' attributes (digitally extracted from ID documents or obtained via an eID process);

⩔ Description of other checks implemented if any (e.g. matching with other data, verification of expiry date, etc);

⩔ Description of external (governmental) sources queries if any;

⩔ Applicable technical standards if any.

- Mapping ID attributes with applicant or the attribute binding process can be defined as the steps taken to confirm, with a given degree of confidence, that the claimed identity credentials (for example those shown in a passport or ID card) which have been obtained and confirmed as valid are indeed those of the applicant and not of someone else

- Use cases

  - Face to face (on premise) physical presence of the applicant

  - Attended video interview (remote)

  - Unattended video interview (remote)

  - Use of eID, eSign/Seal, access to trusted sources

- **On premise 'physical presence'** is generally viewed as a benchmark for binding purposes ... but is rarely specified
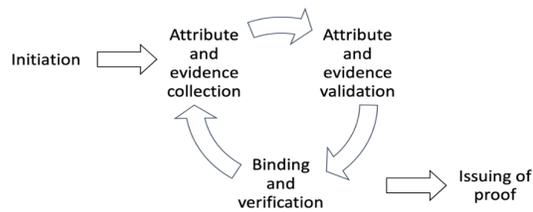
  This generates uncertainty as to the meaning of 'equivalent assurances in terms of reliability to physical presence'
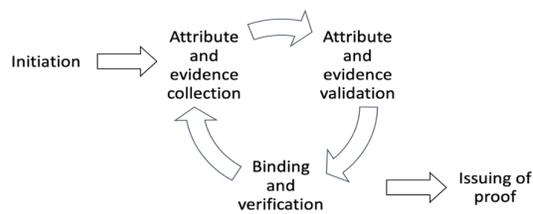
TS 119 461 - Technical Specifications
1 baseline level for diverse use cases

- Specify how identity proofing processes can be constructed by <u>combining</u> means to meet a <u>consistent level</u> of the identity proofing process <u>for each use-cases</u> (with physical on-site presence of the applicant, remote video interview, remote unattended process and automated process) i.e.;

  - means and technologies' combinations to be considered to reach a comparable confidence in the identity proofing outcome, by requiring fulfilment of general best practice requirements for the identity proofing process considered suitable for the currently defined trust service policies as defined by ETSI.

  - this level aims to protect against attacks up to level 'moderate'

- Annex A: Application to trust services as specified in ETSI EN and TS:

  - for issuance of NCP certificates

  - Application for issuance of QCP certificates

  - Application for ETSI EN 319 521 – registered delivery services

  - Application for ETSI TS 119 431-1 & CEN EN 419 241-1

- Annex B: Presentation of Attack scenarios and risks, covered or not-covered by the technical specification

Next steps and further information

▿ ETSI TS 119 461 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for identity proofing of trust service subjects : to be published **Q3 2021**

▿ Detail on project on web page: https://portal.etsi.org/STF/STFs/STF-HomePages/STF588

▿ ENISA "Analysis of Methods to carry out identity proofing remotely"

▿ ... and many other references in the ETSI TR 119 460 on identity proofing:
https://www.etsi.org/deliver/etsi_tr/119400_119499/119460/01.01.01_60/tr_119460v010101p.pdf

Many thanks!

Sylvie Lacroix