The Standards People

ETSI ESI
Best practice ID procedures for eIDAS Trust Services

Presented by: **Sylvie Lacroix**

For: **The 13th CA Day - Berlin**

22.09.2021

© ETSI 2021 – All rights reserved

STF 588 - rationale

- The 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 was not well-defined as no requirements were 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 was up to subjective judgement.
  - Concrete guidelines for remote identity proofing were needed to avoid cumbersome and expensive physical presence procedures when possible.
- TSPs tend to outsource identity-proofing processes to dedicated service providers
- The above needs became even more pressing under the eIDAS Regulation revision

(note: green text indicates evolution since CA Day 2020)

© ETSI 2021 – All rights reserved

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 specifies 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 security practices for different technological approaches and the use of these technologies in different use-cases, with a consistent '**baseline**' outcome level.

TS 119 461 finalised - published

© ETSI 2021 – All rights reserved

Policy and security requirements for trust service components providing identity proofing of trust service subjects (1/2)

- **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.

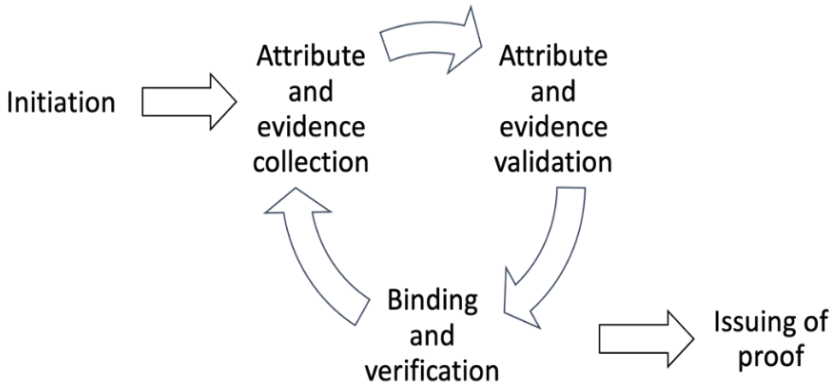
- Identity proofing is not an eIDAS trust service by itself, but a trust service component. An identity proofing service component may be used by many different trust services. Remains true under eIDAS 2.0
  - ETSI EN 319 403-1 auditable -> one audit that can be reused for different purposes

- Security requirements are provided to cover commonly faced risks falling in 4 main categories (Informative Annex on threats to IdP)
  - Falsified evidence : An applicant claims an incorrect identity using forged evidence.
  - Identity theft : An applicant uses valid evidence associated with another person.
  - Operational risks
  - Social risks (e.g. constraint)

© ETSI 2021 – All rights reserved

Policy and security requirements for trust service components providing identity proofing of trust service subjects (2/2)

- Security and policy requirements
  - Based on ETSI EN 319 401 – common requirements for all trust services (existing and new): operational risk assessment, policies and practices, service management and operation
  - Specific requirements for identity proofing - specify best practice requirements on how to use selected means to implement the tasks of attribute and evidence collection, attribute and evidence validation, and binding to applicant + initiation and result.
    - Includes specific requirements to support qualified trust services (does not mean the ID Proofing is a (Q)TS)



© ETSI 2021 – All rights reserved

TS 119 461 - Technical Specifications one baseline level for diverse use cases

- Specify how identity proofing processes can be constructed by combining means to meet a consistent level of the identity proofing process for each use-cases
- Use-cases (natural person, natural person representing legal person, legal person)
  - with physical on-site presence of the applicant,
  - attended remote (manual and hybrid manual/automated processes)
  - unattended remote (manual, hybrid, automated processes)
  - use of eID means
  - use of digital signature supported by digital certificate
- Consistent level:
  - 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 circumvent threats described in Annex and to provide a **high level of confidence on the proved identity**

© ETSI 2021 – All rights reserved

TS 119 461 - Technical Specifications Annexes

- Annex A: Application to use TS 119 461 in conjunction with trust services as specified in ETSI EN and TS:
  - EN 319 411-1 / -2 clauses 6.2 for issuance of certificates :
    - NCP certificates
    - QCP certificates
  - ETSI EN 319 521 – registered delivery services
  - ETSI TS 119 431-1 & CEN EN 419 241-1 (referring to CIR 2015/1502 level subst. & high) – remote creation of (qualified) signatures
- Annex B: Presentation of Attack scenarios and Threats and how they are covered by the technical specification

© ETSI 2021 – All rights reserved

TS 119 461 and eIDAS trust services

- eIDAS I trust services: ETSI TS 119 461 (incl. possibility to rely on eID means susbt. & high) is written for this purpose
- eIDAS 2.0 trust services: ETSI TS 119 461 still applicable
  - Art 24 - verify the identity on the basis of:
    - notified eID means Substantial or High (no more physical presence for issuance)
    - qualified electronic Attestation of Attribute (eAA) or certificate of a QES or QSeal
    - identification methods which ensure the identification of the natural person with **a high level of confidence** (confirmed by CAB)
    - Physical presence
  - TS 119 461 is already **designed** for **a high level of confidence** on the proved identity and can easily consider identity proofing for eAA issuance and check for eID means notification

© ETSI 2021 – All rights reserved

TS 119 461 and eIDAS

- Expected difficulties with Regulation (EU) No 2019/1157 strengthens the security of identity cards
  - No possibility to access to the citizen's picture stored in the eID chip -> counter-balanced by the availability of the eID wallet (interface to QTSP foreseen)
  - Access to authentic sources for QTSP issuing EAA
- Open to changes if perceived necessary for applicability to eIDAS 2.0 requirement for "high" identity proofing and verification for eIDs

© ETSI 2021 – All rights reserved

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
  https://www.etsi.org/deliver/etsi_ts/119400_119499/119461/01.01.01_60/ts_119461v010101p.pdf
- 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

© ETSI 2021 – All rights reserved

Many thanks!

Sylvie Lacroix

© ETSI 2021 – All rights reserved