Standard on Identity proofing

Context & challenges

ETSI TS 119 461 - Rationales – Existing - Future

Sylvie Lacroix SEALED
Trust Services Architects

ENISA – ETSI workshop – 03.05.2022

Identity proofing standard in context

How

Driving rules

set objectives

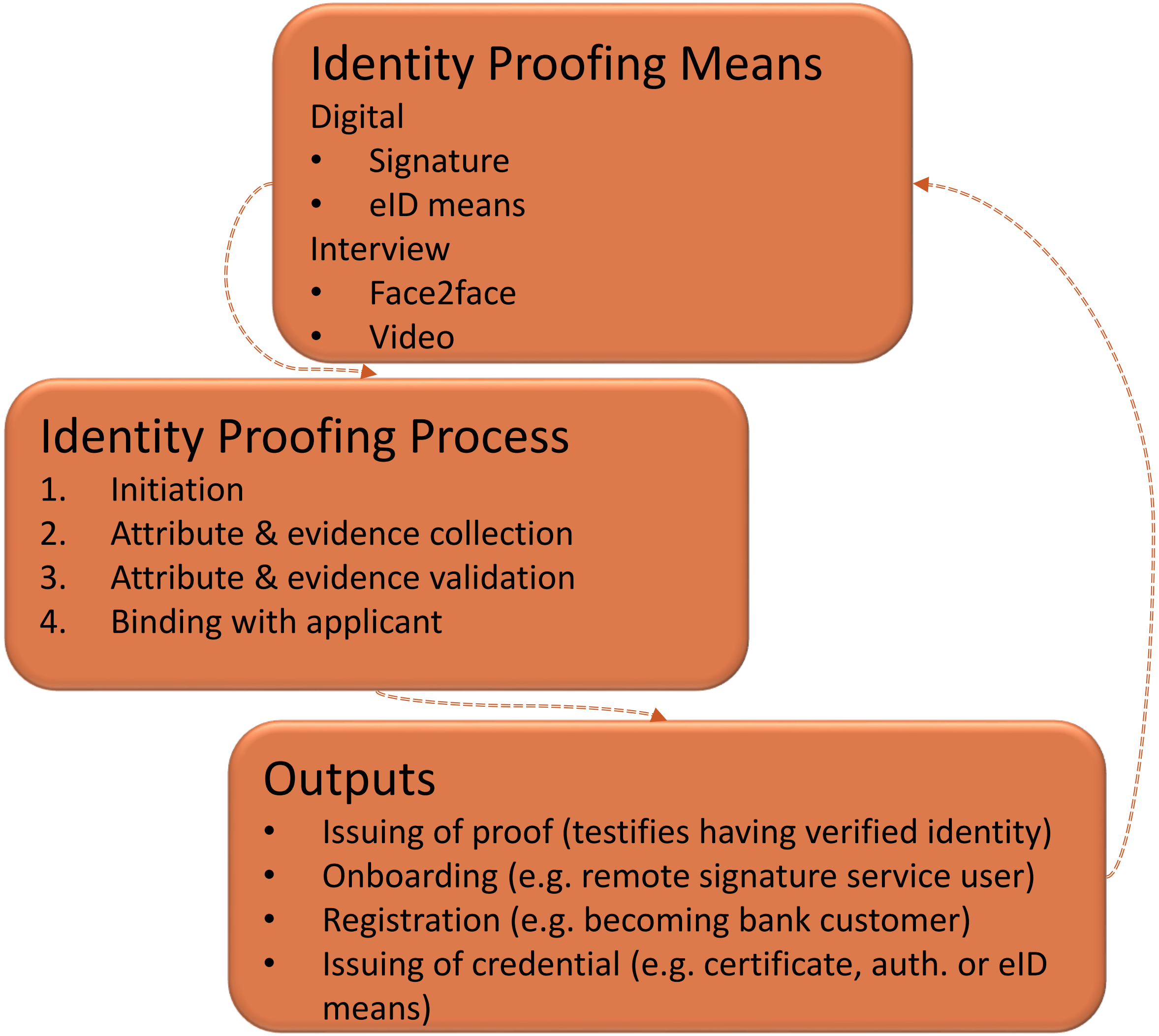
e.g. eIDAS trust services, AML regulations, eIDAS eID means

Standards

set controls, reqs & best practices to reach objectives

- Measurable
- Auditable

What



Identity Proofing Means

Digital

- Signature
- eID means

Interview

- Face2face
- Video

Identity Proofing Process

1. Initiation
2. Attribute & evidence collection
3. Attribute & evidence validation
4. Binding with applicant

Outputs

- Issuing of proof (testifies having verified identity)
- Onboarding (e.g. remote signature service user)
- Registration (e.g. becoming bank customer)
- Issuing of credential (e.g. certificate, auth. or eID means)

Identity proofing standard challenges

Diversity of driving rules

Need for 'best practices' addressing commonly faced risks, so defining a 'good' level of security

- As stand alone as possible
- As independent as possible (i.e. not too context based, but **contextualizable**, i.e. further specified / customised for a certain context)

… still scoped, by driving rules "generic / specific" balance

Lifecycle

standard edition vs technology evolution

Need for active references

'Componentisation'

IDP is a component of broader activity

e.g. part of TSP issuing certificate tasks

ID.Proofing can be outsourced … but a standard cannot put requirements on component not in control of the conforming party

Need for securing interfaces, smooth articulation of Id.Proofing consumer specifications vs IPSP specifications (e.g. CA / IPSP)

- Method to address (audit) common / shared elements; GDPR, GTC & practice statements, service operation (ISO27K)
- Consumer of IDP must be able to specify / shift requirements on IPSP
- Ensure all objectives are covered here or there (e.g. 'Refresh' conditions on consumer side)
- Audit 'portability'

ETSI TS 119 461

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

TECHNICAL SPECIFICATION

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

Standard

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

ETSI is a European Standards Organization (ESO) dealing with telecommunications, broadcasting and other electronic communications networks and services. ETSI role includes **supporting European regulations and legislation** through the creation of Harmonised European Standards. Only standards developed by the three ESOs (CEN, CENELEC and ETSI) are recognized as European Standards (ENs).

Regulation 910/2014/EU of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (eIDAS)

Driving rules

Based on a survey of 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)

eIDAS Reg. (EU) 910/2014 – Trust services

eIDAS 2 pillars:

- Trust services
- Issuance of eID Means by member states, under 3 levels: low, substantial or high

eIDAS 2.0 EU Wallet for eIdentification & signature: an eID means of level High

Closed list of trust services:

- Creation, verification, and validation of **electronic signatures**, electronic **seals** or electronic time stamps, electronic registered delivery services and certificates related to those services;
- Creation, verification and validation of certificates for website authentication;
- The preservation of electronic signatures, seals or certificates related to those services;
- Creation, verification, and validation of **electronic attestations of attributes** and certificates related to those services

eIDAS 2.0

- Electronic archiving of electronic documents;
- Management of remote electronic signature and seal creation devices
- The recording of electronic data into an electronic ledger

Identity proofing is not an eIDAS trust service by itself but a component of such services.

In particular, eIDAS currently specifies 4 ways to verify the identity of subjects to whom a qualified certificate is issued:

- with the physical presence of the applicant,
- by means of an eID means (high/substantial),
- by means of a QC supporting a qualified signature,
- by other identification methods recognized at national level which provide equivalent assurance in terms of reliability to physical presence

eIDAS 2.0 (or which ensure the identification of the natural person with a high level of confidence)

Driving rules for TS 119 461

ETSI TS 119 461 objectives

- ✓ A consistent level of confidence for different 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 with certificate

Each use-case ‘equivalent’ thanks to best practice security and policy requirements & combination of means to implement the Id. Proofing Process

- ✓ Auditable (concrete, measurable requirements to be used by CABs)
- ✓ Includes requirements and controls on operating the service

Ref. to 319 401 (base for all services)

- ✓ High level of confidence on the proved identity (best practices based)
- ✓ Protect against typical attacks (in annex, presentation of Attack scenarios and Threats and how they are covered by the technical specification)
  - 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. coerced action)

References to specific standards (e.g. for face biometrics in ISO/IEC 19795-1)

ETSI TS 119 461 – roadmap

ETSI TS 119 461 still applicable for eIDAS 2.0 trust services

Art 24 - verify the identity on the basis of:

- notified eID means Substantial or High (physical presence is no longer mentioned)
- 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 (as 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

eIDAS (1.0 & 2.0) requirements for identity proofing for eIDs means level high / substantial issuance

- Currently TS 119 461 claims compliance to level substantial (annex demonstrating compliance with EN 419 241-2 referring to CIR 2015/1502 level substantial)
  - For level high, similar exercise can be done to highlight potential gaps to be fulfilled for a contextualised policy building on TS 119 461
- A specific TS can be produced for compliance with CIR 2015/1502, building on TS 119 461 with additional / customised requirements

Contextualisation. Context based options are pointed in the TS
(the TS could also, in addition, specify the framework for the definition of other policies like other TS)