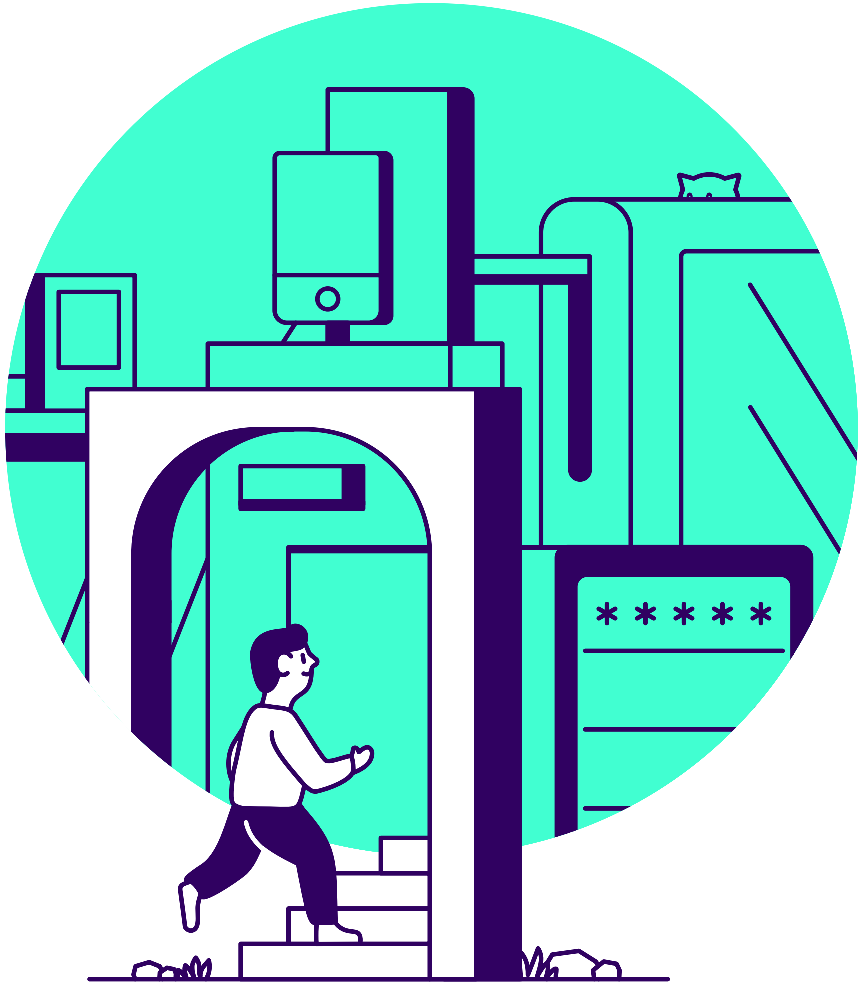
Signicat

Identity proofing harmonization

Jon Ølnes
Tribe Lead Sign and Trust Services
Signicat
ETSI TS 119 461 editor

CA Day, Heraklion, 2024.09.26



signicat.com

First there was chaos

Three main areas for identity proofing

1. Issuing of qualified certificates
   - Other means recognised at national level to provide equivalent assurance to physical presence (eIDAS v1 Article 24.1(d))
2. Issuing of eID
   - Issuing done at national level with identification done according to national rules, then maybe doing an eIDAS notification
3. Financial services
   - remote or electronic identification process regulated, recognised, approved or accepted by the relevant national authorities (AMLD5 Article 13.1(a))

Signicat

The current ETSI standard (1)

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

- **ETSI TS 119 461 published July 2021**
- **One 'baseline' level («sort of» 'substantial')**

- **Update covering eIDAS v2 in progress**
  - Target approval by ETSI TC ESI in November

- **Authoritative (identity) evidence (natural person):**
  - Digital identity document (ICAO eMRTD)
  - Physical identity document (passport or ID card)
  - eID for authentication
  - Certificate of a digital signature
- **Supplementary evidence:**
  - Trusted register
  - Documents and attestations (including attribute attestations)
  - Proof of access (e.g. to bank account)
- **Authoritative source**
  - A source trusted for identity information
  - Can be authoritative and supplementary evidence

The current ETSI standard (2)

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

Use case requirements for:

- Physical presence
- Attended remote (with identity document)
  - "Physical presence at a distance"
- Unattended remote (with identity document)
- eID for authentication
- Digital signature with certificate

Natural person
Legal person
Natural person representing legal person

A baseline standard

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

ETSI World Class Standards

Onboarding to trust services

EBA EUROPEAN BANKING AUTHORITY

Guidelines on the use of Remote Customer Onboarding

cen

Onboarding to European Digital Identity Wallet (and other eID onboarding?)

Signicat

Onboarding is more than identity proofing

Remote identity proofing using identity documents

- Remote capture of facial image requires real-time video – not photo only

- Fully automated remote process requires digital identity document (eMRTD)
  - Document verification by validating signature on document
  - Face biometrics against high resolution reference picture from document

- With scanning of physical identity document, a manual step is required
  - For verification of document and binding to applicant
  - Combined manual and machine learning technology recommended, manual only allowed
  - Automated analysis of document features, face biometrics, plus manual judgement
  - Physical identity document scanning requires real-time video – not photo only

- Server-side verification, including server-side biometrics
- ETSI does not standardize technology for biometrics etc.

eIDAS Article 24.1 changes from v1 to v2

eIDAS v1	eIDAS v2
Scope: Issuing of qualified certificates	Scope: Issuing of qualified certificates and QEAA
a) Physical presence	d) Physical presence with appropriate evidence and procedures, in accordance with national law
b) eID means at level ‘substantial’ or ‘high’ issued based on physical presence	a) EUDIW or other notified eID at level ‘high’
c) Certificate of qualified signature with certificate issued based on a or b	b) Certificate of qualified signature with certificate issued based on a, c, or d
d) Other identification means providing equivalent assurance to physical presence and approved at national level, assessed by conformity assessment body	c) Other identification means ensuring a high level of confidence, assessed by conformity assement body
(No implementing act)	By 21.05.2025, the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the verification of identity and attributes

European harmonisation

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

?

What’s new in ETSI TS 119 461 revised?

The fully automated remote use case (digital document, biometrics) is kept for ‘extended’, and should be allowed for the EUDIW.

My opinion

- New level ‘extended’ («sort of» ‘high’)
- Align with latest version of ETSI EN 319 401
- Requirements on risk intelligence to adapt services
  - Risk landscape changing rapidly, providers must prove that they keep pace
  - Too specific requirements in standard today means standard obsolete tomorrow
- Tightening some requirements and some updates
- Supplementary evidence “documents and attestations” can be (Q)EAA
- Use cases for ‘baseline’ generally good also for ‘extended’
  - With the tightening that also applies to ‘baseline’
  - Exception: eID assurance level – ‘substantial’ versus ‘high’
  - Exception: Unattended remote with manual only processing not for ‘extended’
- Added Annex C on use cases specifically for eIDAS qualified
  - Both eIDAS v1 and v2
  - Article 51 (4): Existing QTSPs have until May 2026 to comply with new Article 24.1

From ‘substantial’ to Q-certificate (and to eID ‘high’?)

eIDAS v2 Recital (74) on Q-cert and QEAA

It should be possible to combine methods to provide an appropriate basis for the verification of the identity of the person to whom the qualified certificate or a qualified electronic attestation of attributes is issued. It should be possible for such a combination to include reliance on electronic identification means which meet the requirements of assurance level substantial in combination with other means of identity verification.

eIDAS v2 recital (28) on the EUDIW

Electronic identification means issued at assurance level substantial should be relied upon only where harmonised technical specifications and procedures using electronic identification means issued at assurance level substantial in combination with supplementary means of identity verification will allow the fulfilment of the requirements set out in this Regulation as regards assurance level high.

Updated ETSI TS 119 461 proposal is eID ‘substantial’ plus one of:

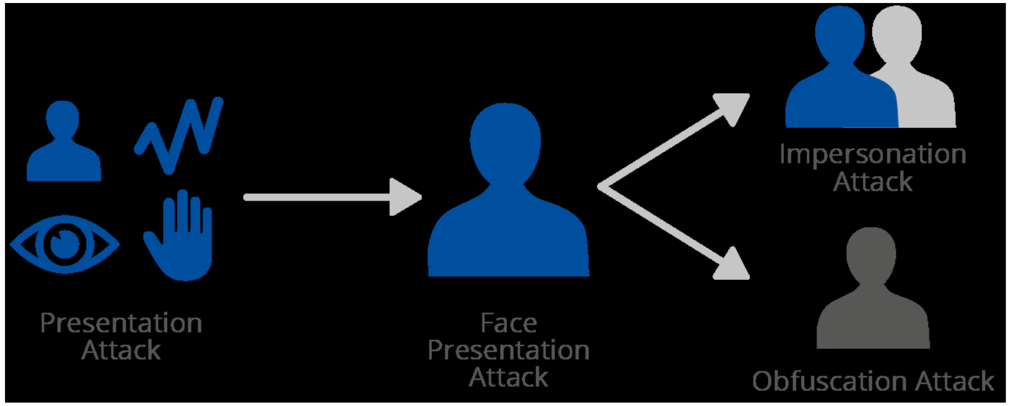
1. Remote validation of a (digital or physical) document showing the same identity
   - eID substantial + document
2. Face image capture and biometrics against existing reference photo linked to same identity
   - eID substantial + show your face

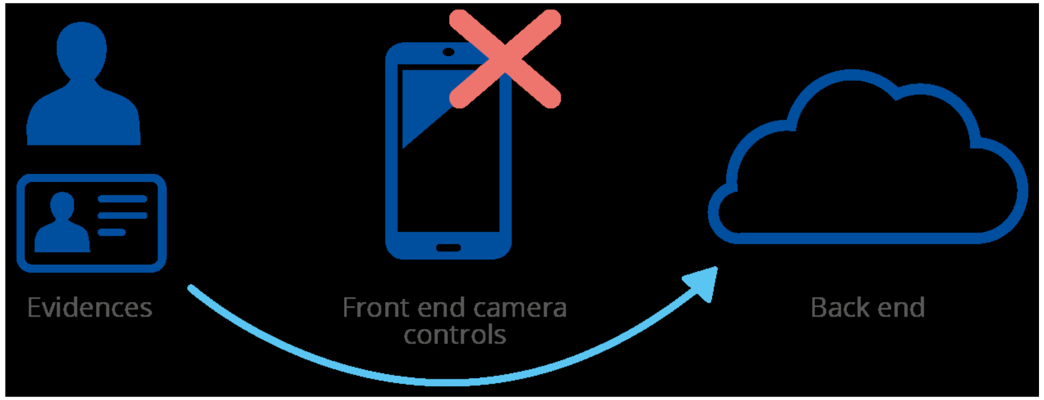
What about?

- eID substantial + QES or QEAA?)
- Other – many methods can be envisaged

Presentation and injection attacks

- Remote identification with identity documents and selfie-video is done from the user's equipment
- **Presentation attack: spoof the video recording**
  - Wearing a mask, showing a video, deep fake, manipulating recording
- **Injection attack: inject a video stream bypassing the camera**
  - Recorded video or deep fake of document or selfie-video





Signicat

CEN standardisation work

- **CEN TC 224 Personal identification and related personal devices**
  - Guidelines for the onboarding of user personal identification data within European Digital Identity Wallets (started)
  - Biometric data injection attack detection (soon, referred from ETSI TS 119 461)
  - European biometric requirements (in progress)

CEN TC 224 WG 18 and WG 20

Note also ENISA reports on remote identity proofing

ISO standards

- ISO/IEC 30107-3:2023: Information technology -- Biometric presentation attack detection (multi-part)
- ISO/IEC 19795-1:2021: Information technology - Biometric performance testing and reporting (multi-part)
- ISO/IEC 19989-3:2020: Information security - Criteria and methodology for security evaluation of biometric systems (multi-part)

- And a lot more…..
- Many referred from ETSI TS 119 461

Compliance – and where we are heading

- **ETSI TS 119 461 CAB conformity assessments are common**
  - New, explicit statement of use cases supported is required

- **New version has a clear indication for the following direction:**
  - Establish an EUCC scheme for identity proofing
  - Or at least for core parts – biometric processing, presentation attack detection/prevention, injection attack detection/prevention
  - Establish an EU accreditation system for evaluators (labs)

- **When this is done, require the scheme and external lab tests**
- **Future version of the standard – premature at this time**

My opinion

Signicat

Signicat

Please reach out for questions!

jon.olnes@signicat.com
+47 478 46 094