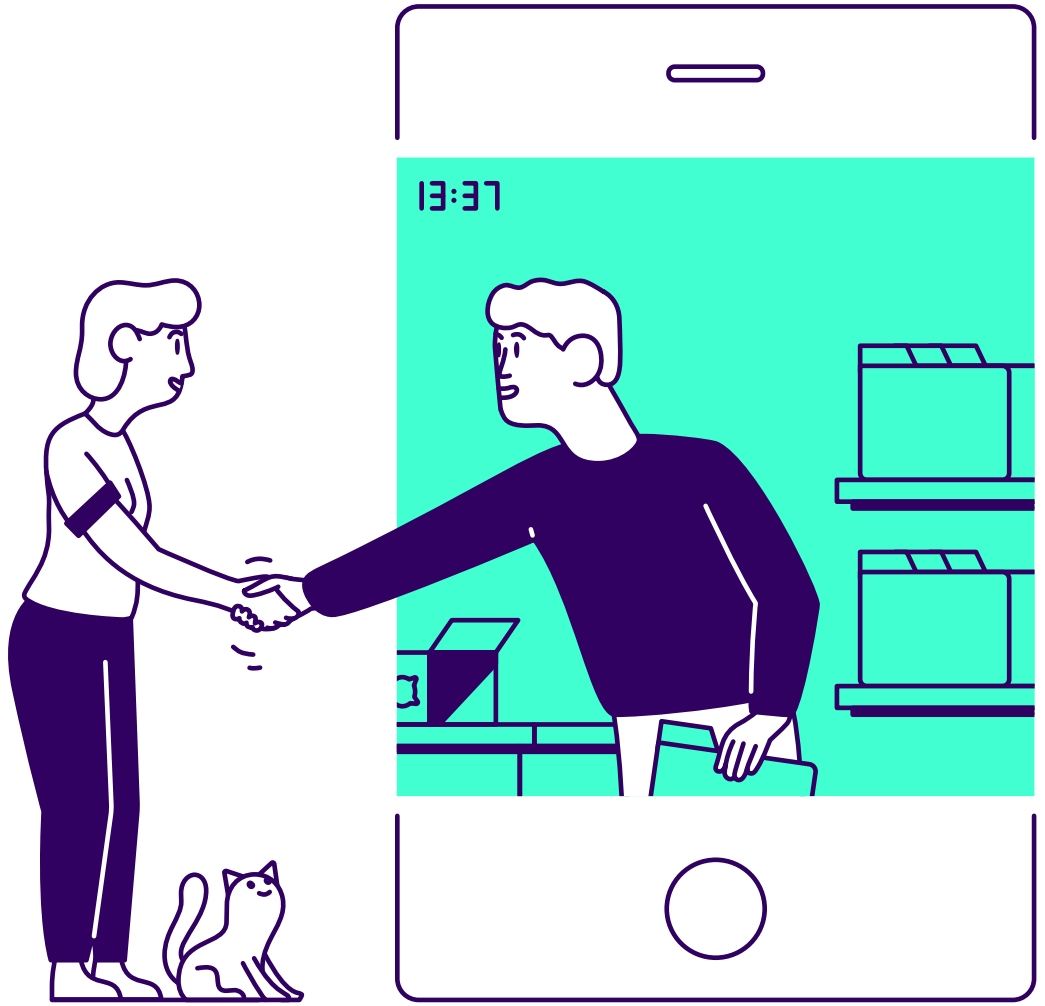
Harmonizing identity proofing for Europe

Jon Ølnes, Tribe Lead signing and trust services, Signicat
ETSI TS 119 461 editor/rapporteur

Norstella, Oslo, 4 September 2025



Signicat webinar 10 September

Signicat

Harmonising Identity Proofing Across Europe: The Impact of the New ETSI Standard

Register here

- 10 September 2025 at 11:00 CET
- English
- Webinar

First there was chaos

Three main areas for identity proofing and onboarding:

1. **Issuing of qualified certificates**

   Other means recognised at national level to provide equivalent assurance to physical presence (eIDAS v1)

2. **Issuing of eID**

   Issuing done at national level with identification done according to national rules

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 standardization process

Harmonization requires standardization

Get it in place for eIDAS v1

1. Get work item approved in ETSI TC ESI
2. Apply for EU funding
3. Establish an ETSI Specialist Task Force (STF) to fast track
   - Group of partly paid experts reporting to ESI
4. Write standard and get it approved, V1.1.1 July 2021
5. Promote, lobby, get it used

Then came eIDAS v2.....

6. New work item approval for revision
7. Revise with a large group of people involved
8. Get standard approved, V2.1.1 February 2025
9. Promote, lobby, get it used

The ETSI standard

Formally for identity proofing for trust services – certificates for signing etc.

ETSI TS 119 461 v1.1.1
(July 2021)

One ‘baseline’ level
(sort of eID ‘substantial’)

ETSI TS 119 461 v2.1.1
(Feb 2025)

Covers eIDAS v2
Adds ‘extended’ level
(sort of eID ‘high’)

Signicat provides the editor for both versions

Signicat

Use cases – ways of identity proofing

ETSI TS 119 461 V2.1.1 (2025-02)

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

Use case requirements

- 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 a legal person

Signicat

Use cases – ways of identity proofing

Authoritative evidence (identity of person present)

- Digital identity document (ICAO eMRTD from NFC chip)
- 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 (identity information of person)

- A source trusted for identity information
- Can be authoritative or supplementary evidence

Signicat

A baseline standard

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?)

If you follow the standard and are audited for that, you may (eventually) be good for identity proofing for all of these in all EU/EEA countries

NB: Onboarding is more than identity proofing

Signicat

Harmonized identity proofing for trust services

1c. By 21 May 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 in accordance with paragraphs 1, 1a and 1b of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).';

Official Journal of the European Union
EN
L series

2025/1566
30.7.2025

COMMISSION IMPLEMENTING REGULATION (EU) 2025/1566

of 29 July 2025

laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards reference standards for the verification of the identity and attributes of the person to whom the qualified certificate or the qualified electronic attestation of attributes is to be issued

(2) In order to ensure equal treatment and ability to trust the result of the verification process, verifications should be carried out in an equivalent manner by all qualified trust service providers when issuing a qualified certificate or a qualified electronic attestation of attributes. In accordance with the objectives of Regulation (EU) No 910/2014, a

Article 2

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

This Regulation shall apply from 19 August 2027.

ANNEX

Reference standard for the verification of the identity and attributes of persons to whom a qualified certificate or qualified electronic attestation of attributes is to be issued

The standard ETSI TS 119 461 V2.1.1 (2025-02) for conformance with Annex C clause C.3 applies with the following adaptations:

- eIDAS v2 Article 24 (1c) and its implementing Regulation
- This is **the only way** to do identity proofing
- Actors get 2 years to adjust
- **ETSI TS 119 461 shall be used** – a few extra requirements

Harmonized identity proofing for eID/EUDI Wallet

TECHNICAL SPECIFICATION
SPÉCIFICATION TECHNIQUE
TECHNISCHE SPEZIFIKATION

FINAL DRAFT
prCEN/TS 18098

July 2025

ICS

English Version

Guidelines for the onboarding of user personal identification data within European Digital Identity Wallets

8.3.3.6.1 REQ

For the identity verification, the requirements as defined in ETSI TS 119 461 §9.1 for LoIP "Extended" shall be fulfilled.

8.3.3.9.3 C-REQ

Condition: identity verification is carried out remotely using an identity document.

The identity verification shall comply with the requirements as defined in ETSI TS 119 461 §8.3.2.

NOTE 1 This requirement implies that identity documents with a chip are used for the identity verification.

The binding to applicant shall be done via a hybrid process using automated face biometrics and manual verification as defined in ETSI TS 119 461 §8.4.3 and §8.4.4 for LoIP "Extended".

NOTE 1 It means that the face of the applicant is compared to the reference portrait extracted from his identity document using both manual verification and biometric comparison.

- ✓ CEN standard in final draft version
- ✓ Identity proofing refers ETSI TS 119 461 as it is
- ✓ Tightening for remote use of identity documents – only digital document (from NFC chip), combined manual and biometric check against face photo

EBA and its guidelines

A single set of rules for all banking institutions in the EU

Basis for the creation of **an EU single market** in the banking sector.

EBA contributes to the **"European Single Rulebook"** in banking through binding Technical Standards and Guidelines

EBA Guidelines are **not legally binding, but** supervisory authorities and financial institutions must make every effort to comply. Supervisory authorities must give reasons if they intend not to comply

AML Regulation, EBA Guidelines Remote Onboarding

- EBA Guidelines refer ETSI TS 119 461
- Actors audited against ETSI for EBA compliance
- EBA Guidelines remain with AMLR(?)

EBA | EUROPEAN BANKING AUTHORITY

Final Report

Guidelines on the use of Remote Customer Onboarding Solutions under Article 13(1) of Directive (EU) 2015/849

In respect of Guideline 4.3 and Guideline 4.4, respondents asked the EBA to align the draft with ETSI TS 119 461 Standards. The EBA agreed to align the draft with ETSI standards where possible and updated the guidelines accordingly.

2024/1624

REGULATION (EU) 2024/1624 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 31 May 2024

on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing

Obliged entities shall obtain the information, documents and data necessary for the verification of the identity of the customer and of any person purporting to act on their behalf through either of the lowing means:

the submission of an identity document, passport or equivalent and, where relevant, the acquisition of information from reliable and independent sources, whether accessed directly or provided by the customer;

the use of electronic identification means which meet the requirements of Regulation (EU) No 910/2014 with regard to the assurance levels 'substantial' or 'high' and relevant qualified trust services as set out in that Regulation.

42. Another example relates to the provision in Article 22(6) of the AMLR, which could be read as suggesting that only tools and solutions that are eIDAS-compliant can be used to verify the identity of customers in an online context. Electronic identities are not mandatory for individuals or for legal persons under Regulation (EU) No 910/2014 (the eIDAS Regulation). What is more, certain customers may be unable to obtain electronic identities, for example because they are not resident in the EU, or because they are disadvantaged or belong to other vulnerable groups. Restricting online verification of identity to e-IDAS-compliant solutions only could therefore exclude certain customers from access to online financial services. To address this, the EBA proposes that eIDAS tools and solutions be mandatory only to the extent that an eIDAS-compliant electronic identity it is available and can be reasonably expected to be provided by the customer. Obliged entities should use alternative, similarly robust means of online verification, in line with the EBA guidelines on remote onboarding[2], where customers cannot provide eIDAS-compliant electronic identity.

Some highlights of ETSI TS 119 461

- Remote identity proofing using identity document
  - Remote capture of facial image of applicant requires video sequence – photo not sufficient
  - Fully automated remote requires digital identity document – validate signature on document, face biometrics against high resolution reference picture from document
  - Physical identity document scanning requires real-time video sequence – photo not sufficient
  - Manual validation of physical document allowed, combined manual and machine learning technology recommended
    - Attended remote: Manual only validation OK. Unattended remote: Manual only not allowed for ‘extended’
  - Requirements for both manual face verification and automated face biometrics
    - Attended remote: Manual only validation OK. Unattended remote: Manual only not allowed for ‘extended’
  - Server-side processing, including biometrics – user device only for evidence capture
- Requirements for manual processes including physical presence
  - Training, face comparison, document validation

- Close co-operation with the EU Cybersecurity Agency, ENISA, who has published two reports
- Consensus in ETSI by several national security authorities and by the industry

Signicat

What's new in ETSI TS 119 461 revised?

- New level 'extended' («sort of» 'high')
- Align with latest version of ETSI EN 319 401 (implies ISO/IEC 27002:2022)
- 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

Signicat

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.

ETSI TS 119 461 v2.1.1 states eID ‘substantial’ plus one of:

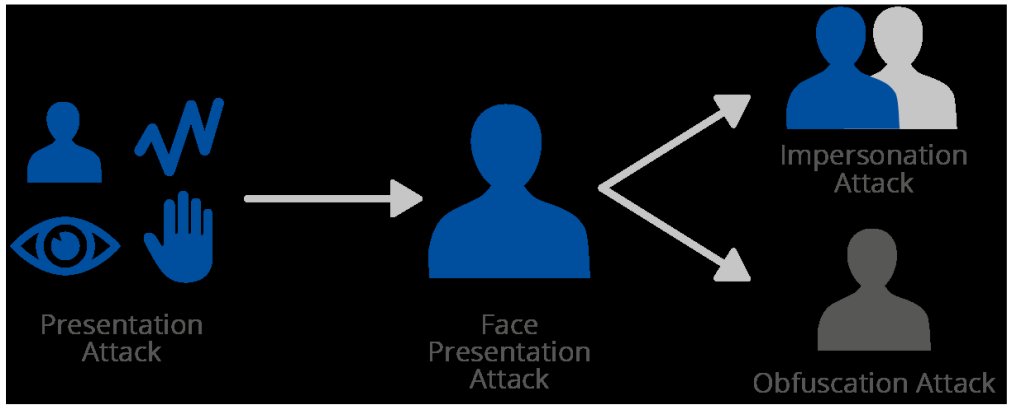
1. Full identity proofing with identity document (any use case) to ‘extended’
   - eID substantial + full identity validation
   - Strictly speaking, the eID is not needed, but see next…..
2. Face image capture and biometrics against existing reference photo linked to same identity
   - eID substantial + show your face
   - Face and identity captured in the full identity proofing

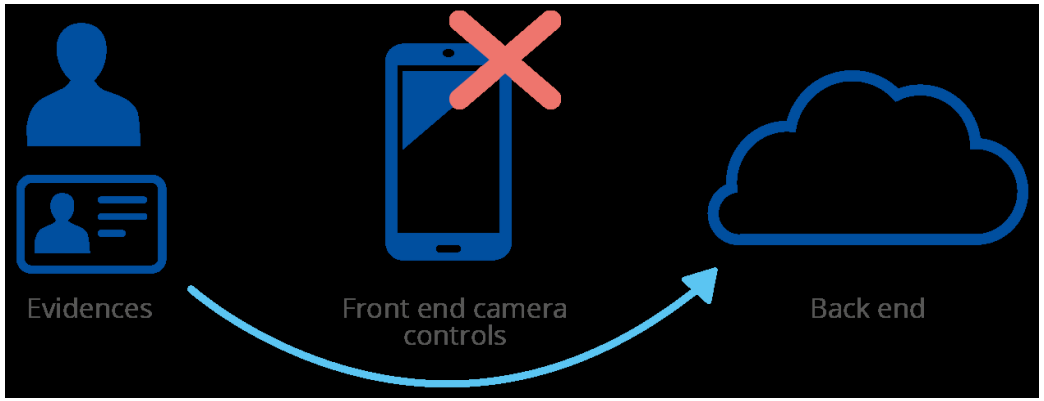
CEN aligns with 1 for TS 18098 onboarding to the EUDI Wallet

Signicat

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

The difficult issues in the standard revision

- **Most issues were on remote use of identity documents**

- **Mandate lab testing for presentation and injection attack?**
  - Labs and security authorities pro, much of «the industry» against
  - Compromise: mandated, but not before end of 2026
  - A bi-annual test is fine but the important is that the provider keeps pace
- **Allow fully automated for 'extended' – conclusion: allowed**
  - Some security authorities wanted a human eye on everything
  - To be seen if this will be allowed for the EUDI Wallet onboarding
- **The eID 'substantial' to Q-certificate and QEAA issue**
- **Requirements for biometric "precision"**
  - Specific values will be outdated, how to formulate?

Signicat

CEN standardisation work

- **CEN TC 224 Personal identification and related personal devices**
  - prCEN TS 18098: Guidelines for the onboarding of user personal identification data within European Digital Identity Wallets (in progress)
  - CEN TS 18099: Biometric data injection attack detection (referred from 119 461)
  - European biometric requirements (in progress)

CEN TC 224 WG 18 and WG 20

Note also ENISA reports on remote identity proofing

Signicat

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

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

Signicat

Compliance – and where we are heading

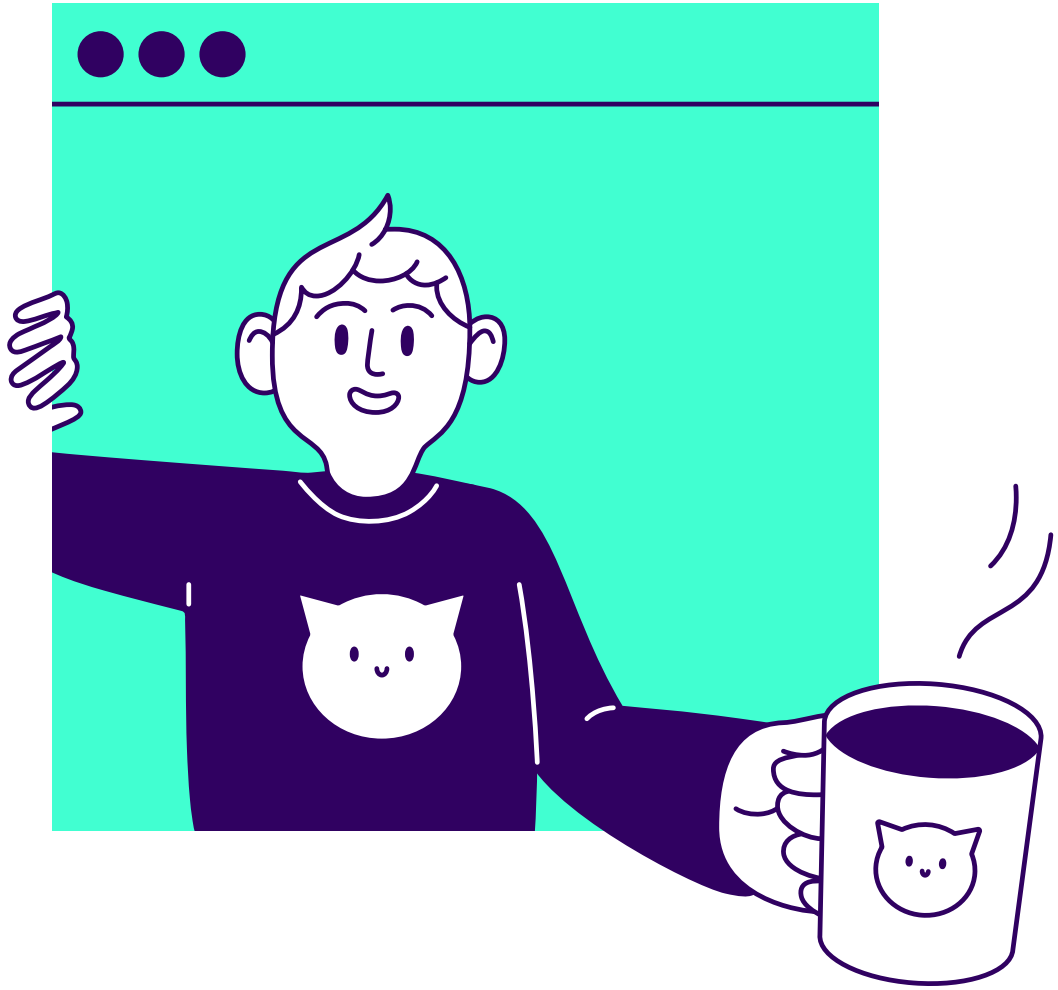
- **ETSI TS 119 461 CAB conformity assessments are common**
  - New, explicit statement of use cases supported is required
- **New version has a clear indication for the following direction:**
  - Establish an EUCC scheme for identity proofing
  - Or at least for core parts – biometric processing, presentation attack detection/prevention, injection attack detection/prevention
  - Establish an EU accreditation system for evaluators (labs)

Norway: Digdir seems interested in adopting the standard for issuing of eID
We should approach Nkom to ask for adoption even before eIDAS v2 is in force

Signicat

Signicat

Please reach out for questions!



A trusted digital world

www.signicat.com