Remote identification under eIDAS

CA-Day, Vienna/online, 2023.10.13

Jon Ølnes, Signicat

Disclaimer

Please note that this presentation is for information purposes only, and that Signicat has no obligation to pursue any course of business outlined in this presentation or to develop or release any functionality mentioned in this presentation.

The future strategy and possible future developments by Signicat are subject to change and may be changed by Signicat at any time for any reason without notice. This document is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. Signicat assumes no responsibility for errors or omissions in this document.

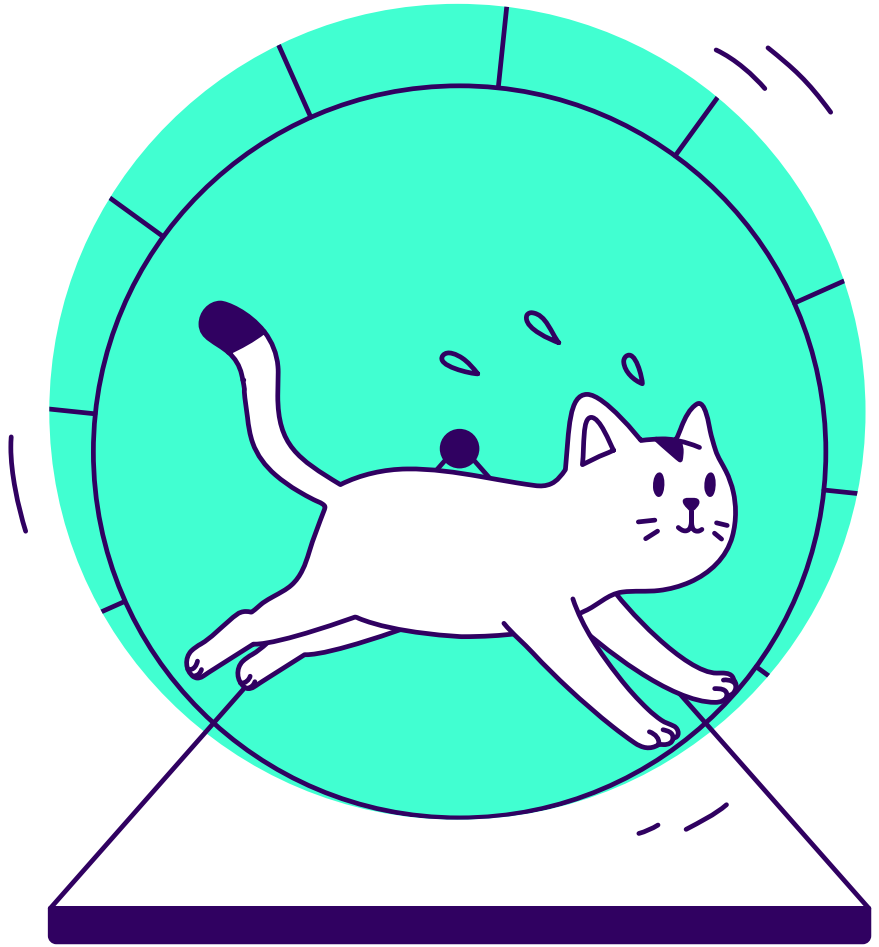
First there was chaos

Three main areas for remote identification

1. Issuing of qualified certificates
   - Other means recognised at national level to provide equivalent assurance to physical presence (eIDAS 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

From chaos to harmonisation Part 1: Legal



Trust services 1:
Revised eIDAS Article 24.1 and Article 44

- **NOTE: Trilogue negotiations will settle the final version**

Bar is raised! Current eIDAS allows 'substantial' based on physcial presence

Article 24.1: Verification of identity for issuing a qualified certificate or qualified attribute attestation shall be:

a) EUDI Wallet or other notified electronic identification means at assurance level 'high'.
b) Certificate of qualified electronic signature or qualified electronic seal (possibly also qualified attestation of attributes).
c) Other identification methods which ensure the identification of the person with a high level of confidence;
d) Physical presence by appropriate procedures and in accordance with national laws.

Not just «physical presence» as today, there will be requirements

Current eIDAS states equivalent assurance to physical presence

«Other» means in practice remote identity proofing by use of identity documents

More important to identify correct sender than correct receiver

Article 44 on qualified electronic registered delivery services

- Ensure identification of sender with a high level of confidence
- Ensure identification of reciever

Signicat

Trust services 2: The new Article 24.1a

- By 12 months after the entry into force of this Regulation, the Commission shall by means of implementing acts, set out **minimum technical specifications, standards and procedures with respect to the verification of identity** and attributes in accordance with paragraph 1, points a, b, c, and d

- "Minimum technical specifications" means a Member State can require more, but not less
- If a Member State does not specify more, then the minimum requirements apply

- Will strongly contribute to harmonization!

- [A goal for the revised version of ETSI TS 119 461 is suitability for reference from this Article]

Signicat

Financial services: AML regulation and EBA Guidelines

- **Digital finance strategy of EU sets direction**
- **AML Regulation (common EU law, 2025?) expected to have rules (implementing acts?) harmonising remote identity proofing and onboarding**

- **EBA (European Banking Authority) guidelines on the use of remote customer onboarding solutions (published November 2022)**
  - EBA guidelines are normative but do not overrule national law

Signicat

Electronic identification, eID:
European Digital Identity Wallet onboarding

- **NOTE: Trilogue negotiations will settle the final version**

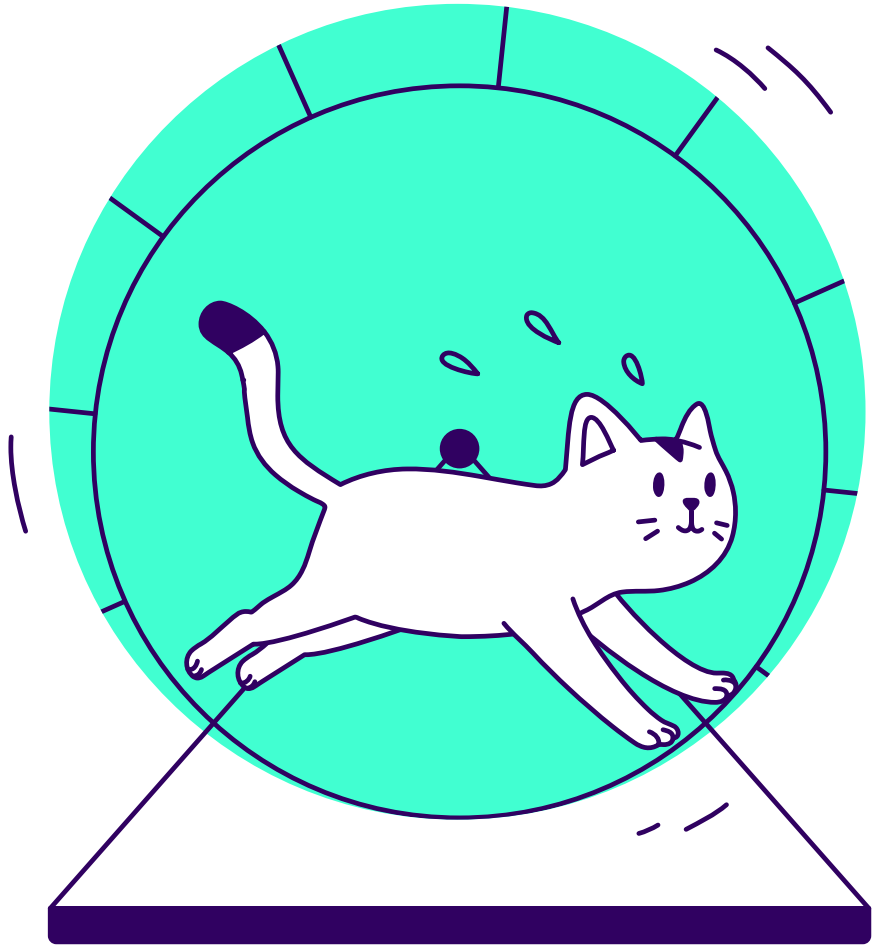
- EUDI Wallet shall be issued according to notified scheme at level ‘high’
- Means CIR (EU) 2015/1502 on assurance levels apply

- Council proposal Article 11a:
  - Identity proofing can be done by existing eID ‘high’ or eID ‘substantial’ plus “something”
  - Implementing act on how to do this

- Use of remote onboarding by use of identity documents not mentioned (“other means”)

Signicat

From chaos to harmonisation Part 2: Standards



Trust services and the ETSI standard

- Harmonization requires common reference
- ETSI TS 119 461 published July 2021
- Now under revision due to eIDAS v2

Use case requirements for:

- Physical presence
- Attended remote ("physical presence at a distance" with identity document)
- Unattended remote (with identity document)
  - Manual evaluation
  - Hybrid manual and automated evaluation
  - Fully automated (only with digital document from NFC chip)
- eID for authentication
- Digital signature with certificate
- Possible new: Use of attribute attestations
- Possible new: Getting from 'baseline' to 'extended'

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?)

Signicat

Onboarding is more than identity proofing

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 (new draft)
  - Biometric requirements (existing and in progress)

CEN TC 224 WG 18 and WG 20

Note also ENISA reports on remote identity proofing

Signicat

ISO standards

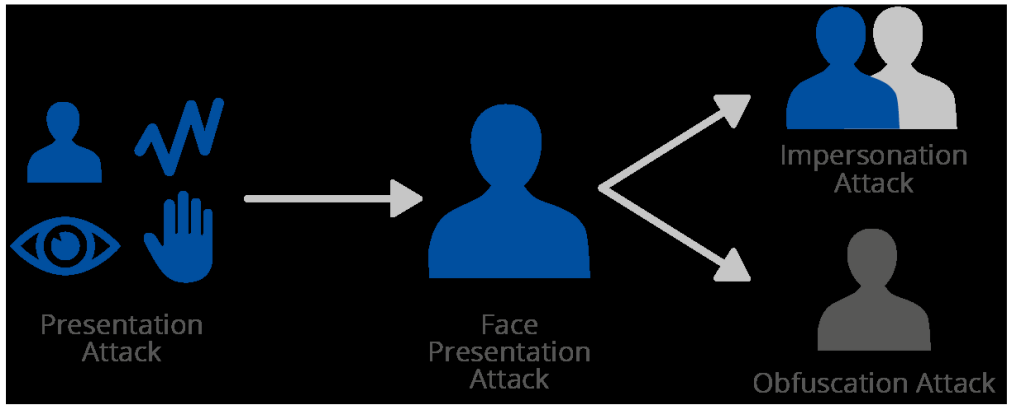
- ISO/IEC 30107-3:2017: "Information technology -- Biometric presentation attack detection (multi-part)
- ISO/IEC 19795-1:2021: "Information technology - Biometric performance testing and reporting (multi-part)
- ISO/IEC 19989-3:2020: "Information security - Criteria and methodology for security evaluation of biometric systems (multi-part)

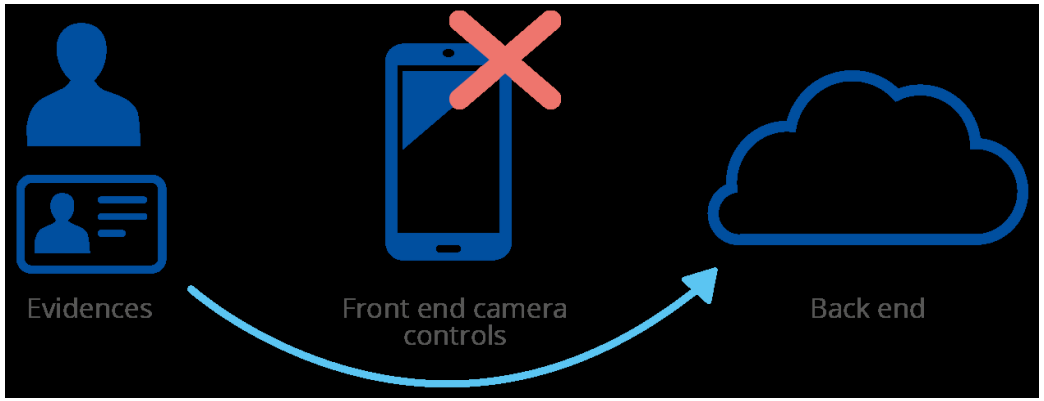
- And a lot more…..

Some major challenges

Presentation and injection attacks

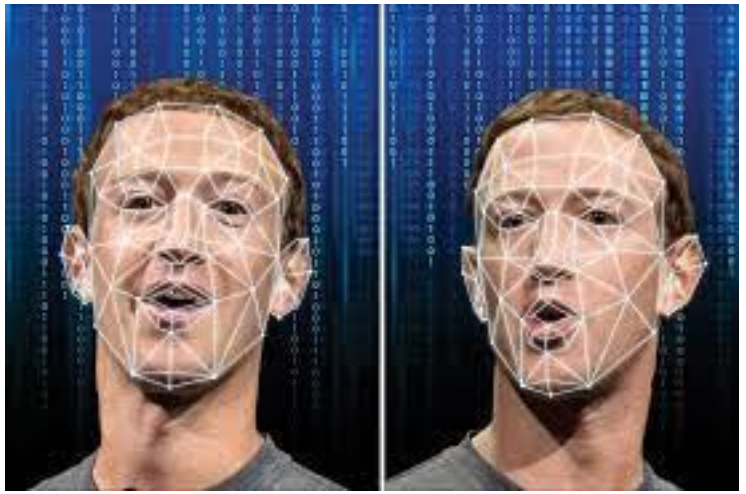
- **Remote identification with identity documents and selfie-video is done from the user's equipment**
- **Presentation attack: spoof the video recording**
  - Wearing a mask, showing a video, manipulating recording
- **Injection attack: inject a video stream bypassing the camera**
  - Recorded video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





Signicat

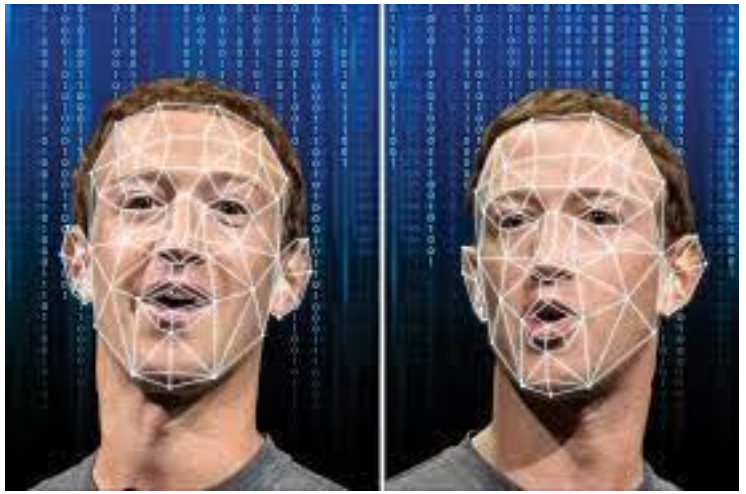
Deep fakes



- **Deep fakes – artificially generated videos**
  - Identity document video or face video
- **Huge increase in attack attempts**
  - Today, mostly «easy» to detect by humans, biometry, presentation attack detection
  - Today, humans likely better at detecting some attacks
- **Not so distant future**
  - Deep fakes indistinguishable from real videos
    - For both humans and biometric recognition systems
  - Ability to produce in real time to answer real-time challenges
  - Requires attacker to have comprehensible resources

Signicat

Injection attack detection



- **Deep fakes must be injected**
- **Protection against video injection gets critical**
  - Mechanisms for injection attack detection not “stabilised”
    - Software/hardware on a phone?
    - Use camera movements, gyros etc.?
- **Future maybe «signature» proving video is from genuine, identified camera?**

- **Read NFC chip of document rather than optical scanning**

Signicat

Can onboarding to the EUDI Wallet be automated?

- **ETSI TS 119 461: Automated identity proofing requires**
  - A suitable eID
  - A suitable signing certificate (e.g. qualified)
  - Use of digital identity document (NFC chip) and face biometrics

Can we use this for Wallet onboarding?

- **270 million people over 15 years**
- **Wallet penetration 80 % = 215 million EUDI Wallet holders**

- **Identity proofing at onboarding and regularly**
- **Repeat onboarding when a person gets a new phone (new Wallet app)?**
- **Some done by "other eIDs"**
- **Most by remote use of documents and selfie-video**

If Wallet onboarding requires a manual step, the costs will be enormous
People employed by the State?
Need for support staff for Wallets has yet to be discussed

Signicat

Please reach out for questions!

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