digicert® + QuoVadis

Remote Identity Validation for High Assurance Certificates

Stephen Davidson

eIDAS

Regulation (EU) No 910/2014

eIDAS - electronic identification and trust services for electronic transactions in the internal market

- Balancing acts of building a Digital Single Market

- So much about identity, but …
  - eIDAS does not try to introduce a common European eID system
  - Identification of citizens is a core national sovereignty

- Member States have option to “notify” their eID scheme to the Commission
  - Facilitate cross-border use and mutual recognition

eIDAS

Polite Opinion

- eIDAS major focus is on technical conformity of Trust Service Providers
  - ETSI: “PKI things we can nail down”
- eIDAS less specific on measures to guarantee uniform electronic identity
- Area of huge interest / utility
- Desire for more clarity on standards for remote identity vetting

eIDAS – What's Required

Recital 16

- Refers to STORK and ISO 29115 as references
- Assurance level high for qualified certificates

Article 8 - Assurance levels of electronic identification schemes

- Low - provides a limited degree of confidence in the claimed or asserted identity of a person
- Substantial - provides a substantial degree of confidence
- High - provides a higher degree of confidence than the assurance level substantial

eIDAS – What's Required

Article 24

Qualified verification allowed by:

a. Physical presence of the applicant

b. Remotely, using electronic identification, ensuring physical presence of the applicant

c. Qualified electronic signature / seal

d. Other methods which provide equivalent assurance to physical presence confirmed by a conformity assessment body

Regulation (EU) 2015/1502

Levels of Assurance used for “notified” electronic identification

Substantial	High
Possession of genuine evidence	Photo or biometric identification evidence
Identity document from same state as vetting	Previous equivalent procedures
Previous vetting for another purpose at equivalent level	Valid notified electronic identification
Valid notified electronic identification	Same State procedures to obtain recognised photo or biometric identification

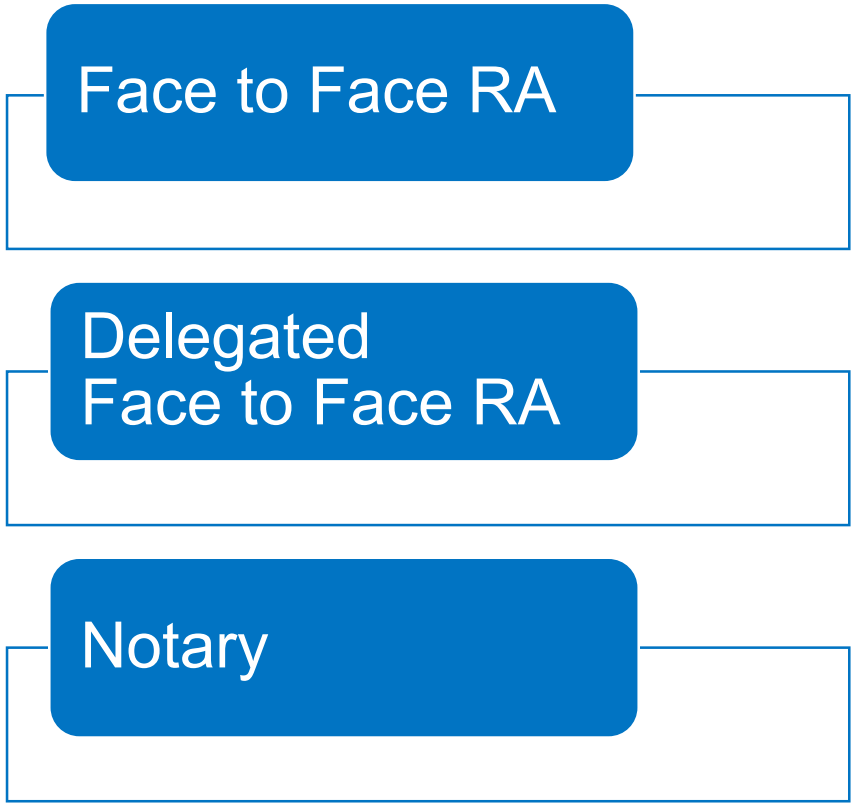
Identity Validation

In past:

- TSPs local focus
- Easier to fulfil physical presence
- “More routine”

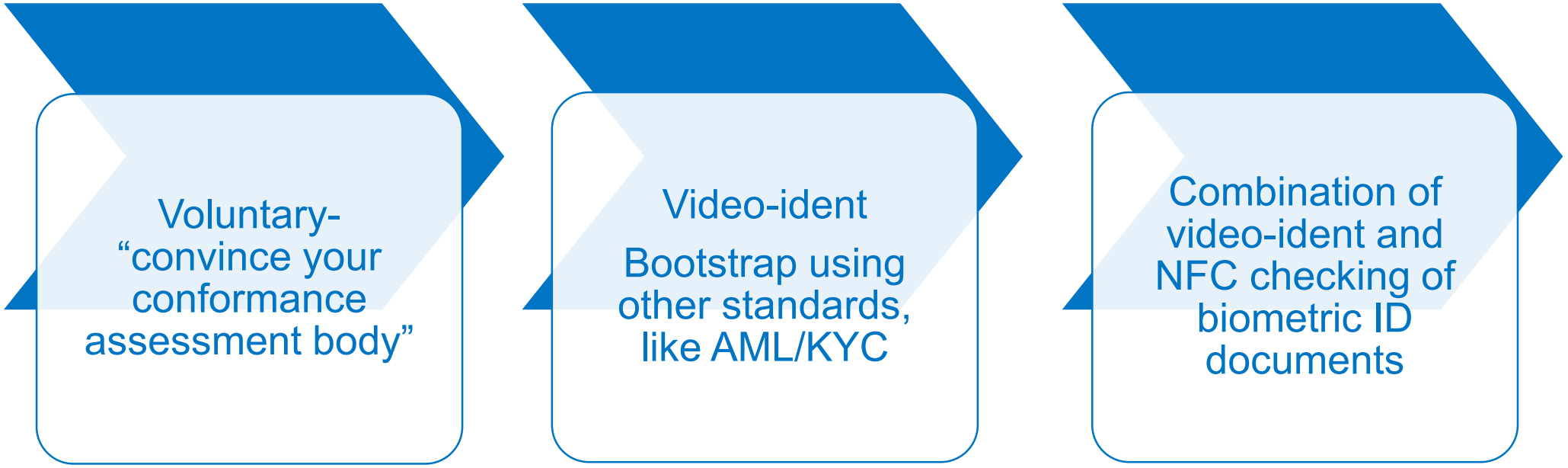
Future:

- TSPs regional+ focus
- TSPs involved in wider eIDAS platforms like server signing; agility
- Regional initiatives like PSD2 certs



Remote Identity Validation

- Massive efforts to ensure technical consistency of Qualified TSPs across Europe
- Significant national variance in the allowance for remote identity vetting:



Example

Germany

1. BSI TR-03147
   Assurance Level Assessment of Procedures for Identity Verification of Natural Persons
   - 38 pages
   - Detailed coverage of process, threats, and assessment for remote vetting

2. BaFin Circular 3/2017
   Video-ident under German Money Laundering Act → KYC/AML
   - 6 pages
   - Baseline coverage of video chat by trained RA, consent
   - Confirmation using TAN (shared secret)

Challenge

- Growing demand for remote vetting
  - Speed and convenience
  - Cross border reach
- Divergent view of requirements among member states
- Less focus on new machine learning tools for biometric “selfie” matching and ID authentication

- Much innovation is coming from outside the core TSP sector (KYC/AML, digital onboarding, account recovery)

- How can eIDAS CABs assess compliance to Article 24 without recognized standard?
- Other groups, such as FIDO Alliance, are seeking to assuming leadership
  - Authoritative guidance, performance evaluation, certifications

Thoughts ?

digicert® + QuoVadis

Thank you!

Remote Identity Validation for High Assurance Certificates

Stephen Davidson

Substantial LOA

1. Verified to be in possession of evidence representing the claimed identity and the evidence is checked to determine that it is genuine, and is known to exist and relates to a real person, and steps have been taken to minimise the risk that the person's identity is not the claimed identity
OR

2. An identity document is presented during a registration process in the Member State where the document was issued and the document appears to relate to the person presenting it and steps have been taken to minimise the risk that the person's identity is not the claimed identity
OR

3. Procedures used previously by a public or private entity in the same Member State for a purpose other than the issuance of eID at an equivalent assurance (confirmed by a conformity assessment body) do not need to be repeated
OR

4. Valid notified electronic identification having the assurance level substantial or high, can be relied upon taking into account the risks of a change in the person identification data. Not notified allowed if confirmed by a conformity assessment body.

High - Qualified LOA

1. Level substantial, plus:

   (a) Applicant has possession of photo or biometric identification evidence matching the claimed identity; the evidence is checked to determine that it is valid; and the applicant is identified as the claimed identity through comparison of one or more physical characteristic of the person with an authoritative source
   OR

   (b) Previous equivalent procedures if steps are taken to demonstrate that the results of the earlier procedures remain valid;

   OR

   (c) Valid notified electronic identification if steps are taken to demonstrate that the results of the earlier procedures remain valid

   OR

2. Same procedures used at the national level in the Member State of the entity responsible for registration to obtain such recognised photo or biometric identification evidence