ETSI The Standards People

Update on standardisation under eIDAS

Presented by: **Arno Fiedler**

For: **CA/B- Forum**

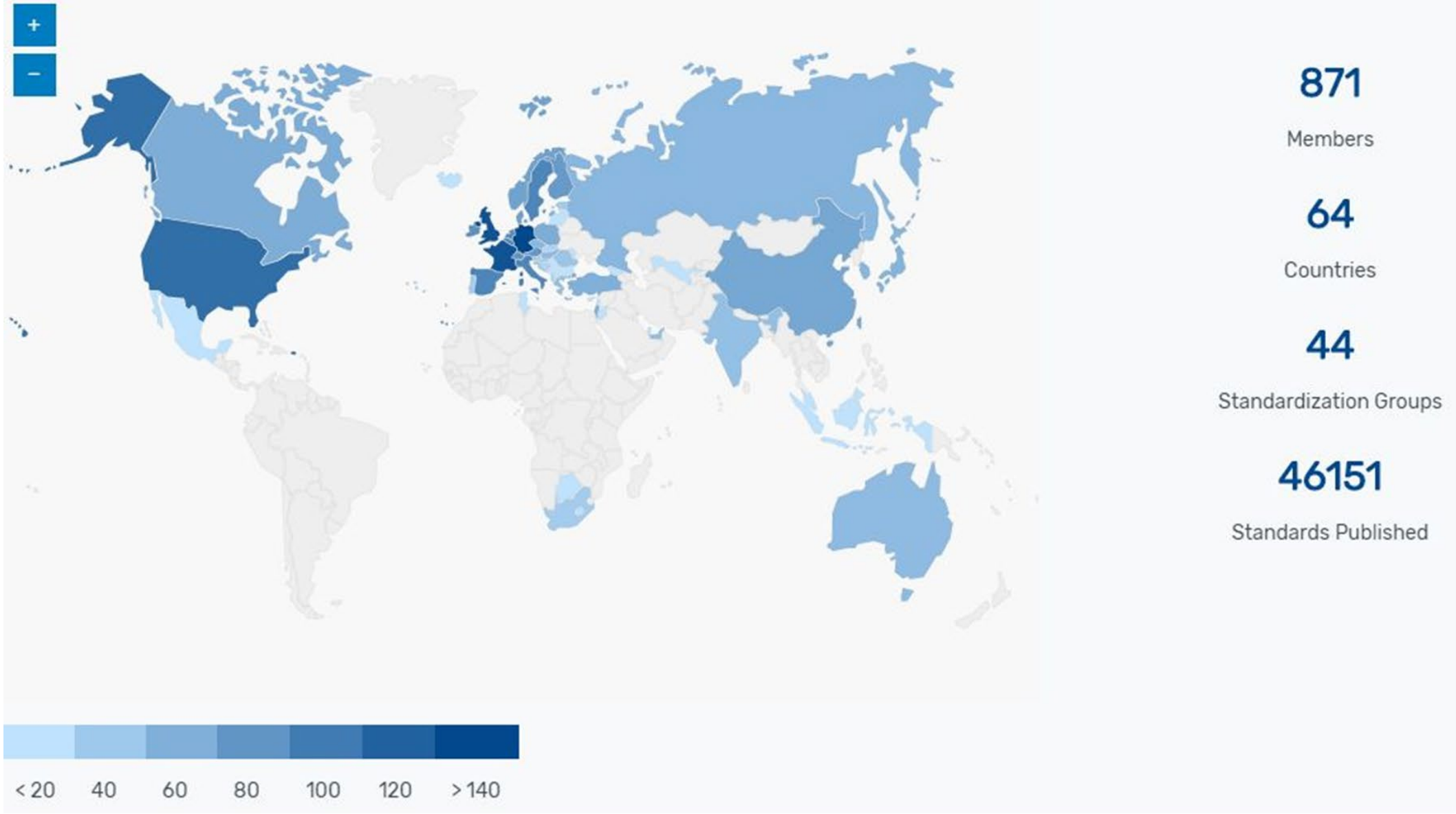
13.03.2019

Agenda

- Updates to CA policy requirements: EN 319 411-1/2
- Support for PSD2 use of qualified certificates
- Signature validation
- Remote signing (CEN & ETSI standards)
- Electronic Registered Delivery and Registered Electronic Mail (REM) services
- Long-term (signature) preservation
- Using Trusted Lists
- Need for clarifying audit requirements
- New activity: Machine processable signature policies and global acceptance of trust services

→ **When completed, standards will cover all trust services defined by eIDAS**

ETSI Member on Global Scale



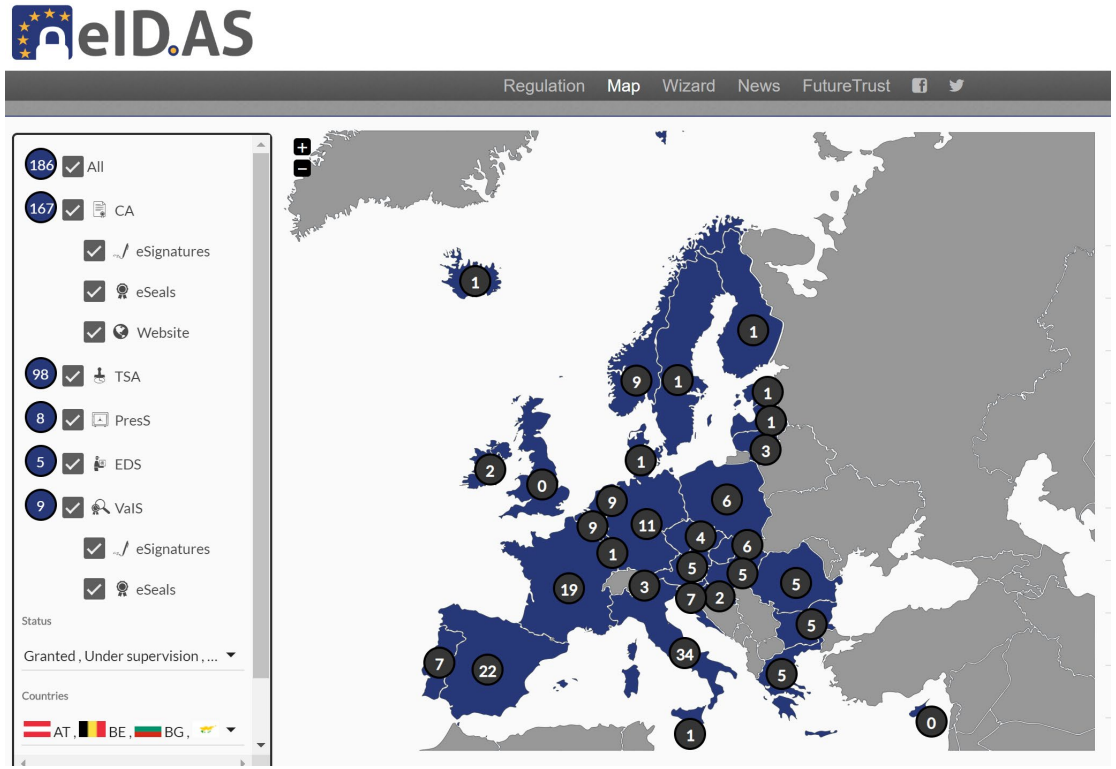
Background EU Trust Services

EU Regulation 910/2014

- Establishes legal framework for trust services in the EU

ETSI TC ESI:
“Electronic Signatures and Infrastructures”

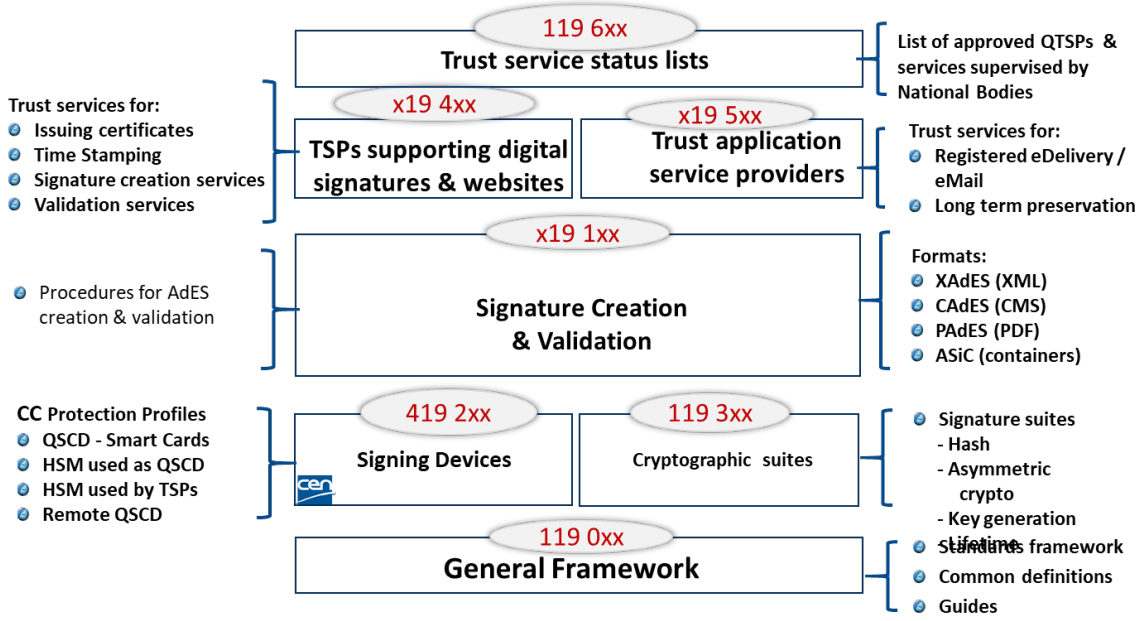
- Defines standards for trust services



ETSI Standards for Trust Services

Examples:

- **EN 319 411-1:** Policy requirements for Trust Service Providers issuing certificates
  ElSig: LCP; NCP
  TLS: DVCP; IVCP;OVCP; EVCP
- **EN 319 411-2:** Policy requirements for Trust Service Providers issuing EU qualified certificates
  ElSig: QCP
  TLS: QCP-W
- EN 319 403: Requirements for conformity assessment bodies assessing Trust Service Providers
- TS 119 612: Trust list of Trust Service Providers



Qualified Certificates under PSD2

ETSI joint work with ECB ERPB PIS WG / Open Banking Europe

Qualified Certificate profiles

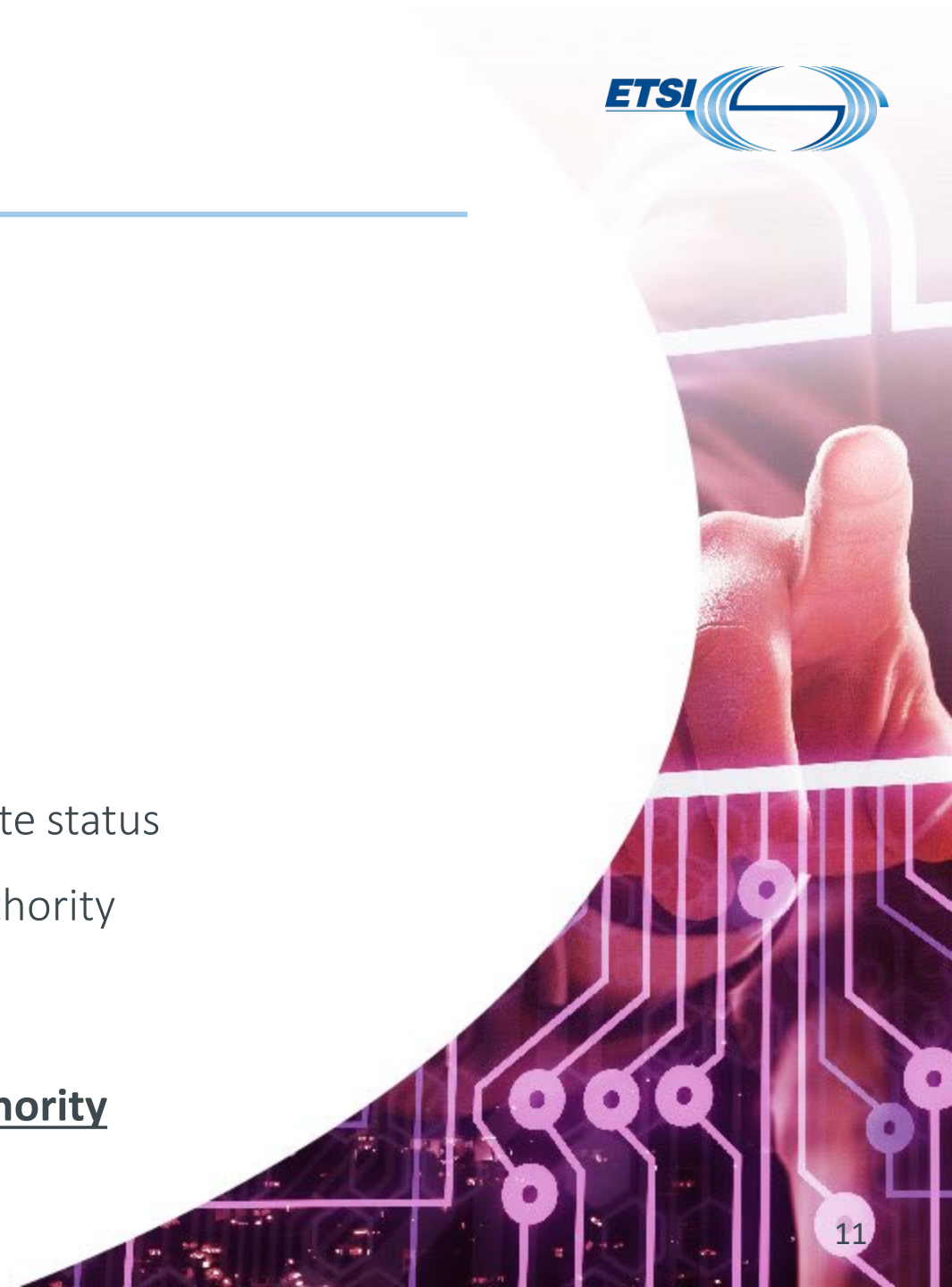
- PSD2 Qualified Website Authentication Certificates
- PSD2 Qualified Seal Certificates

CA Policy Requirements for PSD2 Qualified Certificate

- Requirements for validation of PSD2 specific attributes
- Revocation of PSD2 certificate due to change in PSD2 attribute status
- Involves interaction with National (Financial) Competent Authority

Published as TS 119 495 in May 2018

Update taking into account input from European Banking Authority



TSP Audits

Supplements to EN 319 403 TSP Audit Requirements

TS 119 403-2: Part 2: Additional requirements for Conformity Assessment Bodies auditing Trust Service Providers that issue Publicly-Trusted Certificates (e.g. as in CA/Browser Forum)

- Annual audit (versus bi-annually for eIDAS)
- Audit covers period of time since last audit
- *Change requirement: "PTA -4.3-08: The Audit Attestation shall be issued only if no critical non-conformities are identified and shall include a statement on each sub-clause of the referenced requirements where there is a finding of nonconformity noted during the audit which had been corrected prior issuing the Audit Attestation"*
- Latest version 08/18
  https://www.etsi.org/standards-search#search=TS119403-2

New Activities

About the Technical Committee Cyber (TC Cyber) Working Group for Quantum-Safe Cryptography (QSC)

- Founded March 2015 with focus on the practical implementation of quantum safe primitives, including performance considerations, implementation capabilities, protocols, benchmarking and practical architectural considerations for specific applications.
  - ETSI GR QSC003 Quantum-Safe Case Studies & Use Cases
  - ETSI GR QSC004 Quantum-Safe Threat Analysis
  - ETSI GR QSC006 Limits of Quantum Computing on Symmetric Key Cryptography
  - ETSI TR 103 570 **Quantum-Safe Key Exchanges, Implementation Analysis**
  - ETSI TR 103 617 Quantum-Safe Virtual Private Network (VPN)
- Ongoing Work Items:
  - QSC-008: Quantum-Safe Cryptographic Signature assessment, (INRIA)
  - QSC-12: Quantum-Safe Identity-Based Encryption (IBE), (NCSC)
  - QSC-13: **Migration Techniques to Quantum-Safe Systems,** (Cadzow Communication)

X.509 certificate standard made crypto-agile

- The X.509 certificate standard is the most widely-used cryptographic standard in the world
- Recently, the ITU-T SG17 accepted a proposal to update the next version of the ITU Rec. X.509 certificate to be crypto-agile
- The certificate is now able to support multiple signing algorithms, some of which may be quantum-safe

Global acceptance of European Trust Services

Study report on Global Acceptance of EU Trust Services: Analysis of international, regional and sector specific communities adopting Public Key Infrastructure technology

International co-hosted workshops:

- UAE, Dubai with TRA on Mai 02th
- Japan, Tokyo with JIPDEC and Keio University on May 23th
- Mexico, Mexico City with LOGALTY on June 27th
  and other important Events:
- ETSI Security Week: June 17 -21th
- TSP Day Berlin by ENISA and D-TRUST on September 25-26th

Conclusions

Information on available standards and current activities:
https://portal.etsi.org/TBSiteMap/ESI/ESIActivities.aspx

ETSI standards: available for free download
http://www.etsi.org/standards-search

CEN standards: available through National Standards Organisations

Updates on standardisation:
https://list.etsi.org/scripts/wa.exe?SUBED1=e-signatures_news&A=1