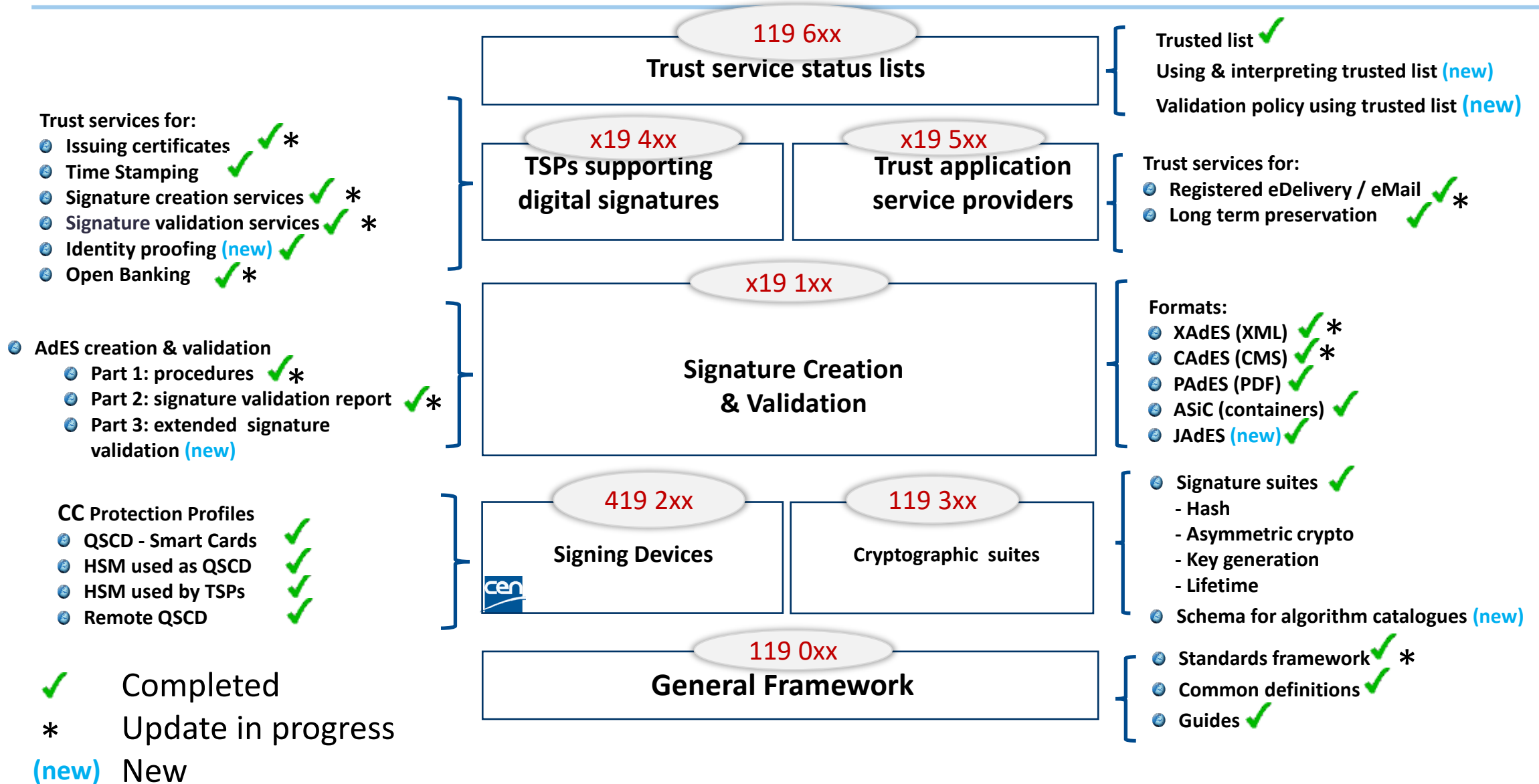# Update on ETSI ESI standardisation related to Publicly Trusted Certificates for CA/B-Forum Berlin Meeting

Arno Fiedler / Nick Pope
ETSI ESI Vice Chairs

Changes since last report highlighted

October 2022

ETSI & CEN Standards supporting eIDAS – the overall picture

119 6xx
Trust service status lists

Trusted list ✔
Using & interpreting trusted list (new)
Validation policy using trusted list (new)

Trust services for:
- Issuing certificates ✔ *
- Time Stamping ✔
- Signature creation services ✔ *
- Signature validation services ✔ *
- Identity proofing (new) ✔
- Open Banking ✔ *

x19 4xx
TSPs supporting digital signatures

x19 5xx
Trust application service providers

Trust services for:
- Registered eDelivery / eMail ✔ *
- Long term preservation ✔ *

x19 1xx
Signature Creation & Validation

- AdES creation & validation
  - Part 1: procedures ✔ *
  - Part 2: signature validation report ✔ *
  - Part 3: extended signature validation (new)

Formats:
- XAdES (XML) ✔ *
- CAdES (CMS) ✔ *
- PAdES (PDF) ✔
- ASiC (containers) ✔
- JAdES (new) ✔

CC Protection Profiles
- QSCD - Smart Cards ✔
- HSM used as QSCD ✔
- HSM used by TSPs ✔
- Remote QSCD ✔

419 2xx
Signing Devices

119 3xx
Cryptographic suites

- Signature suites ✔
  - Hash
  - Asymmetric crypto
  - Key generation
  - Lifetime
- Schema for algorithm catalogues (new)

119 0xx
General Framework

- Standards framework ✔ *
- Common definitions ✔
- Guides ✔

✔ Completed
* Update in progress
(new) New

2

Identity Proofing

TS 119 461: Policy and security requirements for trust service components providing identity proofing of trust service subjects

Published : July 2021: https://www.etsi.org/standards-search#search=TS119461

Working with other bodies to make this generally applicable

EN 319 401 / 411-1 / 411-2 Policy Requirements further updates

Further changes requests under discussion:

- EN 319 401 – Update to align with new ISO 27002 and NIS2 proposed regulation

  - Started study report into requirements additional measures in EN 319 401

- EN 319 411 – Various detailed updates including alignment with latest CAB Forum documents and recommended use of TS 119 461

- EN 319 412-1 & 2 – Proposals for detailed changes to certificate profiles

EN 319 411-1 Updates

CR#1	HSM certification - Update status of CEN standards, Allows FIPS 2 or 3
CR#2	Revocation request - 'by default' the 24 hours is respected for revocation processing, but allow TSP to specify procedures for handling exceptions
CR#3	Separation of TSP entity to avoid conflict of interest - certificates issued for TSP / RA operations from certificates for entities not identified in relation to the TSP
CR#4	Refer to TS 119 461 for identity proofing
CR#5	Re-validation of entity identity
CR#6 & 7	Keeping up with the Baseline Requirements and EV Guidelines
CR#8	Editorial Typo: OVR-5.1-03A should be 5.2

CRs ratified

CRs under discussion

EN 319 412-x Updates

412-1 CR#1	Reflect identity proofing method in certificate
412-1 CR#2	Identification of EU government entities
412-2 CR#1	Clarification on givenName/surname for more formal representation
412-2 CR#2	Specifying where to include the local language
412-2 CR#3	handle the case of natural persons without a given name (or surname)
412-2 CR#4	Remove pseudonym option for natural person issuer

CRs ratified

CRs under discussion

TR 119 411-5: Guidelines for the coexistence of web browser and EU trust controls

Certificate format:

▽   Common certificate format following EN 319 412-4 and CA/B Baseline

Issued:

▽   Based on EN 319 411-x and CA/B Forum Baseline policies

▽   Browser: Browser root store policy & EN 319 403-1 + TS 119 403-2 Audit

▽   EU: EN 319 411-2 policies QNCP-w or QEVCP-w & EN 319 403-1 + TS 119 403-3 Audit

Validated:

▽   Browser: against browser root store

▽   EU: Trusted lists as in ETSI TS 119 615

Display:

▽   EU Trust Mark & EU Identity displayed if passes both Browser and EU validation

▽   Browser may continue to display website if just passes Browser validation

EN 319 403 TSP Audit / Conformity Assessment Requirements

▽ EN 319 403-1 V2.3.1 (2020-06) : Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers

▽ TS 119 403-**2** V1.2.4 (2020-11): Part 2: Additional requirements for Conformity Assessment Bodies auditing Trust Service Providers that issue Publicly-Trusted Certificates (as in CA/Browser Forum)

  ▽ Further updates to Audit Statement requirements to align with Audit Letter Validation (ALV) tool

▽ TS 119 403-3 (2019-03): Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 3: Additional requirements for conformity assessment bodies assessing EU qualified trust service providers

International alignment of ETSI standards

➢ ETSI standards adopt standards that have been internationally supported wherever possible, this includes alignment of ETSI standards for website authentication certificates with CAB Forum guidelines

➢ Establish collaboration with:
- ❑ Safe Identity,
- ❑ Asia PKI,
- ❑ Japan Network Security Association,
- ❑ Arab ICT Organisation
- ❑ PKI Consortium
- ❑ OpenID

➢ Monitoring UNCITRAL "Draft Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services"
https://documents-dds-ny.un.org/doc/UNDOC/GEN/V22/009/38/PDF/V2200938.pdf?OpenElement

Further information

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

THANK YOU

arno.fiedler@nimbus.berlin

nick.pope@secstanassoc.com