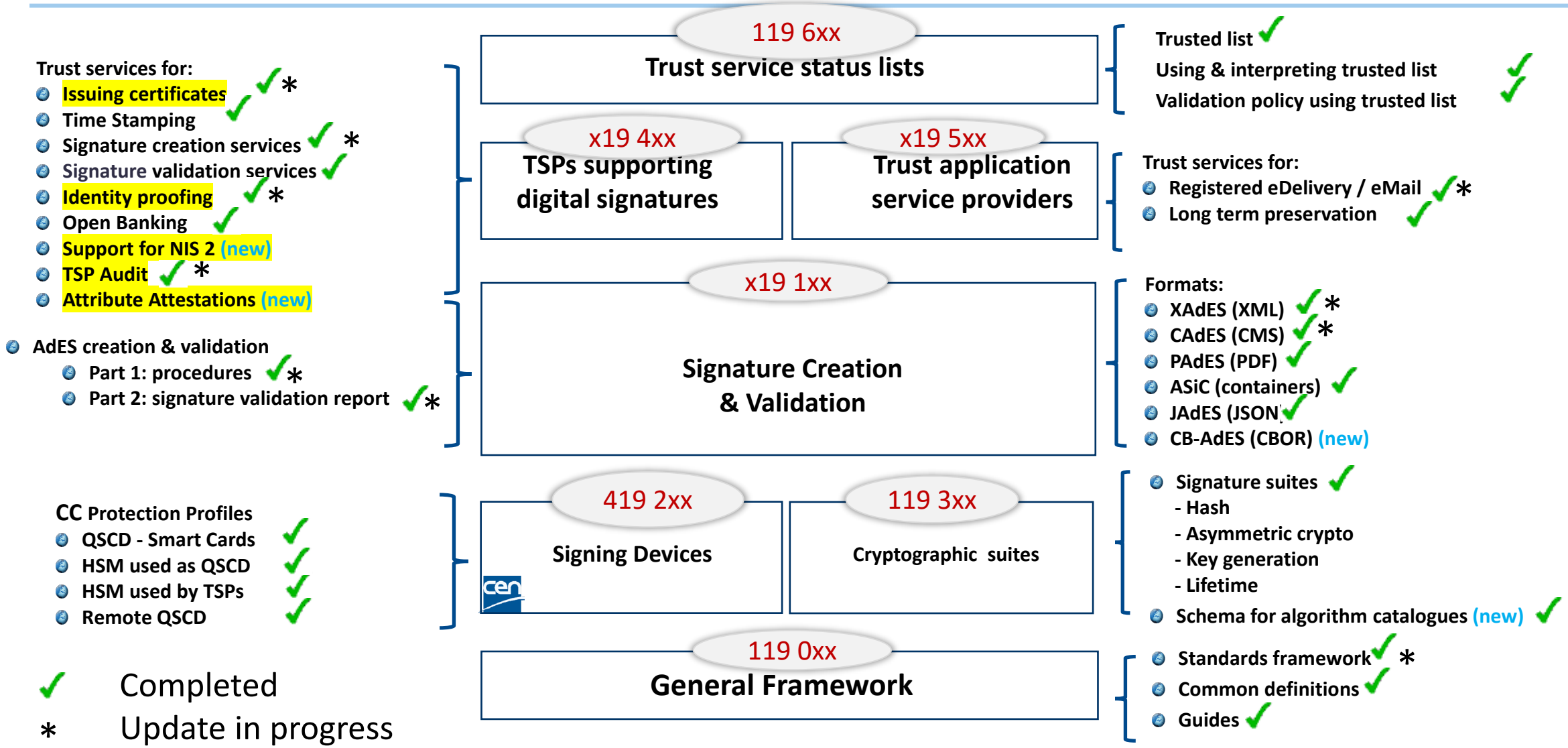
# Update on ETSI ESI standardisation related to Publicly Trusted Certificates

# CA/B-Forum #58. Ottawa Meeting

Arno Fiedler / Nick Pope
ETSI ESI Vice Chairs

1 March 2023

# ETSI & CEN Standards supporting eIDAS – the overall picture




✓ Completed

* Update in progress

(new) New

# TSP issuing certificates – Recent Activities

- TR 119 411-5: Guidelines for the coexistence of web browser and EU trust controls
- Clarifying the use of EN 319 411-1 & -2 for (Qualified) Website certificates with full CA/B Forum Alignment
- Other updates to EN 319 411-1 & -2 & EN 319 412-x
- New work item for TSPs issuing publicly trusted S/MIME certificates

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

- Guidance for browsers to facilitate support their existing Browser Root Programs & EU Trusted Lists
- Based Certificate Policies which fully aligned with CA/B Forum Baseline & support ETSI EN 319 411-x requirements for website certificates
- Uses common Audit based on EN 319 403-x
- Acceptance by browser depends on certificate fulfilling Browser Root Program
- If also passes requirements of EU Trust List then displays Entity behind web site & EU Trust Mark

Published: https://www.etsi.org/standards-search#search=TR119411-5

# ETSI Website Authentication Qualified Certificate Policies

- QEVCP-w Fully compliant with latest CA/Browser forum extended validation

- QNCP-w NCP + Full compliant with latest CA/Browser baseline

- QNCP-w-gen NCP + General purpose Website authentication requirements
  Essential CA/Browser baseline not already covered

# Other Updates – EN 319 411-1 General Policy Requirements

| | |
|---|---|
| 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 | Conflict of interest |
| CR#4 | Refer to TS 119 461 for identity proofing |
| CR#5 | Re-validation of entity identity for renew, rekey etc |
| CR#6 & CR#7 | DV/IV/OV/EV etc (Fully CABF Aligned), w-gen (only essential CABF requirements) |
| CR#8 | Editorial Typo: OVR-5.1-03A should be 5.**2** |
| CR#9, 11, 12 | Editorial |
| CR#10 | OCSPnoCheck is absent |

CRs ratified

CRs under approval

CRs under discussion

# Other Updates – EN 319 411-2 Qualified Policy Requirements

| | |
|---|---|
| CR#1 | Editorial |
| CR#2 | QNCP-w (Fully CABF IV/OV Aligned), w-gen (only essential CABF requirements) Aligned with EN 319 411-1 CR#6 |
| CR#3 | Clarify how to keep revocation status after expiry |
| CR#4 | Mapping clauses to eIDAS |
| CR#5 | Editorial |
| CR#6 | Re-validation of entity identity for renew, rekey etc |

CRs ratified

CRs under approval

CRs under discussion

# EN 319 412-x Certificate Profiles Updates

| | |
|---|---|
| 412-1 CR#1 | QC Statement to Reflect identity proofing method in certificate (Deferred until eIDAS 2 requirements clarified) |
| 412-1 CR#2 | Identification of EU government entities |
| 412-2 CR#1 | Clarification on givenName/surname for more formal representation Withdrawn (replaced by CR#5) |
| 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 |
| 412-2 CR#5 | Clarification on givenName/surname for more formal representation |
| 412-4 CR#1 | Alignment with QNCP-w, QNCP-w-gen |

CRs ratified

CRs under approval

CRs under discussion

# NWI TS 119 411-6 Requirements for TSP issuing publicly trusted S/MIME certificates

- Incorporates requirements CA/Browser Forum S/MIME Baseline Requirements

- Builds on existing certificate policy requirements defined in EN 319 411-1

# 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

Updates under discussion:

- Addional support for high level of identity assurance
- Support of EU Wallet onboarding
- Support for EBA Remove (Banking) Customer onboarding

# NIS 2 Alignment

New directive (EU) 2022/2555 (“NIS2”)on
“measures for a high common level of cybersecurity across the Union”

Mandates Trust Services adhere to common cybersecurity measures

Studied impact on ETSI Trust Service policies
TR 119 404 (under final publication checks)

Started work on updates to general requirements document for TSPs (EN 319 401)

# Update to EN 319 403-2
# TSP Audit / Conformity Assessment Requirements

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

Updates to align with Common CA Database / Browser requirements:

#1 Addition to PTA-4.3-04 “audit attestation retrieval for at least one year”

#2 New PTA-4.3.-04a with “audit attestation direct link via https”

#2 Update to PTA-4.3-05a ISO date format to a shall requirement

#3 New PTA-4.3-15 “Cover all Root CA AAL of a TSP in one document”

#4 Addition to Note 3 “Usage of AAL templates provided by ACAB'c”

Publication due: 10 March:

# eIDAS 2

- Architectural Reference Framework v1.0.0 available
- Project let to produce open source implementation of Wallet
- 4 * Pilot projects implementing wallets
- ETSI Leading standardisation of TSP related aspects:
  - Attribute attestation formats,
  - Attribute attestation policies,
  - Wallet to TSP interface

# Concluding points

- With updated approach of directly incorporating latest version of CA/Browser Forum Baseline any updates are automatically incorporated in ETSI EN 319 411-1 etc

- Any browser specific audit process / report requirements can be easily in updates to TS 119 403-2 (assuming they are not in conflict with EU practices).

# 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


arno.fiedler@nimbus.berlin

nick.pope@secstanassoc.com