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

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

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

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

Completed ✓
Update in progress (*)
New (new)

119 6xx
Trust service status lists

x19 4xx
TSPs supporting
digital signatures

x19 5xx
Trust application
service providers

119 1xx
Signature Creation & Validation

419 2xx
Signing Devices

119 3xx
Cryptographic suites

119 0xx
General Framework

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

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

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

Signature suites ✓
- Hash
- Asymmetric crypto
- Key generation
- Lifetime

Schema for algorithm catalogues (new)

* Standards framework ✓
- Common definitions ✓
- Guides ✓
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
<table>
<thead>
<tr>
<th>CR#</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CR#1</td>
<td>HSM certification - Update status of CEN standards, Allows FIPS 2 or 3</td>
</tr>
<tr>
<td>CR#2</td>
<td>Revocation request - ‘by default’ the 24 hours is respected for revocation processing, but allow TSP to specify procedures for handling exceptions</td>
</tr>
<tr>
<td>CR#3</td>
<td>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</td>
</tr>
<tr>
<td>CR#4</td>
<td>Refer to TS 119 461 for identity proofing</td>
</tr>
<tr>
<td>CR#5</td>
<td>Re-validation of entity identity</td>
</tr>
<tr>
<td>CR#6 &amp; 7</td>
<td>Keeping up with the Baseline Requirements and EV Guidelines</td>
</tr>
<tr>
<td>CR#8</td>
<td>Editorial Typo: OVR-5.1-03A should be 5.2</td>
</tr>
</tbody>
</table>

CRs ratified

CRs under discussion
<table>
<thead>
<tr>
<th>CR#</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>412-1</td>
<td>Reflect identity proofing method in certificate</td>
</tr>
<tr>
<td>412-1</td>
<td>Identification of EU government entities</td>
</tr>
<tr>
<td>412-2</td>
<td>Clarification on givenName/surname for more formal representation</td>
</tr>
<tr>
<td>412-2</td>
<td>Specifying where to include the local language</td>
</tr>
<tr>
<td>412-2</td>
<td>handle the case of natural persons without a given name (or surname)</td>
</tr>
<tr>
<td>412-2</td>
<td>Remove pseudonym option for natural person issuer</td>
</tr>
</tbody>
</table>

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

Further information

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