Update on ETSI ESI standardisation related to Publicly Trusted Certificates

CA/B-Forum June 2023 Meeting

Arno Fiedler / Nick Pope
ETSI ESI Vice Chair / Chair (elect)

Changes since last report highlighted

June, 07th 2023 Redmond

ETSI Community:

- Independent, non-profit European Standards Organization (ESO).
- More than 900 member organizations worldwide, drawn from over 60 countries and on five continents
- 30+ years track record of technical excellence in the ICT sector
- Strong community of experts and innovators
- Diverse members: SMEs, micro-enterprises, large companies, research entities, academia, government and public bodies, societal stakeholders

ETSI Members shape:

- ✓ 5G
- ✓ Internet of Things
- ✓ Cybersecurity
- ✓ Network Virtualization
- ✓ Artificial Intelligence
- ✓ Multi-access Edge Computing
- ✓ Blockchain/DLT
- ✓ Quantum Safe Cryptography
- ✓ Radio
- ✓ …and many others……
  like “Techical Committee Electronic Signatures and Infrastructures” TC ESI

ETSI & CEN Standards supporting eIDAS – the overall picture

Trust services:
- TSP Audit ✓
- Issuing certificates ✓ ✓*
- Time Stamping ✓
- Signature creation services ✓
- Signature validation services ✓
- Identity proofing ✓ *
- Open Banking ✓
- Support for NIS 2 (new)
- Attribute Attestations (new)

- AdES creation & validation
  - Part 1: procedures ✓*
  - Part 2: signature validation report ✓*

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

119 6xx
Trust service status lists
- Trusted list ✓
- Using & interpreting trusted list ✓
- Validation policy using trusted list ✓

x19 4xx
TSPs supporting digital signatures

x19 5xx
Trust application service providers

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

Interop tests

x19 1xx
Signature Creation & Validation

Formats + Interop test:
- XAdES (XML) ✓*
- CAdES (CMS) ✓*
- PAdES (PDF) ✓
- ASiC (containers) ✓
- JAdES (JSON) ✓
- CB-AdES (CBOR) (new)

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

TSP issuing certificates – Recent Activities

- Support for QWACs
- Agreed updates to EN 319 411-1 & -2 & EN 319 412-x
- Work item for TSPs issuing publicly trusted S/MIME certificates
- Alignment of all trust services with NIS2 Directive
- Identity proofing

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

Working on 2 certificate approach & security considerations for 1 certificate QWAC

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

EN 319 411-1 Updates Approved by ETSI

CR#01 HSM certification - Update status of CEN standards, Allows FIPS 2 or 3

CR#02 ensure that ‘by default’ the 24 hours is respected

CR#03 Conflict of interest

CR#04 Refer to TS 119 461 for identity proofing

CR#05 Existing evidence to be re-used to validate the identity (for rekey, renew …)

CR#06 (integrating ex-CR#007) Alignment with CA/Browser Forum

CR#08 Typo: OVR-5.1-03A should be 5.2

CR#09 REQ-6.2.2-01 on identity validation contains 2 SHALL

CR#10 OCSPnoCheck absent may create loop

CR#11adapt history

CR#12 Typo: in REV-6.3.9-15, the ref. SDP-6.5.1-2 is incorrect, it shall be SDP-6.5.1-21

CR#13 Add reference to 119 411-5 in the scope

CR#14 Tracing reclamations for short term certificates

CR#15 reference to 101 533 to update

CR#16 Certificates for testing

EN 319 411-2 Updates Approved by ETSI

CR#1 Wrong references to eIDAS article 27 - 37 in clauses 5.5.1 & 5.5.2

CR#2 Qualified Website policies aligned with CA/B Forum (from 411-1 CR#006 & 007)

CR#3 Clarify how to keep revocation status after expiry.

CR#4 Adapt references in Annex A

Outstanding issue on Article 24-1 requirement applied to renewal / re-key

EN 319 412-x Updates

CRs deferred

412-1	QC Statement to Reflect identity proofing method in certificate Identification of EU government entities
412-2	CR#2 Specifying where to include the local language CR#3 Handle the case of natural persons without a given name (or surname) CR#4 Remove pseudonyme for natural person issuer CR#5 Replace "should" by "shall" in the new text clarifying given name and surname CR#8 Inclusion of OrganisationIdentifier for issuer (other CRs either withdrawn of editorial)
412-4	CR#1 Update to align with Web policies in EN 319 411-1 & 2
All parts	Editorial updates to number each requirement

EN 319 411-x and 412-x Updates

- Approved by ETSI
- Going through ETSI pre-publication checks
- To be published as Draft ENs for national approval
- Final publication expect Q4 2023

New TS 119 411-6: S/MIME

Single certificate complies with:

- CA/Browser Forum S/MIME baseline certificate policy
- ETSI EN 319 411-1 / 2 Certificate policy

Stable draft – likely publication Q3 2023

It was agreed at ESI#80a meeting on 05th of Juni for TS 119 411-6 to:

- 2 week review within ETSI ESI of ESI(23)80a005 Draft - TS 119 411-6 v0.0.2
- If no major issues put stable draft in public area
- Send liaison to CABF asking for comments.

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:

- Additonal 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)

Stable draft on 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: 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 for remote signing

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