



The Standards People



Update on ETSI ESI standardisation related to Publicly Trusted Certificates

Arno Fiedler
ETSI ESI Vice Chair

05.11 2019

Agenda

- ✔ Proposed Updates to CA policy requirements: EN 319 411
- ✔ Updates to EN 319 412-x
- ✔ 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
- ✔ Algorithms
- ✔ Using Trusted Lists
- ✔ Audit Update
- ✔ Machine processable signature policies
- ✔ Proposed new work item on identity proofing
- ✔ Global acceptance of trust services

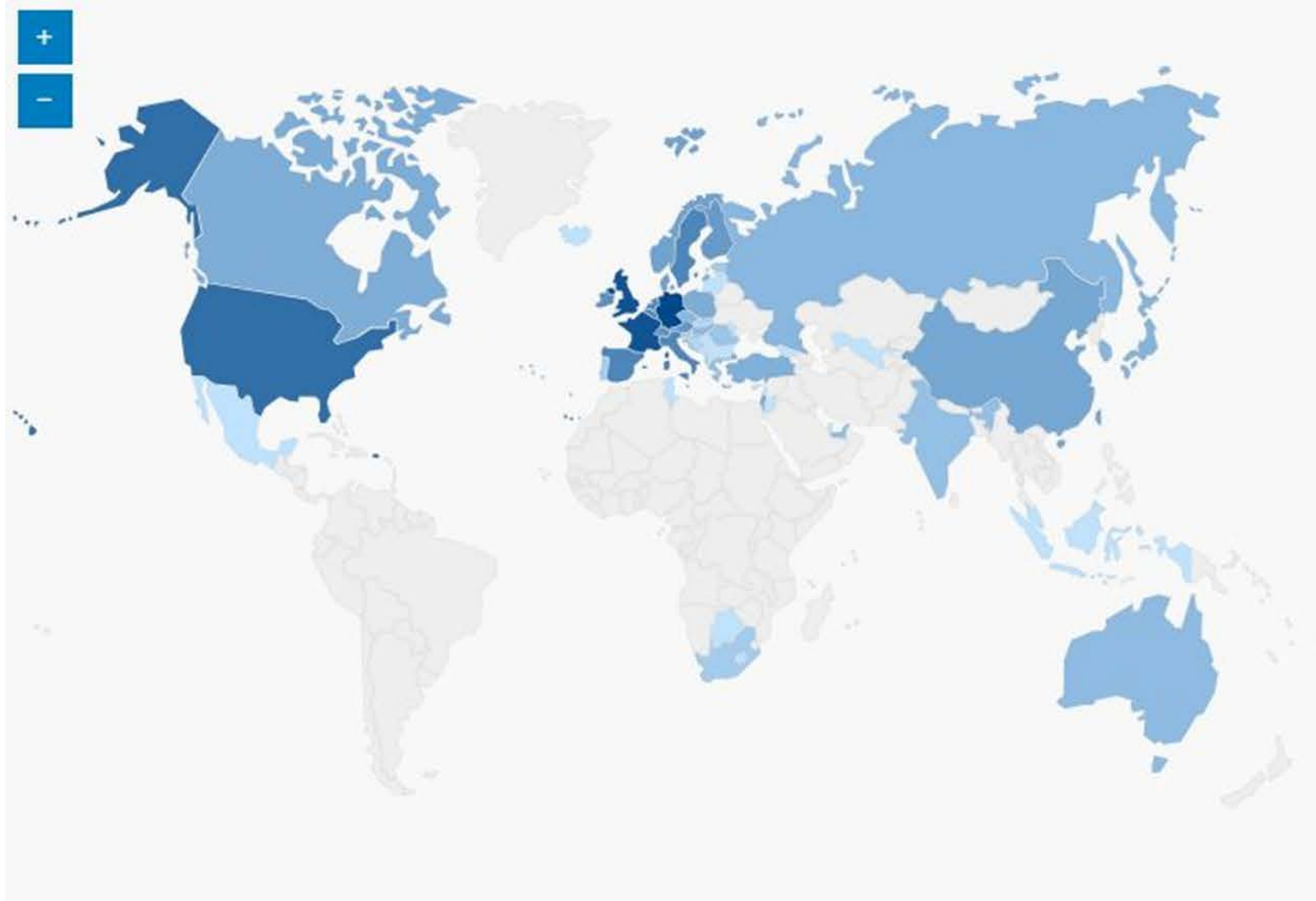
Note: Areas where significant updates have occurred

eIDAS Strategic Goals

(Slide from Andrea Servida; EU Commission; Head of DG CONNECT H4 - "eGovernment and Trust")



ETSI Member on Global Scale



871

Members

64

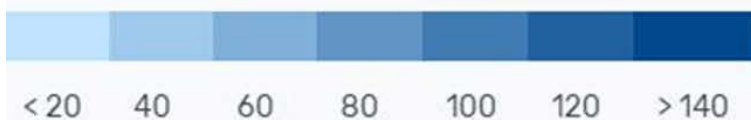
Countries

44

Standardization Groups

46151

Standards Published



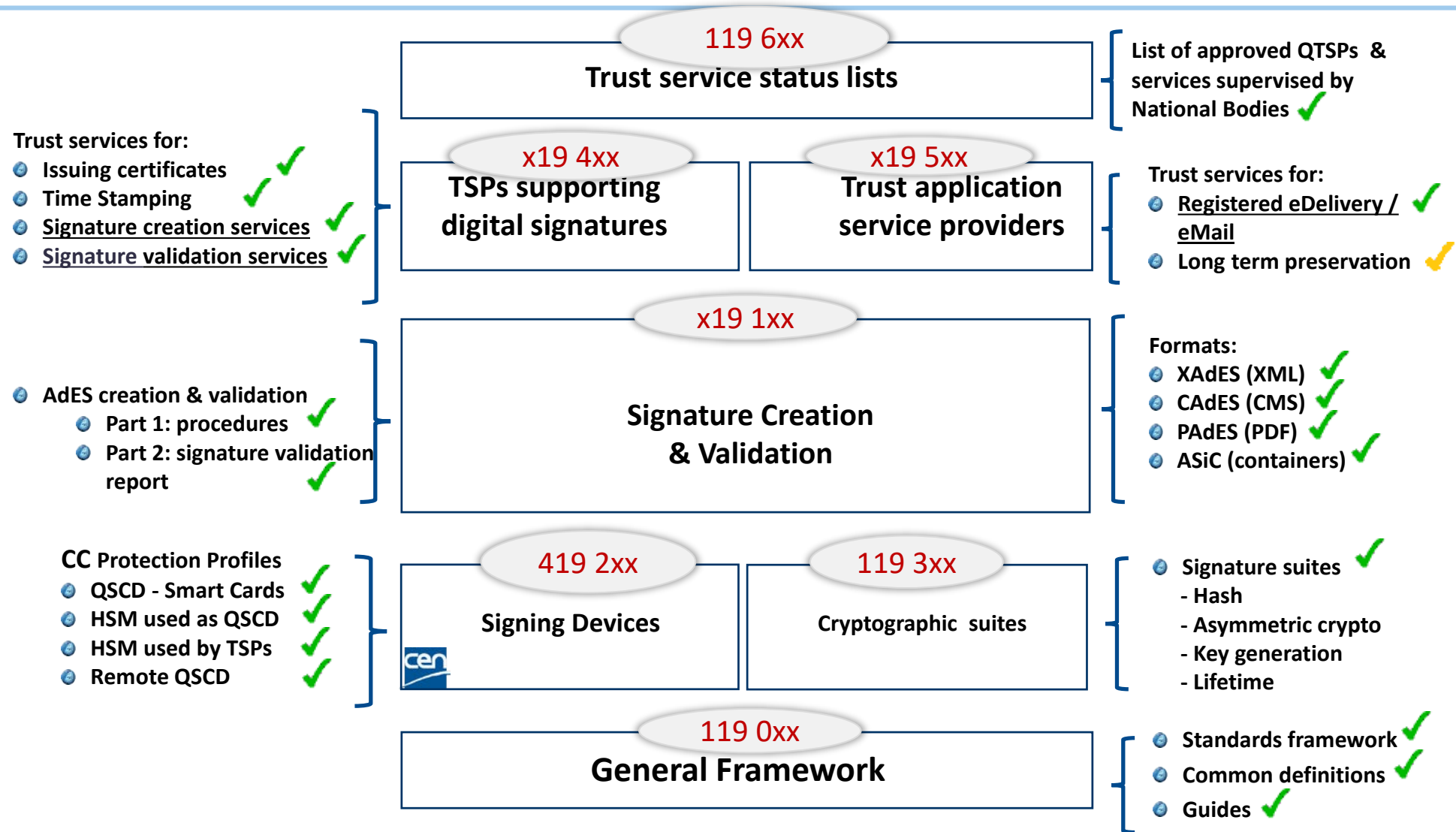
EU Regulation for trust Services & ETSI Standards

- EU Regulation 910/2014 on eID and Trust services (eIDAS)
 - ❑ Governmental supervision scheme for providers of trust services
 - ❑ Similar legislation being applied around the world

- eIDAS Best Practice
 - ❑ Commonly demonstrated by conformance to ETSI standards
 - ❑ Standards being adopted around the world



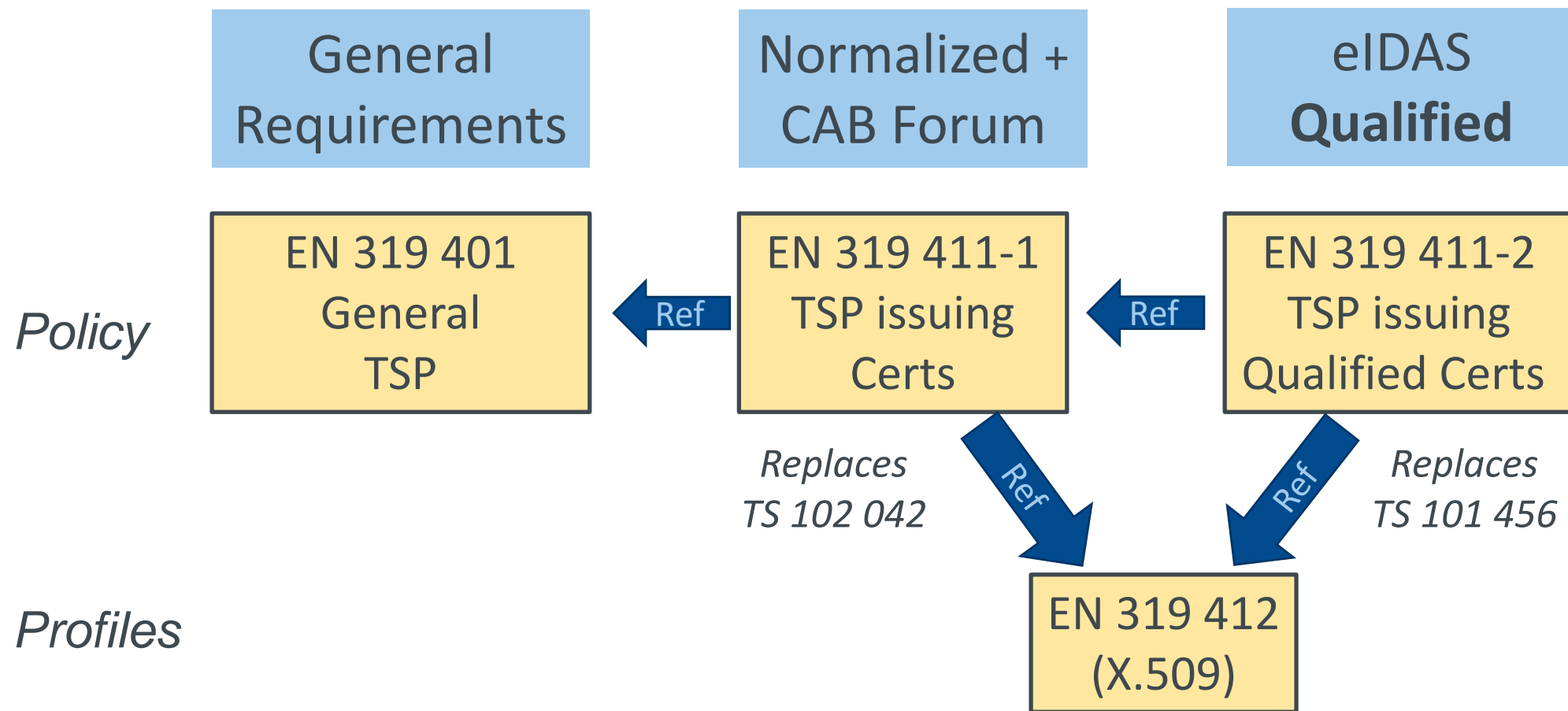
eIDAS Standards Framework: Published Standards





TSP Requirements

Trust services issuing certificates: ETSI standards overview



CA Policy & Certificate Requirements: EN 319 411-x (Planned updates)



➤ EN 319 411 planned updates

- “minor revisions to clarify areas where there has been uncertainty in interpretation of the standard”
- Short term certificates (less than revocation notification period)
- Avoiding CAB Forum issues impacting QWACs, in particular for EV

Certificate Profiles (Updates)

- EN 319 412-1 / TS 119 412-1
 - Support for LEI in Subject
 - Support for eID attributes in Subject Name
 - Short term certificates
- EN 319 412-2 & 3
 - Clarification on Key usage
 - Ongoing: Removal of RFC 5280 attribute size limits (e.g. organisation name > 64 characters)
- EN 319 412-5 QCStatement for non-EU countries
(See globalisation study later)

TS 119 495 Qualified Certificates under PSD2 (Updates)

Coordinated with European Banking Association / Open Banking Europe

- Clarifications on Authorisation Number
- Email interface with “National Competent Authorities” for notifications of certificate issuance and revocation



Signature Formats & Validation

JSON Signatures

1st Draft to define equivalent to CAdES / PAdES / XAdES for JSON data format based on RFC 7515 JSON Web Signatures

Signature Validation

- ✔ TS 119 102-1 (2019-1) Procedures for Creation and Validation of AdES - published
- ✔ TS 119 102-2 (2019-02): Validation Report – Published
- ✔ TS 119 441 (2018-08): Policy Requirements for TSPs Providing Signature Validation Services (including annex for qualified service) - Published
- ✔ TS 119 442 (2019-02): Protocol for Signature Validation Services – Published, To be updated following OASIS DSS v2.0 publication
- ✔ TS 119 172-4: Signature Validation Policy for European Qualified Electronic Signatures/Seals Using Trusted Lists – Draft awaiting Plugtests™ for final approval
See: https://docbox.etsi.org/esi/Open/Latest_Drafts/draft-ts_119172-4v007-public.pdf
- ✔ TS 119 615: Procedures for using and interpreting European Union Member States national trusted lists – Draft awaiting Plugtests™ for final approval
See: https://docbox.etsi.org/esi/Open/Latest_Drafts/draft_ts_119_615_v0.0.9-public.pdf



Remote Signing & CEN Standards

CEN standards for remote signing systems:

- ✔ EN 419 241-1: General System Requirements - published
- ✔ EN 419 241-2: Protection Profile for QSCD for Server Signing - published
- ✔ EN 419 221-5: Cryptographic Module - published

Other CEN Documents recently published

- CEN TS 419 221-6: Conditions for use of EN 419 221-5 (HSM-PP) as qualified electronic signature or seal creation device
- CEN TR 419 210: Applicability of CEN Standards to Qualified Electronic Seal

Standards published:

- ✔ TS 119 431-1: Policy and Security Requirements for TSP Service Components Operating a Remote QSCD / SCD
- ✔ TS 119 431-2: Policy and Security Requirements for TSP Service Components Supporting AdES Digital Signature Creation
- ✔ TS 119 432: Protocols for Remote Digital Signature Creation
To be updated following OASIS DSS v2.0 publication



Electronic Registered Delivery & REM

Published standards:

- ✔ EN 319 522 (2018-09): Electronic Registered Delivery Services
- ✔ EN 319 532 (2018-09): Registered Electronic Mail (REM) Services (Supersedes ETSI TS 102 640)
- ✔ EN 319 521: Policy and Security Requirements for Electronic Registered Delivery Service Providers
- ✔ EN 319 531: Policy and Security Requirements for Registered Electronic Mail Service Providers
- ✔ TS 119 524: Testing Conformance and Interoperability of Electronic Registered Delivery Services
- ✔ TS 119 534: Testing Conformance and Interoperability of Registered Electronic Mail Services
- ✔ TR 119 500: Business Driven Guidance for Trust Application Service Providers



Preservation

Long-Term (Signature) Preservation

- ✔ TS 119 511 Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques (Published)
- ✔ TS 119 512 Protocols for trust service providers providing long-term data preservation services (Approved awaiting publication)



Signature Algorithms

Signature Algorithms

- ✓ TS 119 312: Cryptographic Suites – Updated 2019-02

- ✓ TS 119 322 Generic schema for machine-readable algorithms
 - Takes into account 3 well known schemes: TS 119 312, SOGIS and IETF RFC 5698



Trusted Lists

Trusted Lists

- ✓ TS 119 615 Final draft awaiting feedback from plugtests – expected early 2020
 - ✓ on the use of information within a EU Trusted List by relying parties,
 - ✓ how to process a trusted list in order to obtain information about a QTSP and QTS(s) it provides
 - ✓ Building blocks
 - ✓ for validating a qualified signature/seal (see also upcoming TS 119 172-4)
 - ✓ To link trusted list information to evidences produced by some types of trust services: validation service, preservation service, electronic registered delivery services
 - ✓ See: https://docbox.etsi.org/esi/Open/Latest_Drafts/draft-ts_119172-4v007-public.pdf
- ✓ TS 119 172-4 Final draft awaiting feedback from Plugtests™ – expected early 2020
 - ✓ Signature policy using EU trusted list
 - ✓ See: https://docbox.etsi.org/esi/Open/Latest_Drafts/draft_ts_119_615_v0.0.9-public.pdf
- ✓ TS 119 612 / 602 Updates
 - ✓ Work deferred – new version not expected before 2020



TSP Audits

EN 319 403-1 (previously EN 319 403) Audit

Revised draft EN 319 403 -1:

- Audit of component services
- Clarification regarding handling of TSP requiring corrective actions
 - Audit report issued identifying corrective actions required.
 - Minor non-conformities to be corrected in 3 to 6 months
- New Annex on determining audit time (specifics removed)
- Other minor changes

- ✔ TS 119 403-2 (2019-03): Part 2: Additional requirements for Conformity Assessment Bodies auditing Trust Service Providers that issue Publicly-Trusted Certificates (e.g. as in CA/Browser Forum)
- ✔ TS 119 403-3 (2019-4): Part 3: Additional requirements for Conformity Assessment Bodies auditing Trust Service Providers that issue Publicly-Trusted Certificates



New Activities

Machine-processible signature policy formats

- ✔ TS 119 172-2: XML format for signature policies – final draft under preparation, to be published by 30 November
- ✔ TS 119 172-3: ASN.1 format for signature policies – final draft under preparation, to be published by 30 November

Identity Proofing of trust service subjects

Started work survey for TS on “Policy and security requirements for trust service components providing identity proofing of trust service subjects.

- Can be a separate “component service”
- Subject may be for remote registration
- Supporting:
 - eIDAS Art.24.1.(d) remote electronic identification
 - EN 319 411-1/2: TSP issuing certificates
 - EN 319 521 / 531: ERDS / REM
 - TS 119 431: Remote signing

Study Report on Global acceptance of European Trust Services Executive summary (TR 103 684)



- Aims to facilitate cross recognition between EU eIDAS trust services, and other non-EU schemes.
- The study concentrates on existing PKI-based trust services
- Methodology on 4 pillars: legal context, supervision and audit, technical standards, and trust representation.
- Analysed 37 existing schemes.
- Workshops in Dubai, Tokyo, Mexico City and New York
- The study concludes with 18 recommendations
- There is strong interest but remain significant issues to be overcome.

Globalisation Study Report (TR 103 684)

Some conclusions relevant Supervisory Bodies



- h) The lack of agreements under eIDAS article 14 is a barrier to the mutual recognition of trust services outside the EU to be recognised as Qualified trust services inside the EU.
- k) The lack of consistency of the best practices used in the audit schemes for qualified trust services in Europe is jeopardizing their mutual recognition;
- o) ETSI standards should be extended to provide an interoperable equivalent to the EU Qualified Certificate Policies (QCP-I) which may be adopted by non-EU countries and or agreement-based scheme.
- r) The EN 319 412-5 [i.26] QcCompliance statement should be updated to extend its scope to non-EU countries.

(see report – to be published November 2019 for full set of conclusions)

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

