Update on ETSI ESI standardisation related to Publicly Trusted Certificates

Arno Fiedler, Nick Pope
ETSI ESI Vice Chair

11.06.2020

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
- Started work on identity proofing
- Global acceptance of trust services

Note: Areas where significant updates have occurred

eIDAS Strategic Goals

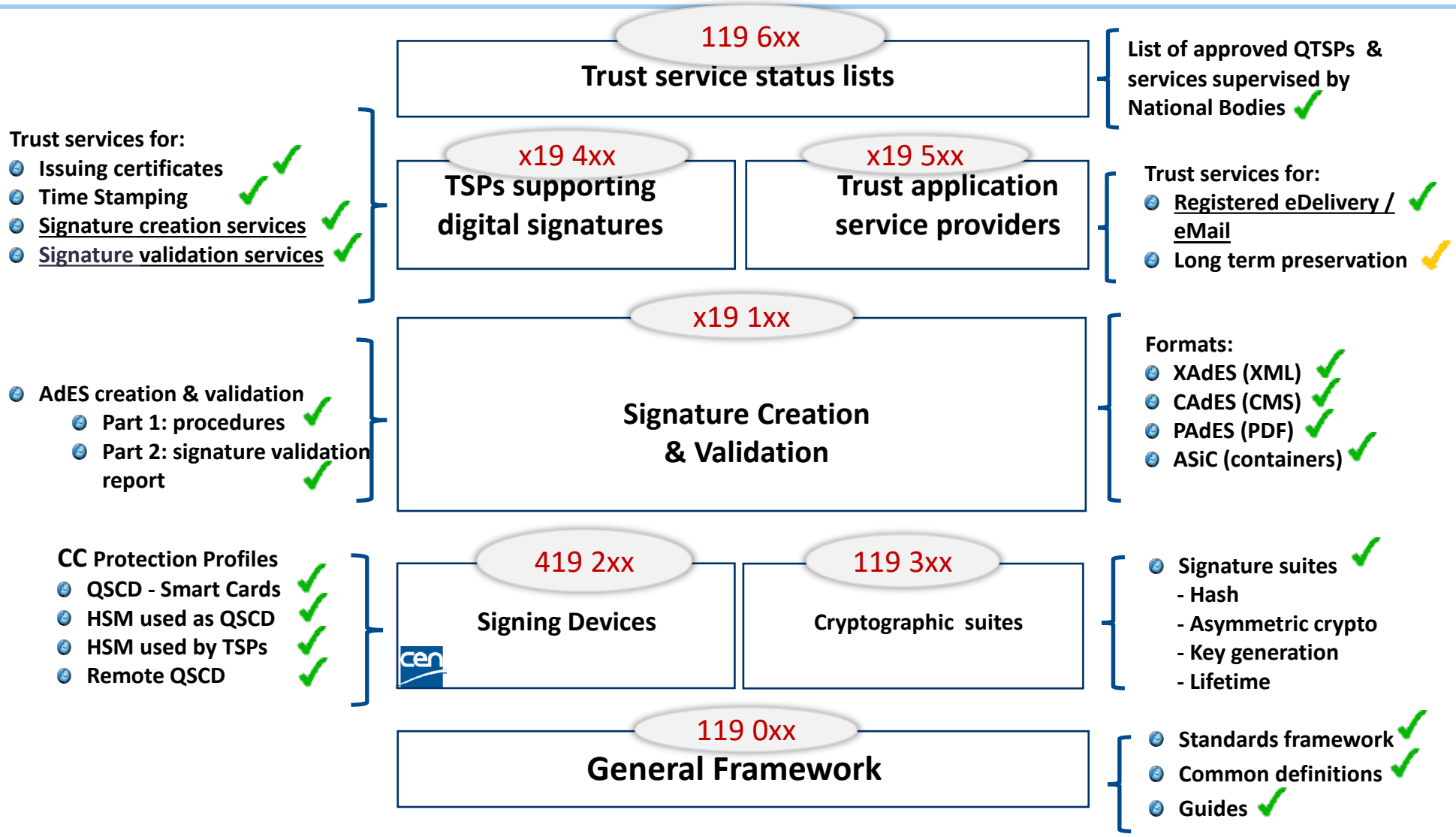
(Slide from Andrea Servida; EU Commission; Head of DG CONNECT H4 - “eGovernment and Trust”)

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

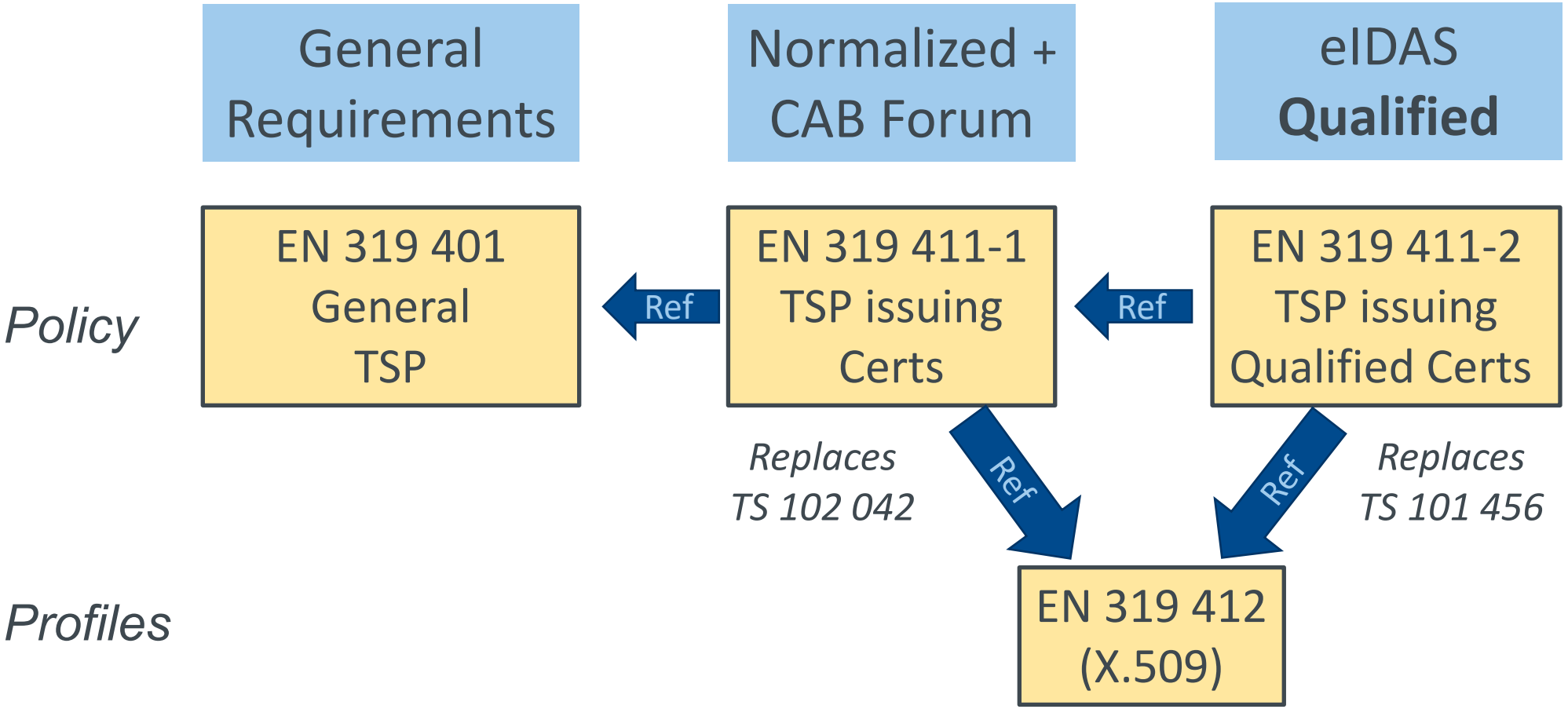
eIDAS Standards Framework: Published Standards



Standards framework complete – excepting preservation which is draft

TSP Requirements

Trust services issuing certificates: ETSI standards overview



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

Multiple detailed changes to clarify requirements including;

- Trust service components (subcontracted components e.g. RA, server signing ….)
- Alignment with Short term certificates, and opening RFC 5280 size limits in EN 319 412-x
- Re-wording existing requirements, clarifying terminology
- Alignment of 411-1 requirements with 411-2, some general requirements moved from 411-2 to 411-1.

Changes agreed: EN 319 401: 12, EN 319 411-1: 22, EN 319 411-2: 4

2 or 3 changes under discussion

Updated draft ENs to be published Q3/Q4 2020

Certificate Profiles (Updates)

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

Browser / QWAC Alignment

Proposal from Google and Mozilla:

- Remove Specific Requirements link QWAC to Transport Layer Security (TLS/SSL) protocol
- Split QWAC into DV Certificate and ntQWAC (non TLS QWAC)

ETSI Response:

- Enabling website authentication using TLS is an essential requirement of QWACs
- Could split certificates into DV Certificate and non-tlsQWAC but ….:
  - Still need cryptographic link from non-tlsQWAC to DV Cert as EU requirements cover both
  - Yet to fully understand implications of split responsibility for Liability, Audit, Security…….
- Suggested alternative keep single certificate and split requirements:
  - Certificate contents:

    Browsers: domain validation content (as per CABF Baseline)

    EU: natural / legal person identity
  - Certificate validation

    Browsers: Validation against Browser Root Store

    EU: Validation against Trusted List

Signature Formats & Validation

JSON Signatures

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

JSON Web Signature profile for Open Banking based on JAdES

https://www.openbankingeurope.eu/media/1735/preta-obe-jws-stable-draft.pdf

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 – See later
- TS 119 615: Procedures for using and interpreting European Union Member States national trusted lists – See Later

Remote Signing & CEN Standards

Remote Signing & CEN Standards for Trustworthy Systems

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

ETSI Signature Creation Protocols & TSP Component Policy Requirements

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

Electronic Registered Delivery and Registered Electronic Mail

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
- TS 119 512 Protocols for trust service providers providing long-term data preservation services (Published)

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
  - Publication expected Q4 or 2021

Trusted Lists

Trusted Lists

- TS 119 615 Final draft updated following plugtests
  - on the use of information within an 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
  - Draft awaiting publication of updated rules regarding managing issuance of EU Trusted Lists
- TS 119 172-4: Signature Validation Policy for European Qualified Electronic Signatures/Seals Using Trusted Lists – Draft to be completed following TS 119 615

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

Minor editorial changes final ratification due Mid June

Supplements to EN 319 403 TSP Audit Requirements

- TS 119 403-2 (2019-03): Part 2: Additional requirements for Conformity Assessment Bodies auditing Trust Service Providers that issue Publicly-Trusted Certificates (as in CA/Browser Forum)
  - Minor updates being proposed
- 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

New Activities

Globalisation Study Report (TR 103 684)

Establishing liaisons with Asia PKI, Japan and Arab ICT Organisation to take findings forward

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