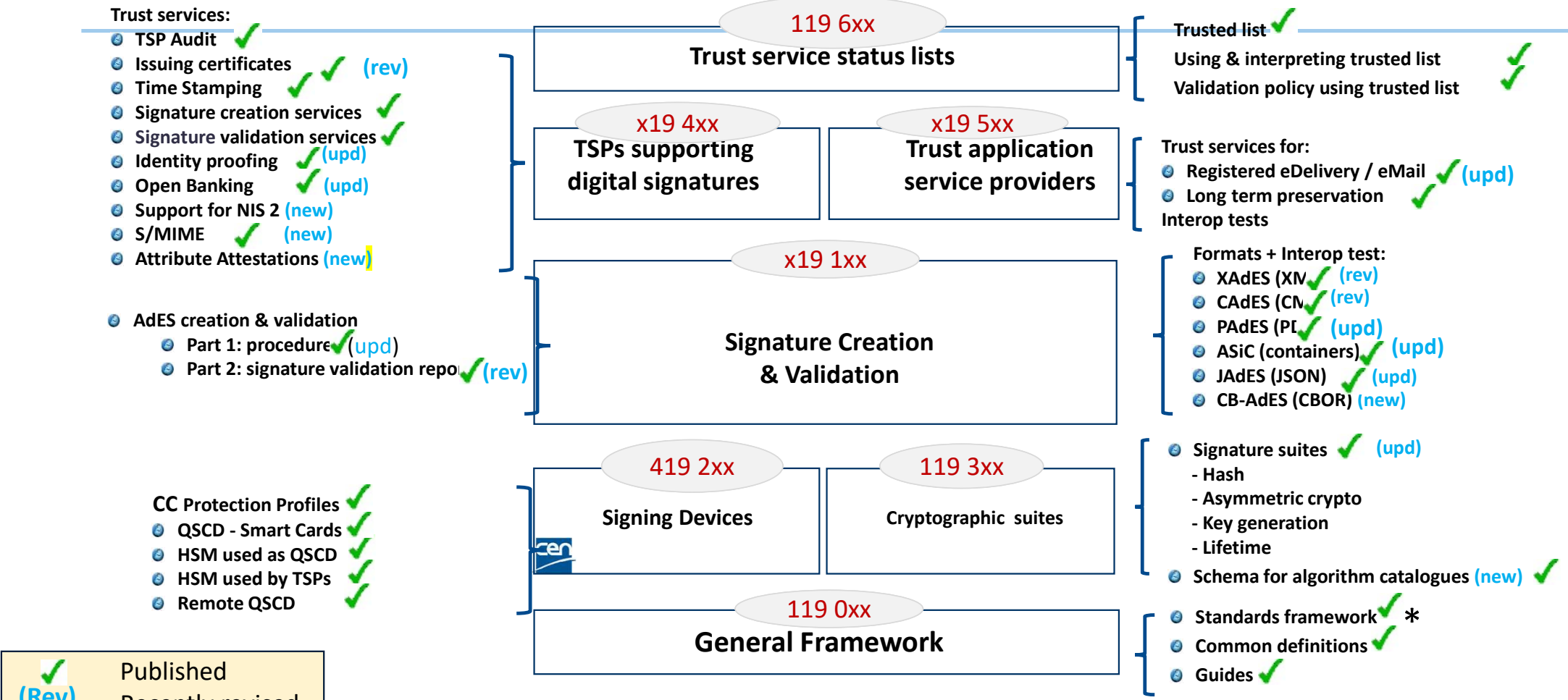
ETSI Standards Update

CA/B-Forum Boston– October 2023

Presented by: **Arno Fiedler – Vice Chair ETSI ESI**

arno.fiedler@outlook.com

ETSI & CEN Standards supporting eIDAS – the overall picture



✓	Published
(Rev)	Recently revised
(Upd)	Update in progress
(New)	New

Trust services issuing certificates

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

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

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

✓ Completed
* Update in pro
(new) New

- EN 319 411-x Cert Policies: ETSI Approved – EN Approval aim 6 Oct
  - Part 1: 16 changes to policies for issuing certificates
  - Part 2: 5 changes to policies for issuing qualified certificates
  - Alignment with CA/Browser Forum
- EN 319 412-x Cert Profiles: ETSI Approved – EN Approval aim 6 Oct
  - 1 changes to EN 319 412-1 (General) & 7 changes EN 319 412-2 (Certificates issued to natural persons)
  - EN 319 412-4 (Website authentication) CA/Browser Forum alignment
- TR 119 411-5 Co-existence Browser Root store and EU Trust List (QWAC)
  Discussions continue on 2 certificate approach
- TS 119 411-6 alignment with CA/Browser forum S/MIME certificates
  Published

Trust services issuing certificates
CA/ Browser Forum Alignment & QWAC Policies

Q-EVCP-w:

- Fully aligned with the CA/Browser forum Guidelines for the Issuance and Management of Extended Validation Certificates
- Meets the requirements for EU qualified certificate

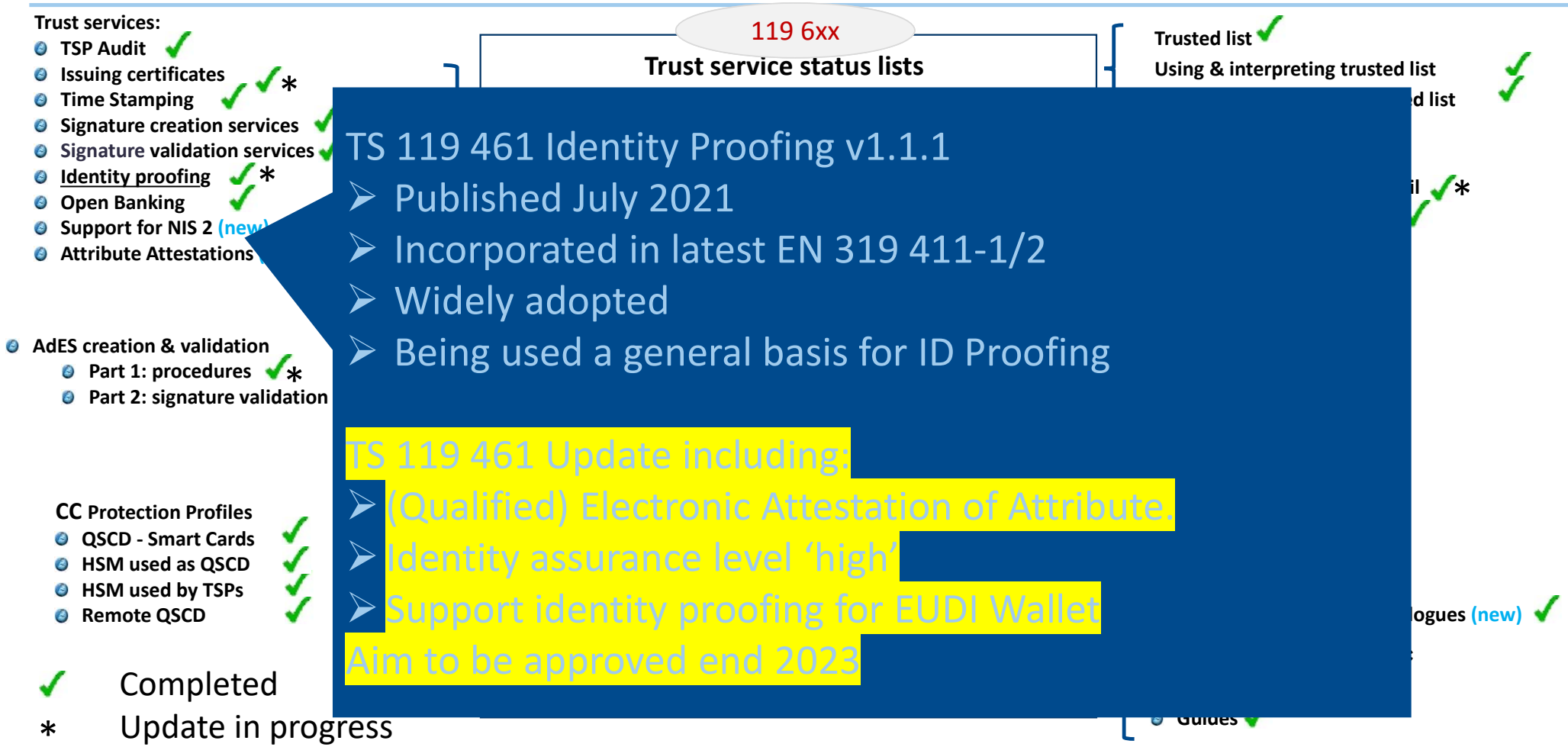
QNCP-w:

- Fully aligned with the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates
- Meets the requirements for EU qualified certificate

QNCP-w-gen:

- Specific requirements for domain name validation as specified by CA/Browser Forum
- Meets requirements for EU qualified certificates.

Trust Services – ID Proofing



Trust Services & NIS 2

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

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

✓ Completed
* Update in prog
(new) New

NIS2 and Trust Services:

- Revised EN 319 401: General Policy Requirements for Trust Service Providers, Aim to specify in a way which does not require update to existing trust service standards

Aim to be available for National EN approval Nov 2023

Signature creation and Validation

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 ✓

ETSI eSignature Validation Plugtests May-July 2022

Plugtest on LTA (Long-Term Archive) formats

23 October to 24 November 2023

Revised EN 319 102-1 signature creation and validation

Aim to be available for National EN approval Q4 2023

✓ Completed

* Update in progress

(new) New

Signature formats

Revised EN 319 122-1 CMS AdES baseline
- Published

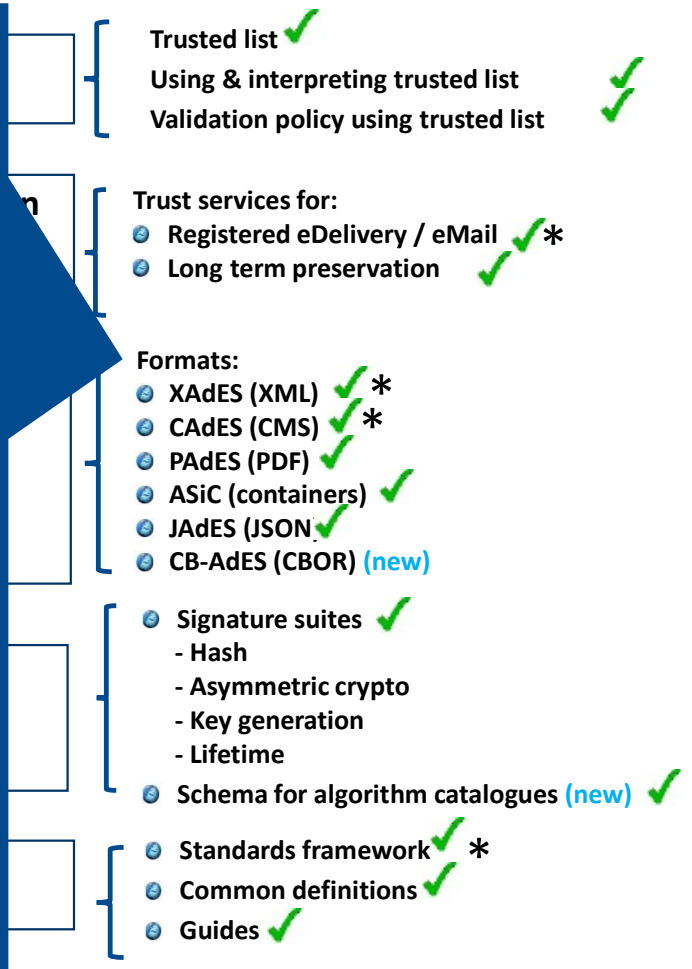
Revised EN 319 132-1 XML AdES baseline
- Also update with simplified validation data attribute (similar to PAdES & CAdES)
- Aim for ETSI Approval Q4 then EN Approval early 2024

Revised TS 119 142- PDF AdES baseline
- Aim for ETSI Approval Q4 then EN Approval early 2024

Revised EN 319 162-1 AsiC (container) baseline
- Aim for ETSI Approval Q4 then EN Approval early 2024

Revised TS 119 182-1 JSON AdES baseline
- Aim for Publicatiion Q4

New TS 119 152-1 CBOR ADES
- Aim for Publicatiion Q4

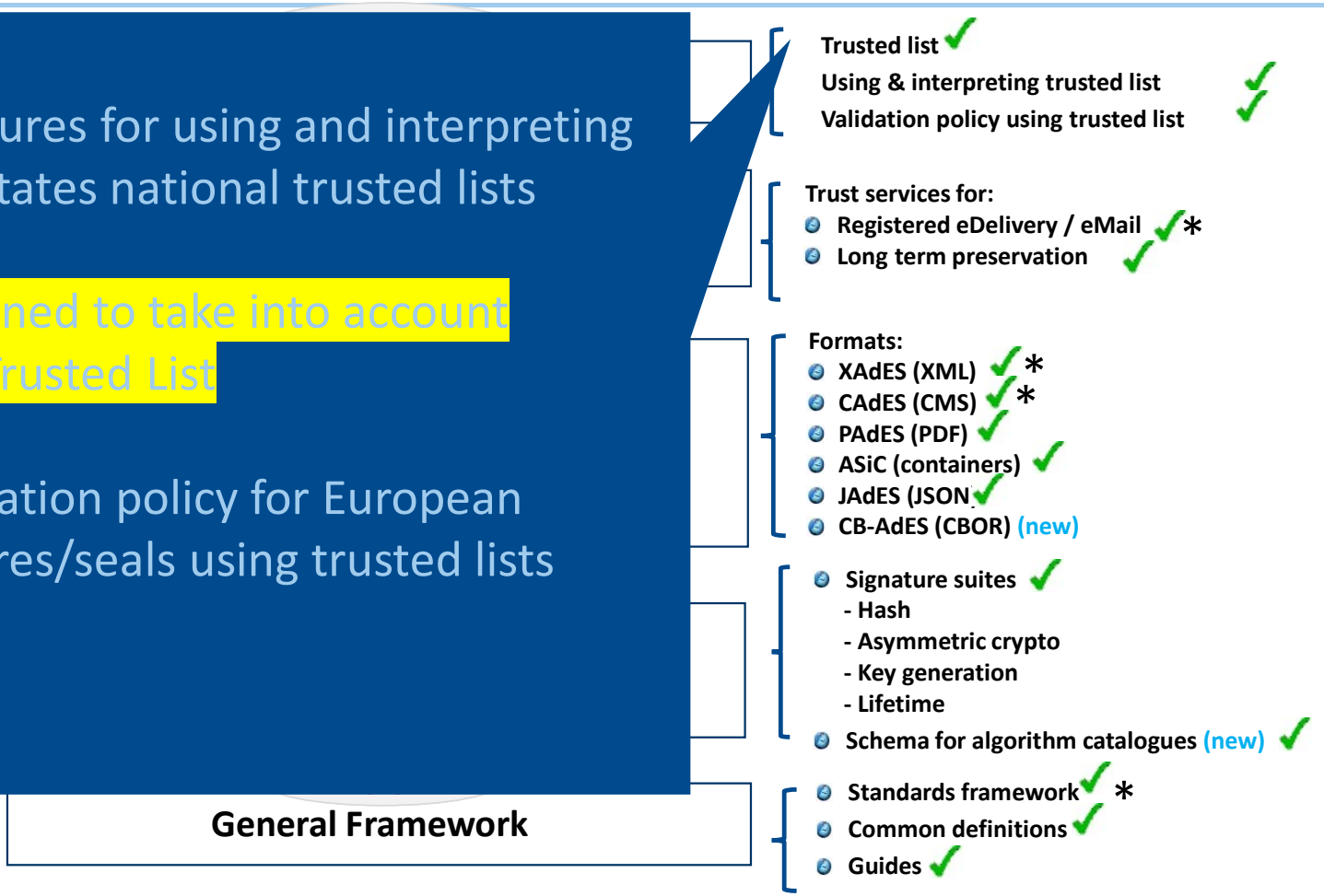


Use of Trusted Lists

Revised TS 119 615: Procedures for using and interpreting European Union Member States national trusted lists

- Published
- Further updates planned to take into account Third Country AdES Trusted List

Revised TS 119 172-4: Validation policy for European qualified electronic signatures/seals using trusted lists



✓ Completed

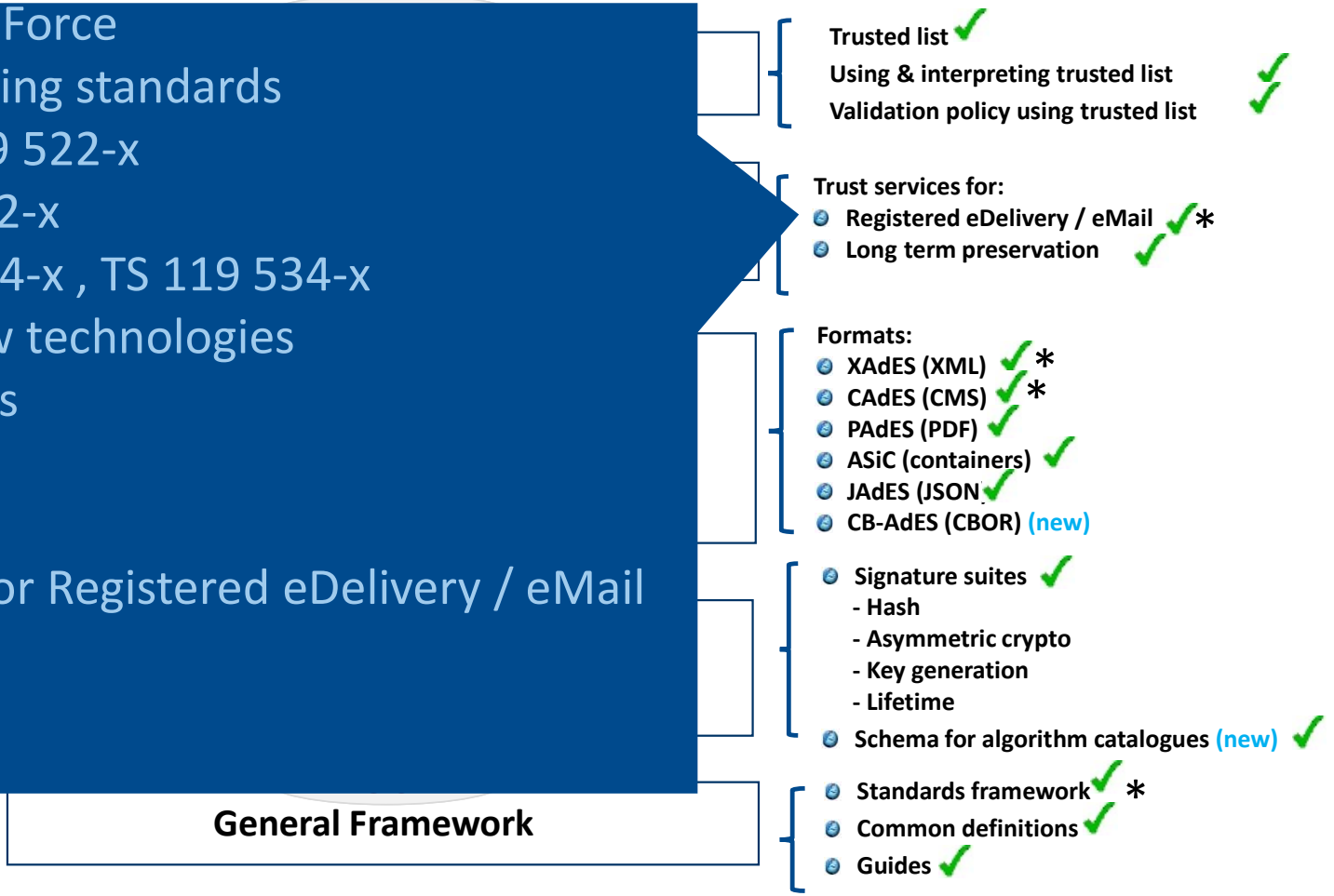
* Update in progress

(new) New

Next Generation Electronic Registered Delivery Services (inc Registered eMail)

ETSI Funded Specialist Task Force

- Maintenance of existing standards
  - eDelivery: EN 319 522-x
  - eMail: EN 319 532-x
  - Testing TS 119 524-x , TS 119 534-x
- Study into use of new technologies
  - Electronic Ledgers
  - eID
  - …
- Revised framework for Registered eDelivery / eMail standards

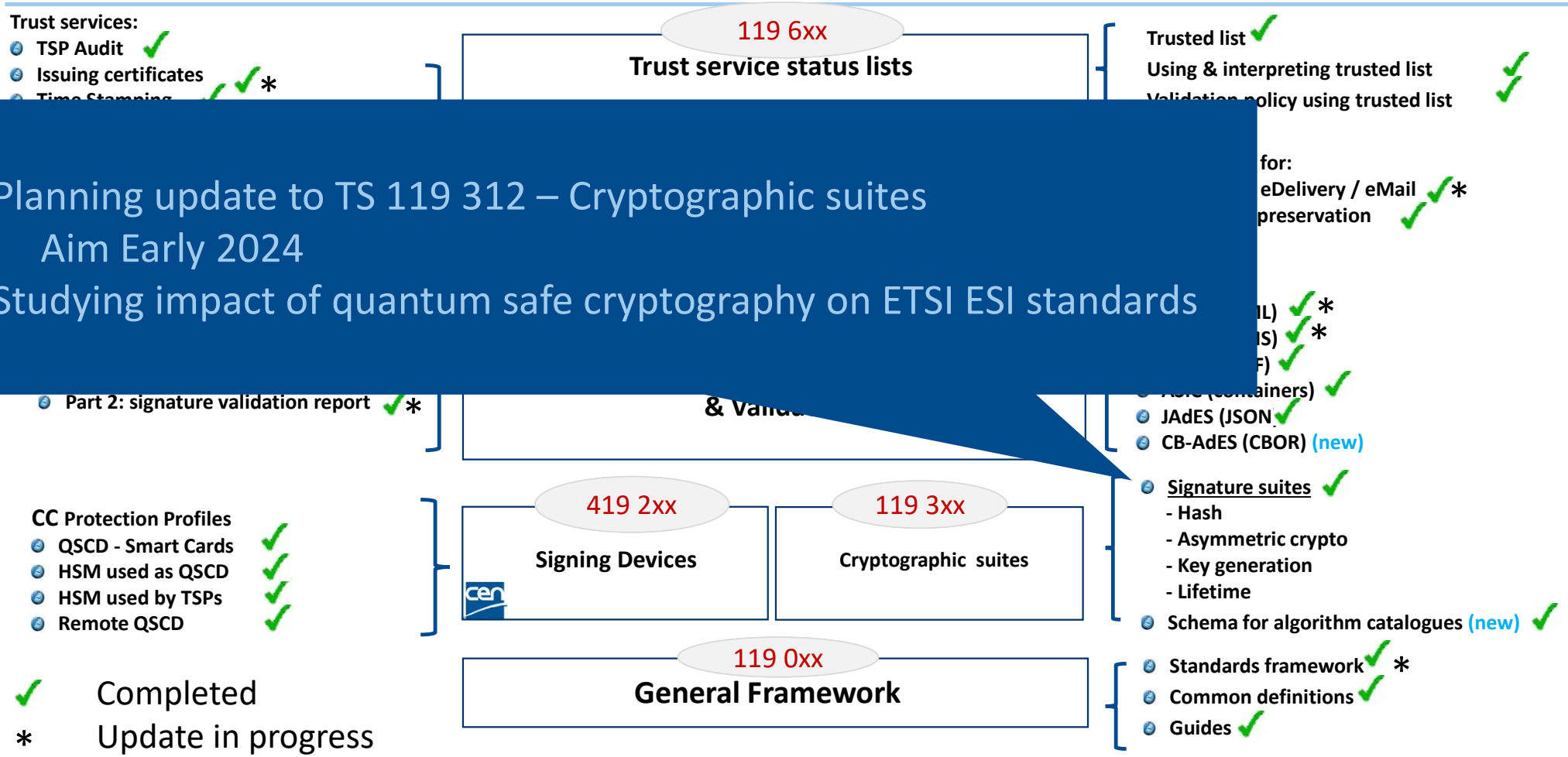


✓ Completed

* Update in progress

(new) New

Cryptographic suites



- Planning update to TS 119 312 – Cryptographic suites
  Aim Early 2024
- Studying impact of quantum safe cryptography on ETSI ESI standards

✓ Completed
* Update in progress
(new) New

ETSI releases standard for IT solution providers to comply with EU regulation on electronic signatures in email messages

Sophia Antipolis, 20 September 2023

ETSI has published a new standard on "Requirements for trust service providers issuing publicly trusted S/MIME certificates" (ETSI TS 119 411-6) helping Trust Service Providers comply with new standards for S/MIME certificates that are enforced since 1 September 2023. Secure MIME (S/MIME) certificates are used to sign, verify, encrypt, and decrypt email messages.

Since the 1st of September 2023, all TSPs issuing digital certificates used for S/MIME that are publicly trusted in certain operating systems and root certificate programs must comply with the S/MIME Baseline Requirements published by the CA/Browser Forum. The new ETSI standard will assist Trust Service Providers in asserting their compliance, when required. It will enable the same public key certificate used for signing electronic mail accepted by major IT solution providers (e.g., Microsoft, Apple, Google) to be also recognized as meeting the EU requirements for electronic signatures, issued to individual persons, and electronic seals, issued to organizations.

This new standard supports the EU regulation for electronic identities, authentication, and signatures (eIDAS – Regulation (EU) 910/2014) and builds on the policy requirements for Trust Service Providers (TSPs), the ETSI EN 319 411 series of standards used for eIDAS audits.

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