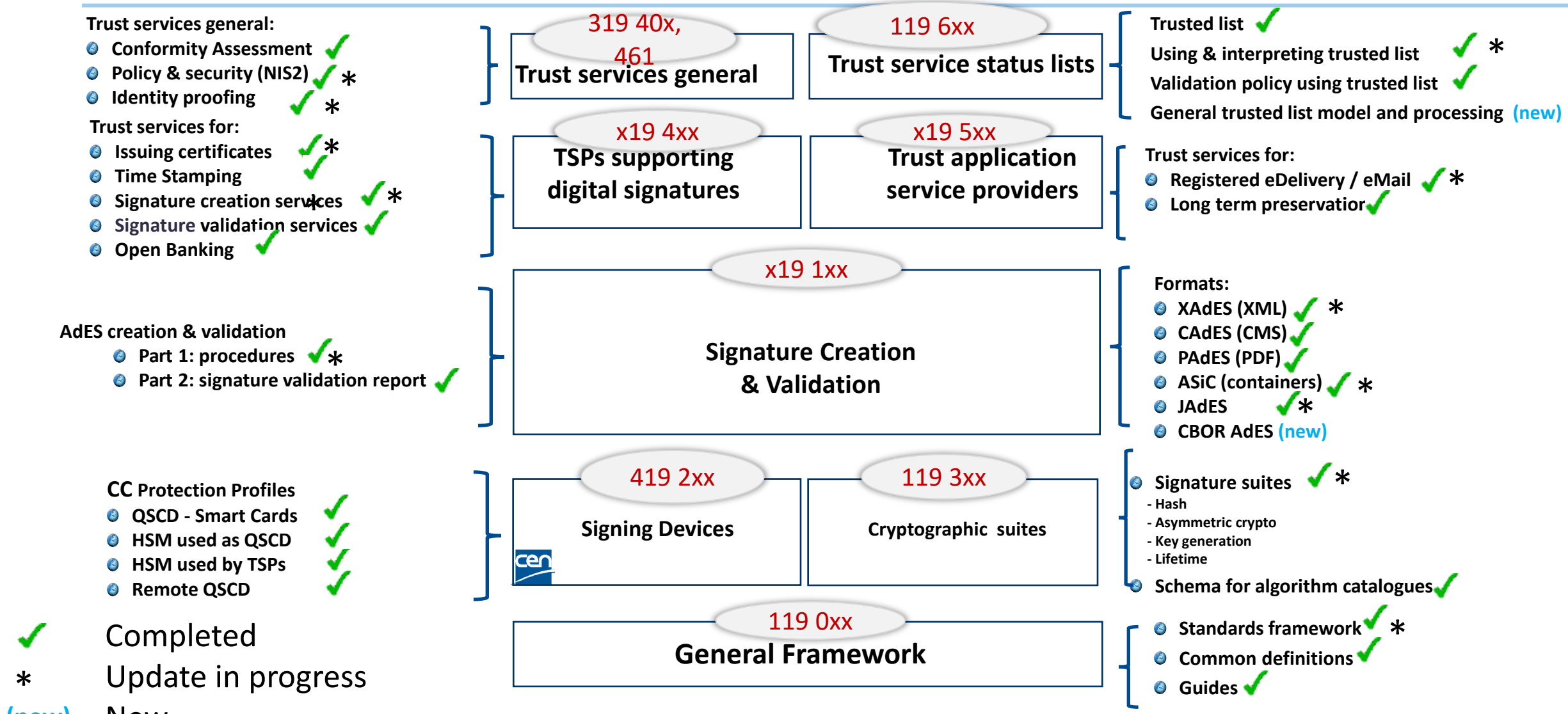
ETSI Standards Update

CAB Forum – October 2024

Presented by: Arno Fiedler – Vice chair ETSI ESI

Maintenance of Existing Standards



✓ Completed

* Update in progress

(new) New

EN 319 401 – General Policy Requirements for TSPs

Update aimed to align with NIS2

- New version 3.1.1 published 2024-06
- Once NIS2 implementing act available aim to update EN 319 401 to fully align

Updated EN 319 401 incorporated by reference from all TSP Policy standards

- EN 319 411-1 which follows RFC 3647 framework for cybersecurity requires updates, similarly TS 119 431
- Other standards which follow general topics structure unaffected.

Supports ACAB'c strategy for single audit covering NIS2 and eIDAS

TS 119 461: Identity Proofing

- New Extended LoIP (Level of Identity Proofing)

- Strengthening requirements for threats and risk assessment and for keeping solutions up to date
  - Threats intelligence process, pointing at ENISA “Methodology for sectoral cybersecurity assessments” as a hint towards future cybersecurity certification requirements

- Adding requirements to enhance Baseline LoIP to reach Extended LoIP

- New Annex C on requirements for identity proofing for eIDAS qualified trust services
  - Qualified certificates according to eIDAS v1
  - Qualified certificates and qualified electronic attestation of attributes for eIDAS v2
  - Qualified registered delivery same for eIDAS v1 and eIDAS v2

- Aim to reference CEN standard on biometric injection attack detection for remote registration

Aim for publication before year end

EN 319 411-1/2 Certificate Policy Updates

- EN 319 411-1 General Requirements
  - Key ceremonies
  - Identify last CRL issued (on termination)
  - Alignment with EN 319 401 NIS2 version

- EN 319 411-2 Qualified
  - Support for validity assured / short term certificates
  - Alignment with CAB Forum Extended Validation

EN 319 412-x Certificate Profile Updates

- EN 319 412-1
  - NTR trade identified region identifier
  - Last CRL issued (on termination)
  - Alignment with EN 319 401 NIS2 version
- EN 319 412-2 Natural person
  - Status services for validity assured / short term certificates
  - Clarification on identification common name vs given name and pseudonym
  - CAB Forum OCSP alignment
- EN 319 412-5 QC Statement
  - QC Statement on verification method (whether have used QES)
  - ASN.1 encoding of non-EU QSCD

eSignature/ eSeal Standards - formats

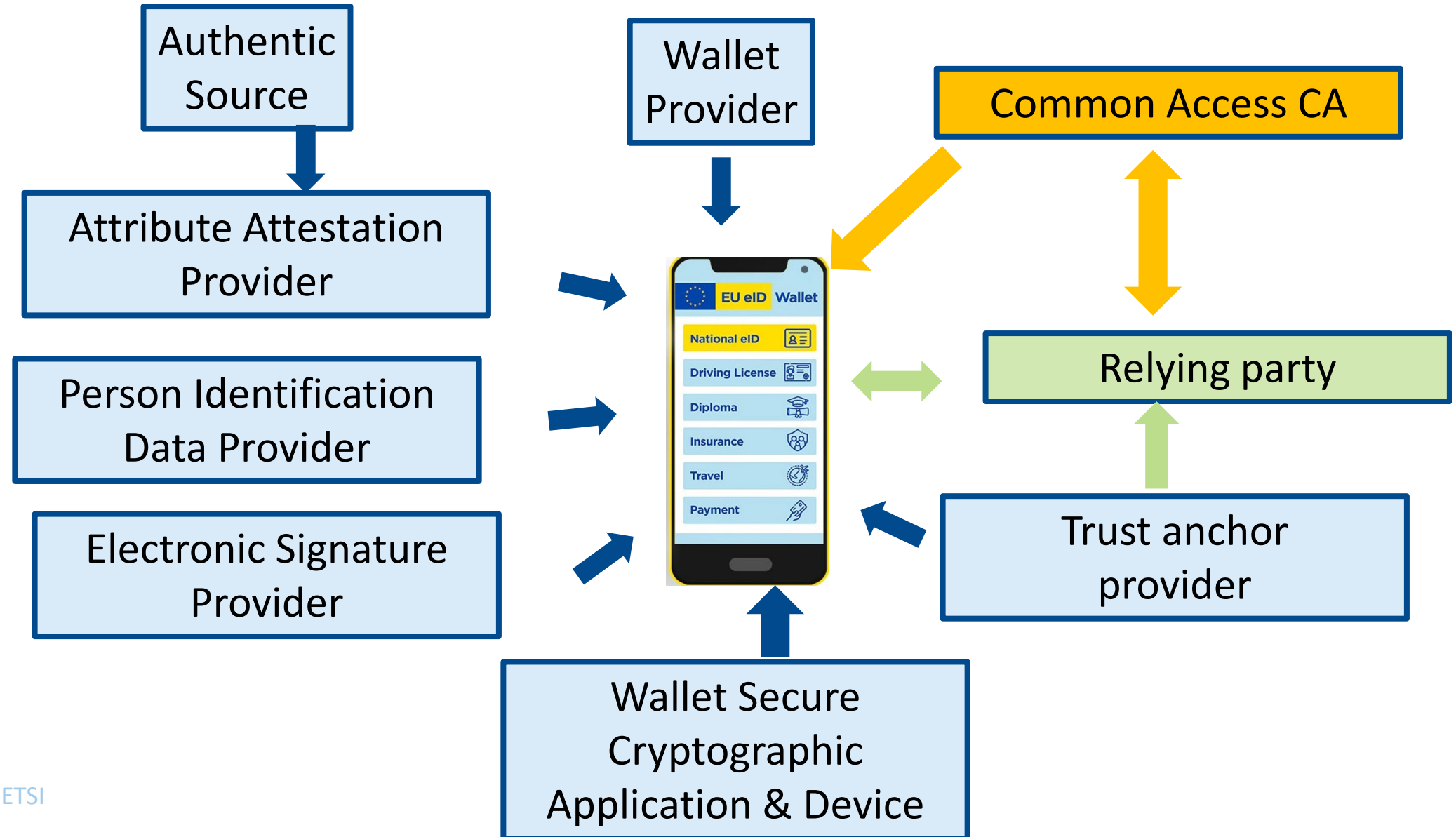
- EN 319 122-1: CAdES
  - No changes since v1.3.1 published 2023-06
- EN 319 132-1 XAdES (XML)
  - Changes includes update to archive timestamp
  - New v1.3.1 published 2024-07
- EN 319 162-1 Associated Signature Container (ASiC)
  - Adding alternative forms (e.g. time assertion),
- TS 119 182 JAdES (JSON)
  - Changes includes replacing claimed signing time: *sigT* with *iat* to facilitate IETF alignment
  - New v1.2.1 published 2024-07
- TS 119 152 CB-AdES (CBOR)
  - Awaiting IETF allocation of numbers to new header parameters
  - Aim publication Q4

eSignature/ eSeal Standards – Signature validation

- EN 319 102-1: AdES Signature creation and Validation
  - 17 Detailed changes
  - New v1.4.1 published 2024-06

- TS 119 172-4 -1: Validation Policy on EU Qualified e-Seals and e-Signatures
  - Remain open issue on revocation checks on preserved signatures

Main components and Interfaces for EUDI Wallet



ETSI TS 119 411-5 (early draft)

The TS defines multiple approaches for issuing qualified certificates for website authentication, deploying them to websites, and their consumption by user agents.

- 1. “1-QWAC Approach”: Single certificate that meets both browser root store **and** EU Qualified requirements both aligned with CA/Browser Forum requirements
- 2. “2-QWAC with Certificate Binding Validation Approach”
  - EU Qualified Certificate signed binding to TLS Certificate
  - + TLS Certificate meets browser root store requirements aligned with CA/Browser Forum requirements
  - Browser validates TLS Certificate against binding
- 3. “2-QWAC without Certificate Binding Validation Approach” (aka 2b)
  - As 2. but browser does not validate the TLS Certificate against binding

Further information

FESA/ECATS “Forum of European Supervisory Authorities for Trust Service” offer take an active part at the next CA/B-Forum Meeting in Tokyo

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