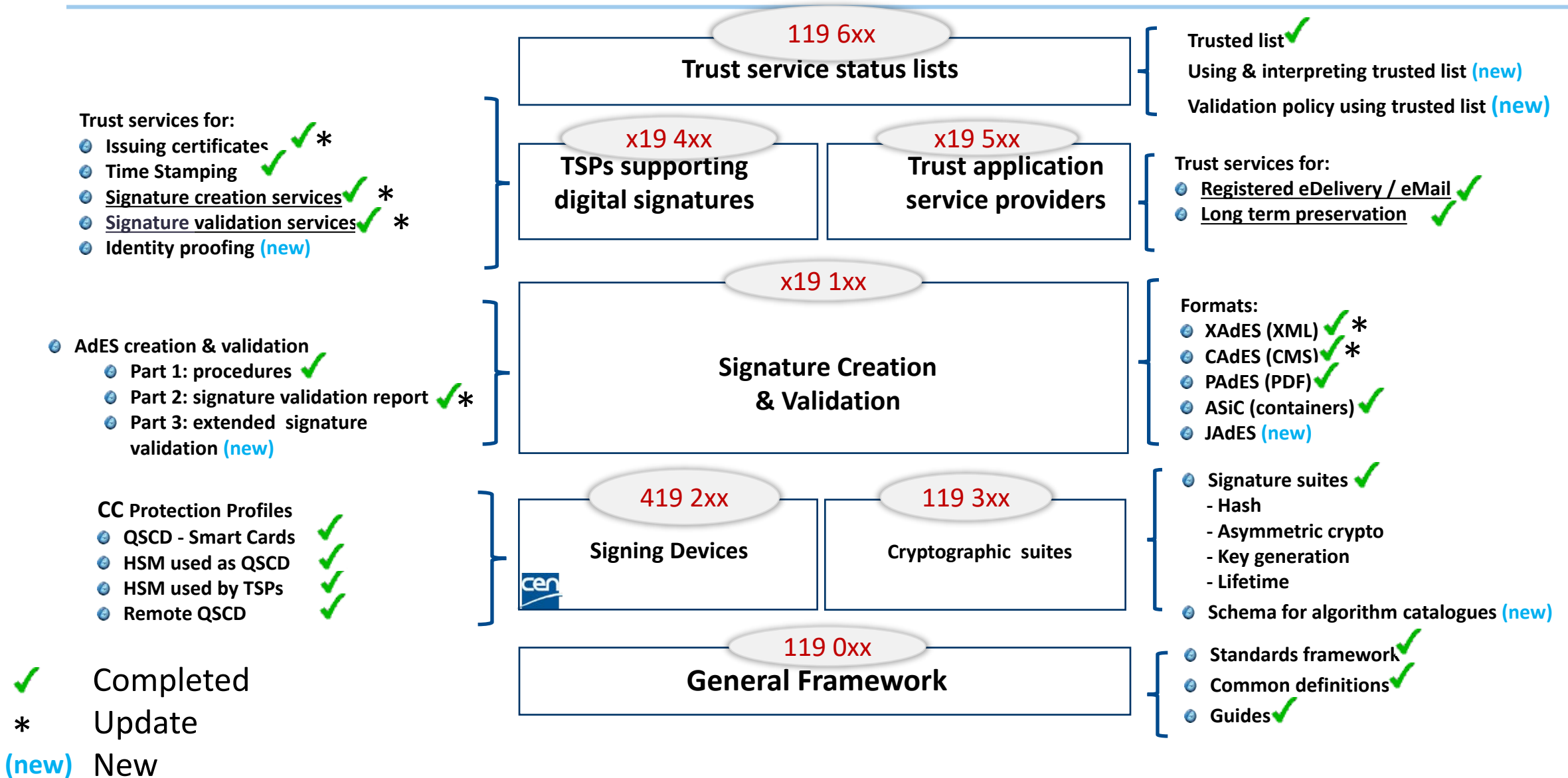# ETSI ESI Activities Update
CA/B-Forum 2020-10-22

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

ETSI & CEN Standards supporting eIDAS – the overall picture

Trust services for:
- Issuing certificates ✔ *
- Time Stamping ✔
- Signature creation services ✔ *
- Signature validation services ✔ *
- Identity proofing (new)

AdES creation & validation
- Part 1: procedures ✔
- Part 2: signature validation report ✔ *
- Part 3: extended signature validation (new)

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 (new)
- Validation policy using trusted list (new)

x19 4xx
TSPs supporting digital signatures

x19 5xx
Trust application service providers

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

x19 1xx
Signature Creation & Validation

Formats:
- XAdES (XML) ✔ *
- CAdES (CMS) ✔ *
- PAdES (PDF) ✔
- ASiC (containers) ✔
- JAdES (new)

419 2xx
Signing Devices

cen

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
(new) New

2

Trust services issuing certificates – Updates
EN 319 401, EN 319 411-1 & EN 319 411-2 – Policy requirements

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

- Use of EU Trusted List by relying parties

EN 319 401: 14 Changes, EN 319 411-1: 25 Changes, EN 319 411-2: 4 Changes

Draft EN October / November

Trust services issuing certificates – Updates
EN319 412-1,-2,-3,-5 Certificate profiles

TS/EN 319 412-1: General
- Placement of eID information to Certificate Profile,
- Indicator of "short term" certificates
- Use of 'EL' as alternative to country code 'GR'

EN 319 412-2: Natural persons & 412-3 Legal persons
- Clarification Key Usage indicator
- Clarification Authority information access
- Removal on RFC 5280 64 character limit on naming fields, (if documented in CPS)

EN 319 412-5: Qualified Certificate Statements
- Facilitate QC Statements by non-EU Qualified certificates

Published

Trust Service Provider Conformity Assessment: Updates on TS119 403-2

ETSI TS 119 403-2 (2020-10): "Trust Service Provider Conformity Assessment;
Part 2: Additional requirements for Conformity Assessment Bodies auditing Trust Service Providers that issue Publicly-Trusted Certificates"

- developed in close cooperation with ACABc,

- with six updates on requirements for audit attestations, e.g.

  - Definition of audit dates and hash values

  - Responsibility for registration services

  - Statements about non-conformities and CA Incidents

- agreed by ETSI ESI on 19.10.2020; published latest 15.11.20

Trusted List
TS 119 612 – Use and interpretation

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

- ➢ 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
- ➢ Publication depends on clarification of EU Official Journal announcement regarding use of "compiled list" / pivot List of Trusted Lists.

Draft TS 119 172-4: Signature Validation Policy for European Qualified Electronic Signatures / Seals Using Trusted Lists

Awaiting EU Official Journal publication regarding EU list of trusted lists.

Extended Signature Validation

TS 119 102-3 Extended signature validation procedures aim to avoid the risks in accepting documents whose signature validates but the data format can lead to misinterpretation of the content (e.g. change in appearance due to macros within the document without changing the signed bytes)

Sub part 1: General

Sub part 2: Signed PDF (PAdES)

Sub part 3: Signed XML (XAdES)

Sub part 4: ASiC packages

Publication Q4 2021

TS 119 152 JAdES digital signatures

➢ Based on JSON Web Signatures RFC 7515

➢ Separate Profile of JAdES for open banking being developed jointly with Open Banking Europe

➢ Publication due end 2020