European standardisation framework for trust services

BITKOM eIDAS Summit

Presented by:	**Andreas Weise**	For:	13.06.2019
	D-TRUST GmbH		

Agenda

- eIDAS Standards Roadmap

- Trust Service Standards

- Electronic signatures and seals
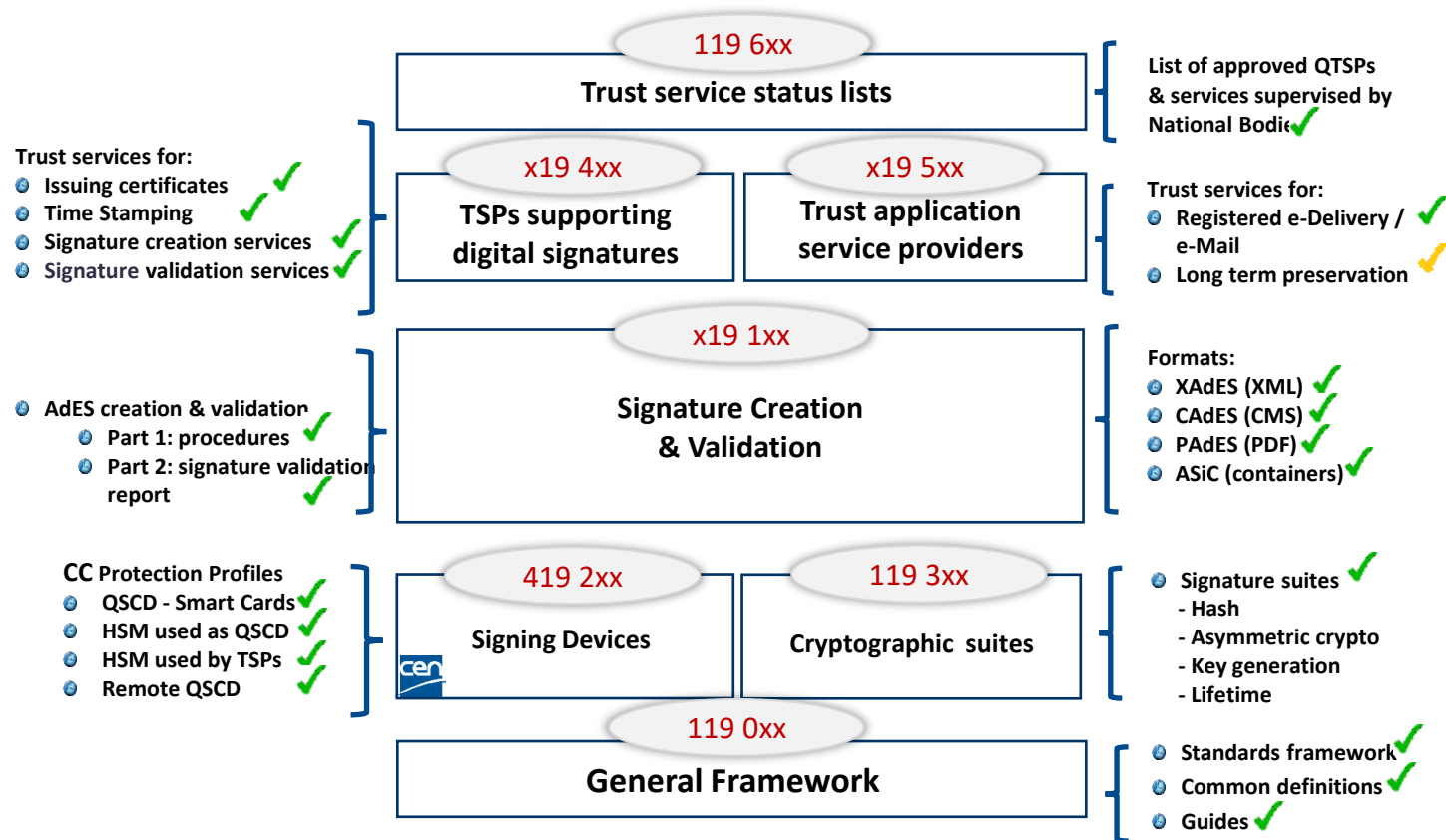
- Trusted Lists

- Conformity Assessment

- Conclusions

eIDAS
Standards
Roadmap

eIDAS Strategic Goals

TRUST

CONVENIENCE

eIDAS

CROSS-BORDER

SEAMLESS

eIDAS Standards Framework:
Published Standards

ETSI

119 6xx

Trust service status lists

List of approved QTSPs & services supervised by National Bodies ✔

Trust services for:
- Issuing certificates ✔
- Time Stamping ✔
- Signature creation services ✔
- Signature validation services ✔

x19 4xx

TSPs supporting digital signatures

x19 5xx

Trust application service providers

Trust services for:
- Registered e-Delivery / e-Mail ✔
- Long term preservation ✔

x19 1xx

AdES creation & validation ✔
- Part 1: procedures ✔
- Part 2: signature validation report ✔

Signature Creation & Validation

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

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

419 2xx

Signing Devices

cen

119 3xx

Cryptographic suites

- Signature suites ✔
  - Hash
  - Asymmetric crypto
  - Key generation
  - Lifetime

119 0xx

General Framework

- Standards framework ✔
- Common definitions ✔
- Guides ✔

Trust services issuing certificates

Trust service issuing certificates

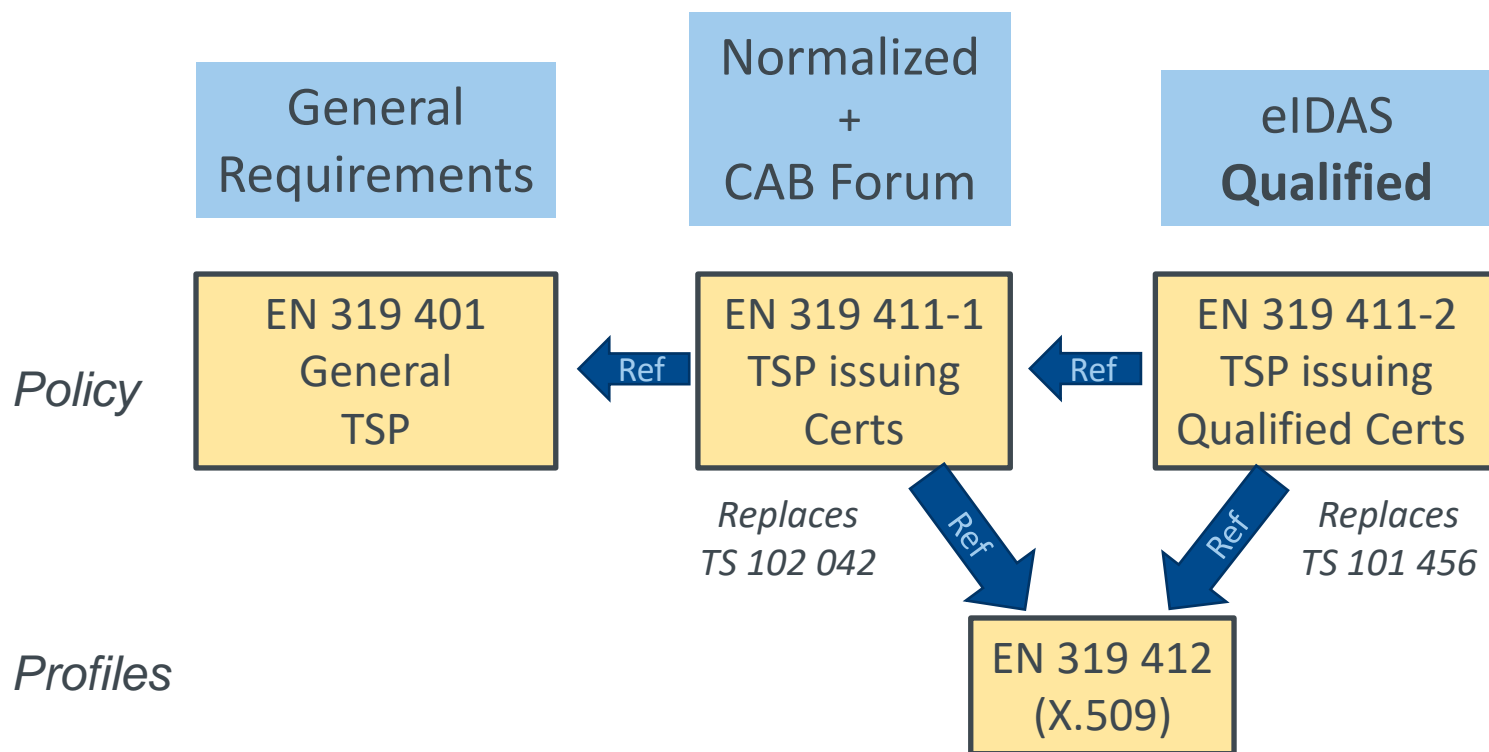**e-Signatures**

- For use by <u>natural</u> persons

e-Seals

- For use by <u>legal</u> persons
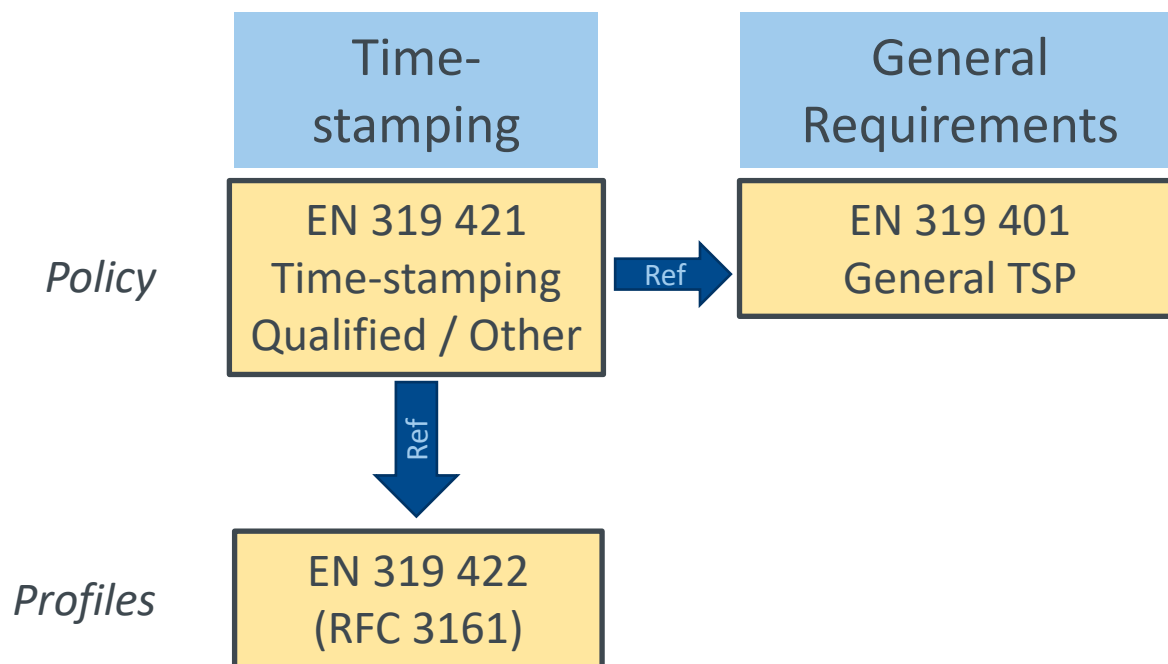
Website authentication

- For websites

Trust services issuing certificates: ETSI standards overview

General Requirements	Normalized + CAB Forum	eIDAS **Qualified**

Policy

EN 319 401 General TSP	←Ref— EN 319 411-1 TSP issuing Certs	←Ref— EN 319 411-2 TSP issuing Qualified Certs

Replaces TS 102 042

Replaces TS 101 456

Profiles

EN 319 412 (X.509)

Ref → ← Ref

Timestamping

ETSI Time-Stamping Standards

Time-stamping

General Requirements

Policy

EN 319 421
Time-stamping
Qualified / Other

— Ref → EN 319 401
General TSP

↓ Ref

Profiles

EN 319 422
(RFC 3161)

Signatures
and Seals

eIDAS, Signatures & Seals

Legal differences addressed by common technical solution:

Electronic signature is for *natural* persons

eIDAS Art. 3(10) "data in electronic form, which is attached to or logically associated with other data in electronic form and which is
used by the signatory to sign"

(a) uniquely linked to the signatory;

(b) capable of identifying the signatory;

(c) created [...] with a high level of confidence, use under his sole control; and

(d) linked [...] in such a way that any subsequent change in the data is detectable.

Electronic seal is for *legal* persons

eIDAS Art. 3(25) "data in electronic form, which is attached to or logically associated with other data in electronic form to
ensure the latter's (electronic data) origin and integrity"

(a) uniquely linked to the creator of the seal;

(b) capable of identifying the creator of the seal;

(c) created [...] with a high level of confidence under its control, use for electronic seal creation; and

(d) linked [...] in such a way that any subsequent change in the data is detectable.

Signature Formats for
Advanced / Qualified Electronic Signatures / seals

- ETSI EN 319 122: : CAdES Digital signatures for binary data objects

- ETSI EN 319 132: XAdES Digital signatures for XML format documents

- ETSI EN 319 142: PAdES Digital signatures for PDF format documents

- ETSI EN 319 162: ASiC Associated Signature Container for ZIP package with signature

- Under development: JAdES Digital signatures for JSON data objects
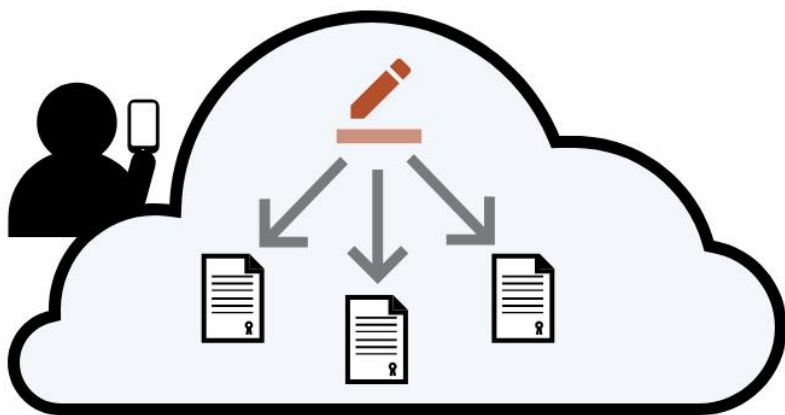
Signature
Enhanced
Services

Signature Enhanced Trust Services

Remote Signing

Validation Services

Long-term Preservation

Signatures: Remote Signing

- **ETSI TS 119 431-1**

  Policy and Security Requirements for TSP Service Components Operating a Remote QSCD / SCD

- **ETSI TS 119 431-2**

  Policy and Security Requirements for TSP Service Components Supporting AdES Digital Signature Creation

- **ETSI TS 119 432**

  Protocols for Remote Digital Signature Creation

Trust services issuing certificates:
Scope of Remote Signing Standards

ETSI

User

Signer Interaction Component

EN 419 241-1 cen

EN 419 241-2 (qualified only) cen

Tamper Protected Environment

Server Signing Application

Signature Activation Module

Crypto. Module

TSP Service Component operating remote QSCD / SCD

TS 119 432 (protocol)

TS 119 431 (policy requirements)

EN 419 221-5 cen

Delegated Authentication

Registration

Certificate Issuance

Revocation Management

Signatures: Validation – cloud based signature validation

ETSI TS 119 441

Policy requirements for TSP providing signature validation services

ETSI TS 119 442

Protocol profiles for trust service providers providing AdES digital signature validation services

Signatures: Preservation Services

2019-2020-2021-2022-2023-2024-2025...

∨ **ETSI 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 *(draft)*

∨ **ETSI TS 119 512**

Protocols for trust service providers providing long-term data preservation services *(draft)*

Electronic
Registered
Delivery
& REM

Electronic Registered Delivery (ERDS) and Registered Electronic Mail (REM)
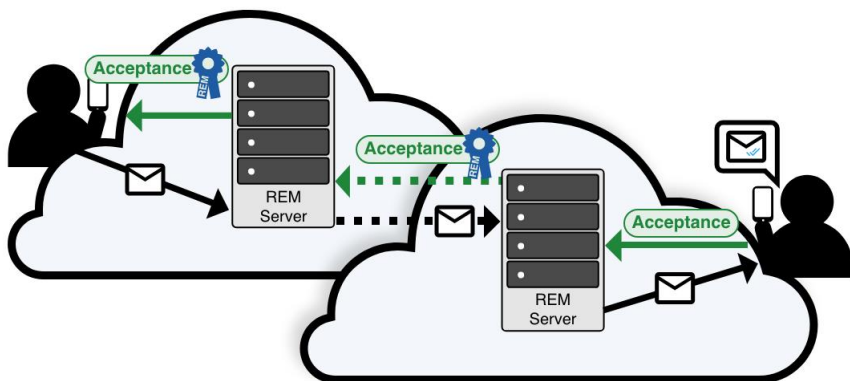
▽ **ETSI EN 319 522**

Electronic Registered Delivery Services (ERDS)

▽ **ETSI EN 319 532**

Registered Electronic Mail (REM) Services (Supersedes ETSI TS 102 640)

▽ **ETSI EN 319 521**

Policy and Security Requirements for Electronic Registered Delivery Service Providers

▽ **ETSI EN 319 531**

Policy and Security Requirements for Registered Electronic Mail Service Providers

Electronic Registered Delivery (ERDS) and Registered Electronic Mail (REM)

Denotes a path from general requirements, common to any ERDS, to requirements that are specific ONLY to REM services and REM services providers.

Policy and security requirements

Technical specifications

ERDS

EN 319 521
General policy & security requirements

EN 319 522
General ERDS evidences
    + ebMS/AS4 binding
    + SML/SMP binding for
        common services

REM

EN 319 531
REM specific policy & security requirements

EN 319 532
SMTP binding
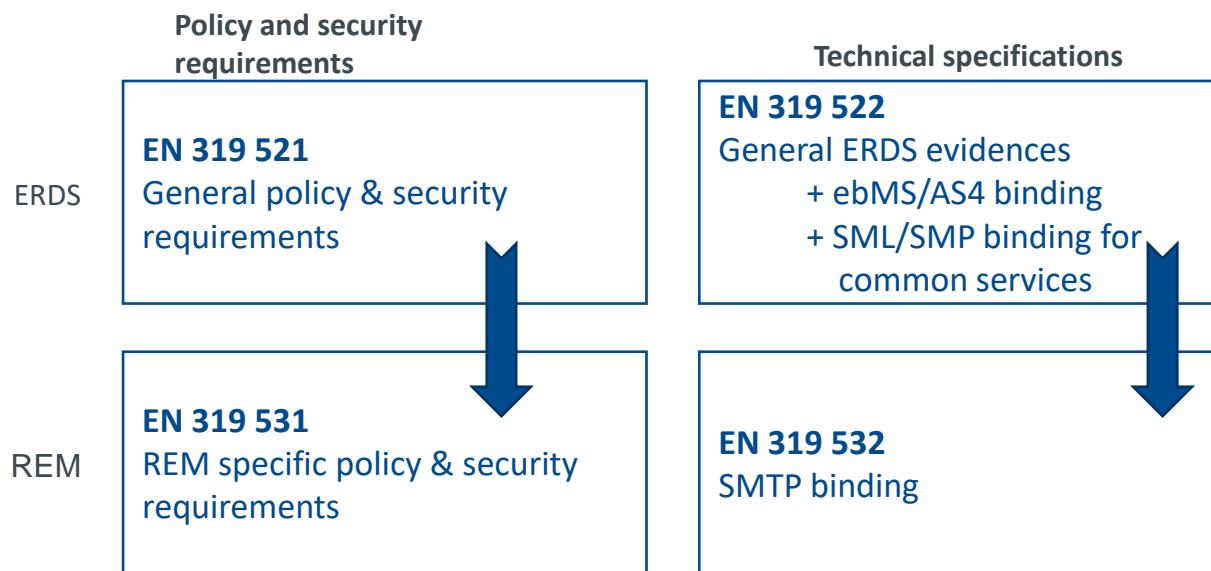
TS 119 524	Testing Conformance and Interoperability of Electronic Registered Delivery Services
TS 119 534	Testing Conformance and Interoperability of Registered Electronic Mail Services
TR 119 500	Business Driven Guidance for Trust Application Service Providers

Conformity Assessment

Basis for EN 319 403 TSP Audit Requirements

Primary reference:

- ⱱ ISO 17065 Conformity assessment -- Requirements for bodies certifying products, processes and services
  - ⱱ Establishing a set of third party requirements against which a high degree of confidence and trust can be established by impartial and competent demonstration of fulfilment of those requirements

Additional requirements incorporated from:

- ⱱ ISO 17021 Conformity assessment -- Requirements for bodies providing audit and certification of management systems
  - ⱱ First published in 2006, was created for assessing certification bodies to ensure their competence and conformance to all types of management systems
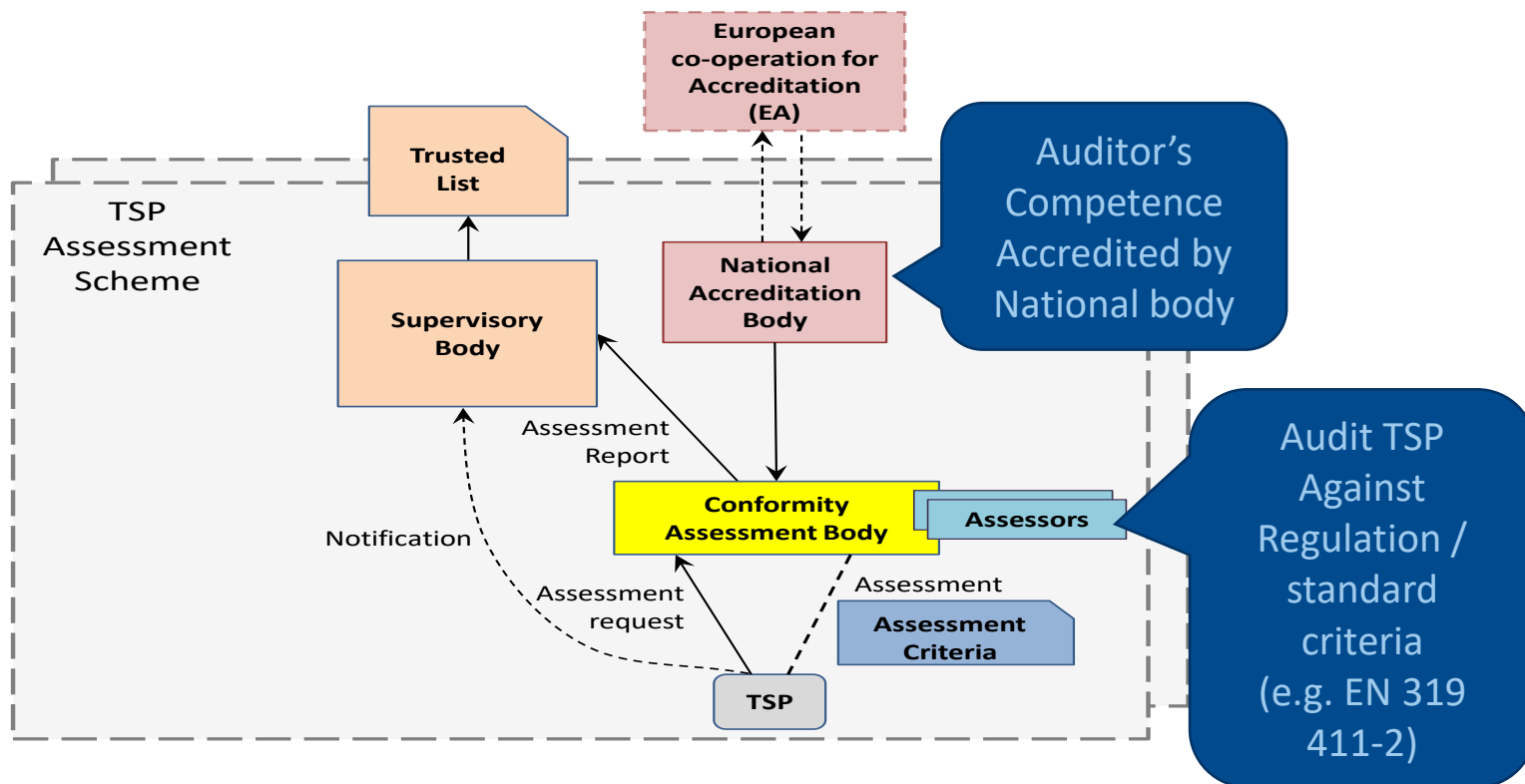
TS 119 403-2: Part 2: Additional requirements for Conformity Assessment Bodies auditing Trust Service Providers that issue Publicly-Trusted Certificates (e.g. as in CA/Browser Forum)

- Annual audit (versus bi-annually for eIDAS)
- Audit covers period of time since last audit
- Audit attestation requirements fitting web browser requirements

TS 119 403-3: Additional Requirements for CABs Assessing QTSPs against the eIDAS Regulation Requirements

- Auditor capabilities to carry out audits under eIDAS
- Required details included in conformity assessment report

ETSI TR 119 411-4: Checklist for TSPs issuing certificates with 500+ controls in total

Trusted Lists

Trusted Lists defined by eIDAS

eIDAS Section 3 Article 22

Each EU Member State has an obligation to establish, maintain and publish **trusted lists**, including information related to the **qualified trust service providers** for which they are responsible, together with information related to the qualified trust services provided by them. The lists are to be **published** in a secured manner, **electronically signed** or **sealed** in a form suitable for automated processing.

ec.europa.eu/digital-single-market/en/eu-trusted-lists-trust-service-providers

Please see: ETSI TS 119 612: Trusted lists
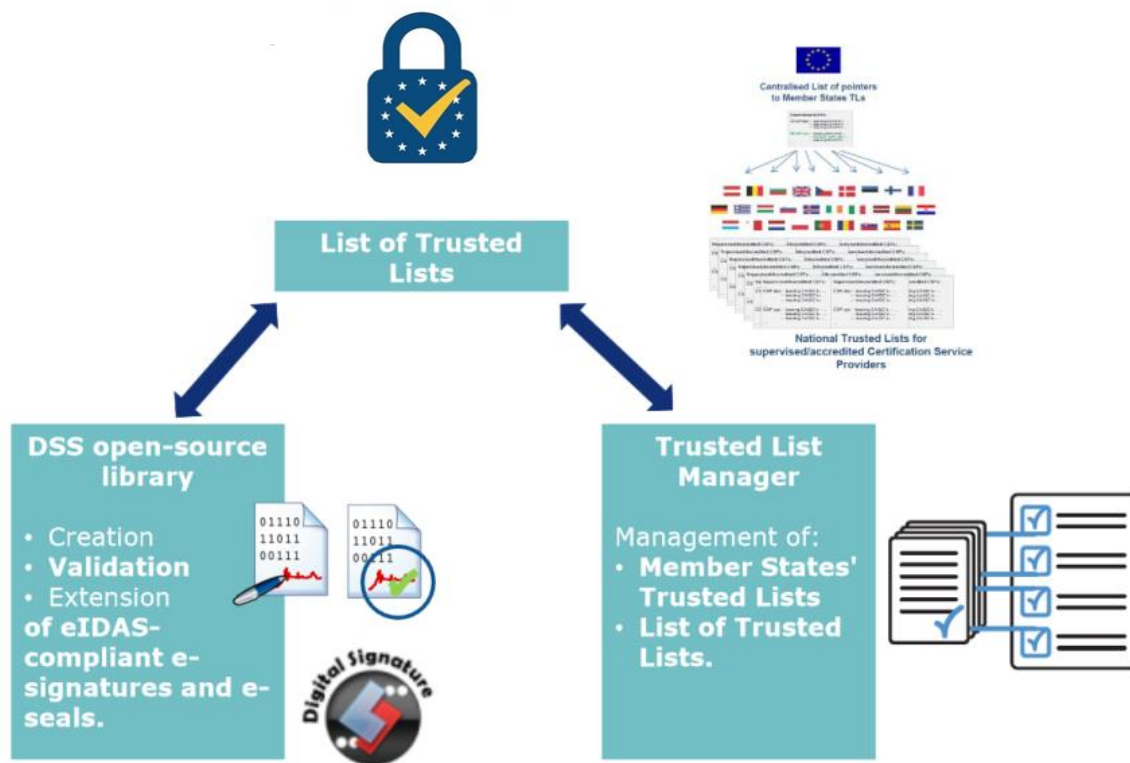
Browsing the EU Trusted Lists

Conclusions

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 EU National Standards Organisations

Updates on standardisation:
https://list.etsi.org/scripts/wa.exe?SUBED1=e-signatures_news&A=1