The Standards People

European standardisation framework for trust services

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

For: **Tokyo Workshop**

23.05.2019

Agenda

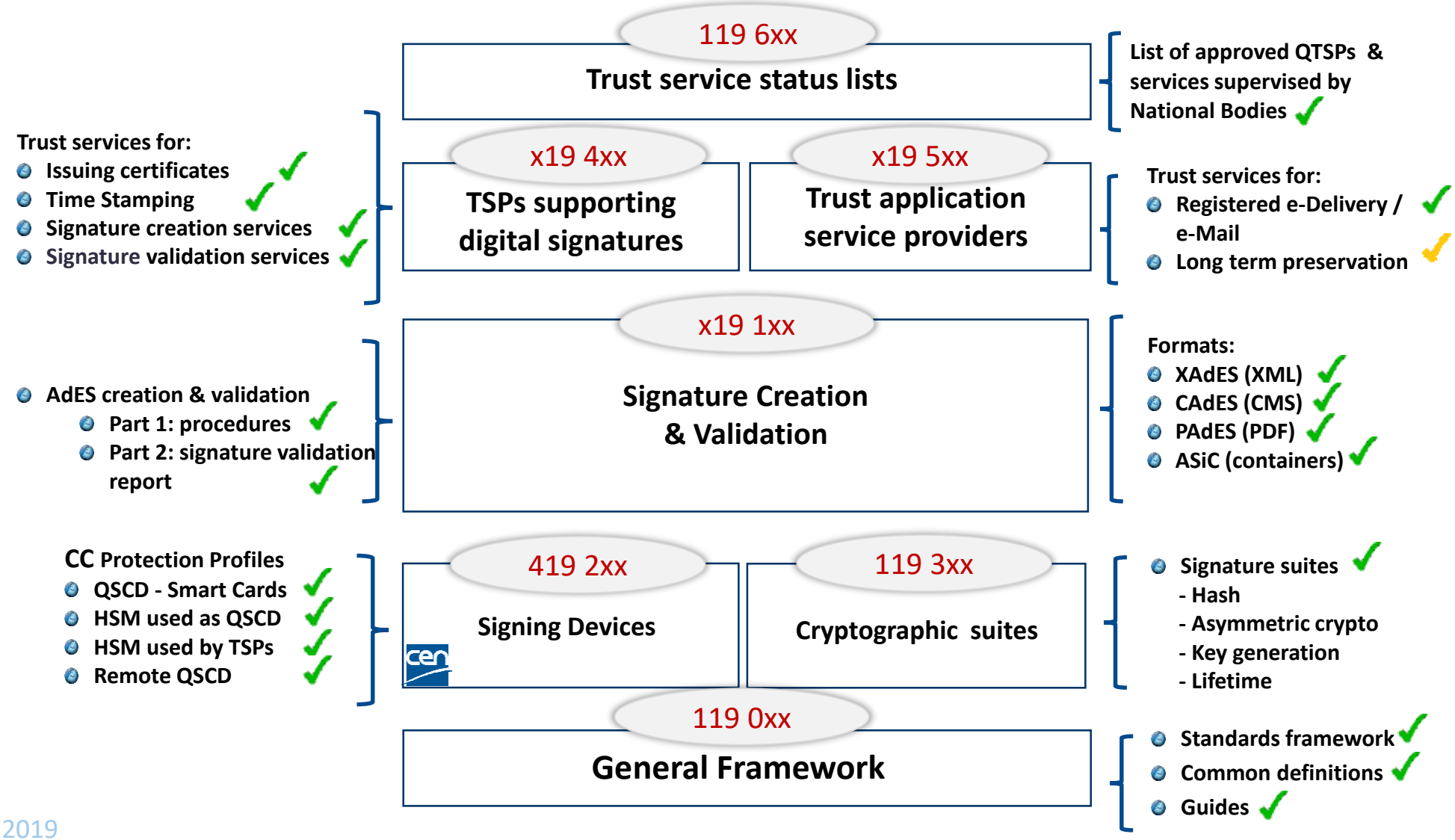
- eIDAS Standards Roadmap
- Trust Service Standards
- Electronic signatures and seals
- Trusted Lists
- Conformity Assessment
- Conclusions

eIDAS Standards Roadmap

eIDAS Strategic Goals

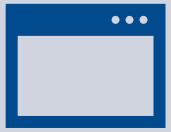
(Slide from Andrea Servida; EU Commission; Head of DG CONNECT H4 - “eGovernment and Trust”)

eIDAS Standards Framework: Published Standards



Trust services issuing certificates

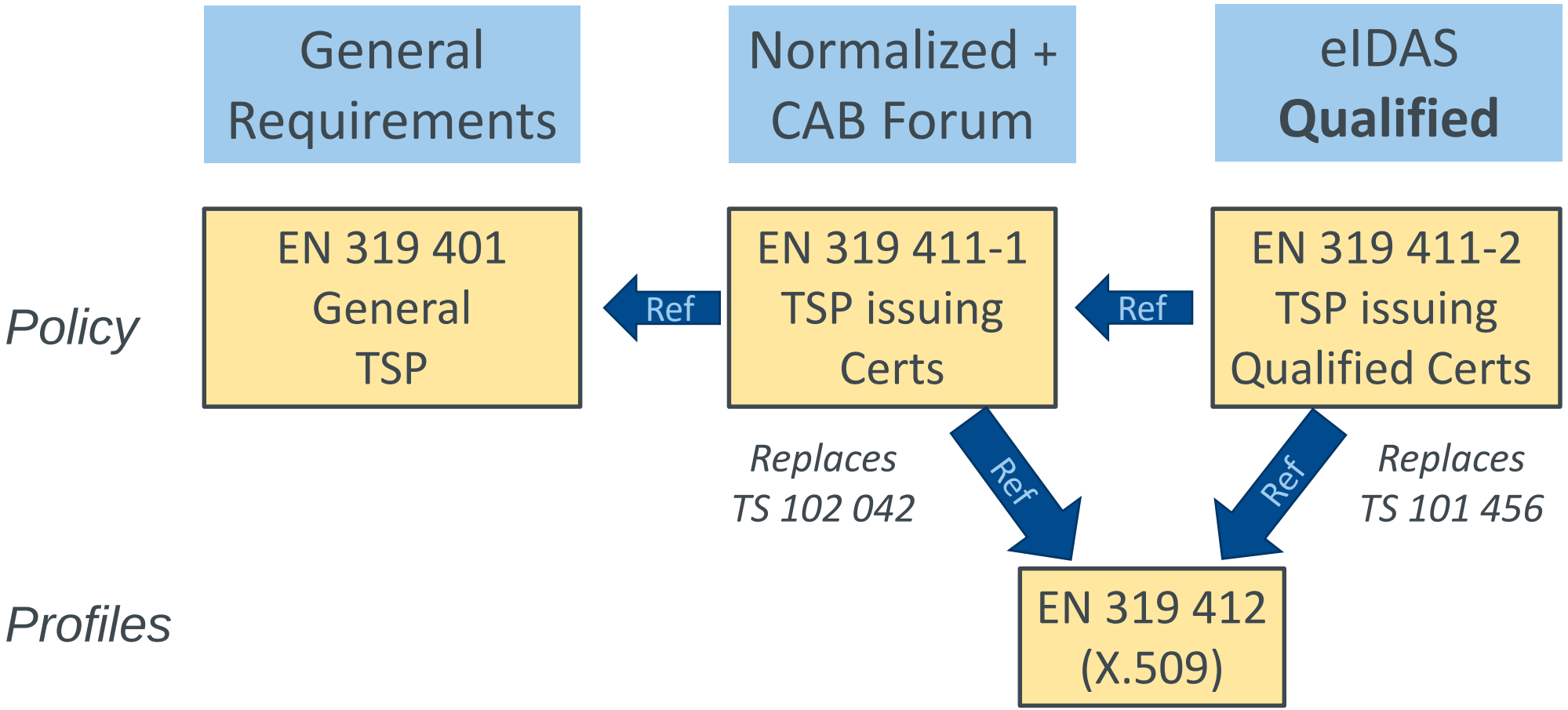
Trust service issuing certificates

e-Signatures	For use by natural persons 
e-Seals	For use by legal persons 
Website authentication	For websites 

Trust service issuing certificates

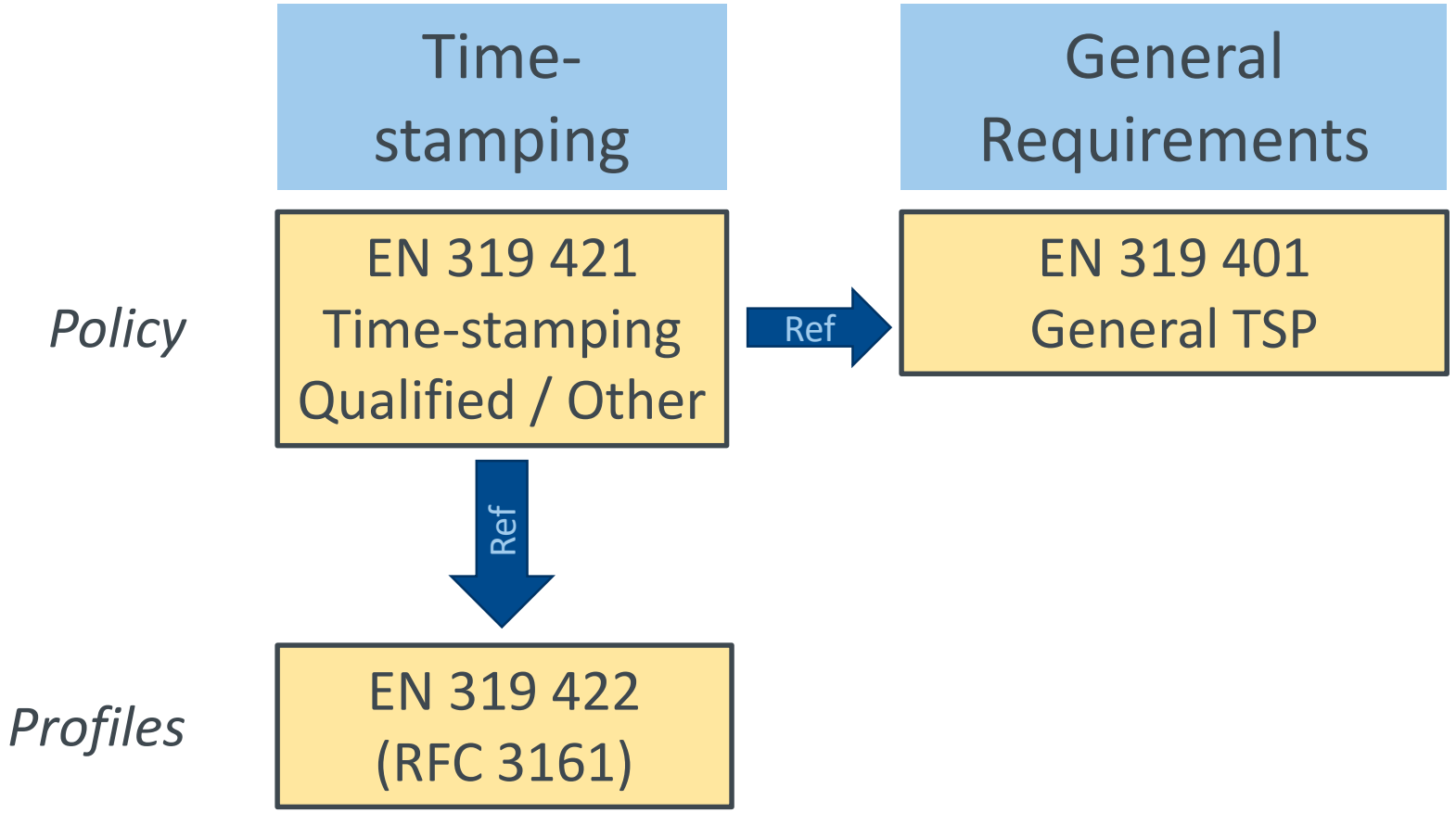
- ETSI EN 319 401 General policy requirements for trust service providers (referenced by the following)
- ETSI EN 319 411-1 Part 1: General Policy and security requirements for TSPs issuing public key certificates
- ETSI EN 319 411-2 Part 2: EU qualified certificates

Trust services issuing certificates: ETSI standards overview



Timestamping

ETSI Time-Stamping Standards



ETSI Time-Stamping Standards, expanded

ETSI EN 319 421: Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

- Introduction to time-stamp policies and general requirements
- Policies and practices
- TSA management and operation
- Additional requirements for qualified electronic time-stamps as per eIDAS Regulation

ETSI EN 319 422: Time-stamping protocol and time-stamp token profiles

- Requirements for a time-stamping client
- Requirements for a time-stamping server
- TSU certificate profile
- Profiles for the transport protocols to be supported
- Object identifiers of the cryptographic algorithms
- Additional requirements for qualified electronic time-stamps as per eIDAS Regulation

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

Signatures: Creation & Validation - General standards

- **ETSI TR 119 100**

Guidance on the use of standards for signatures creation and validation

- **ETSI TS 119 101**

Policy and security requirements for applications for signature creation and signature validation

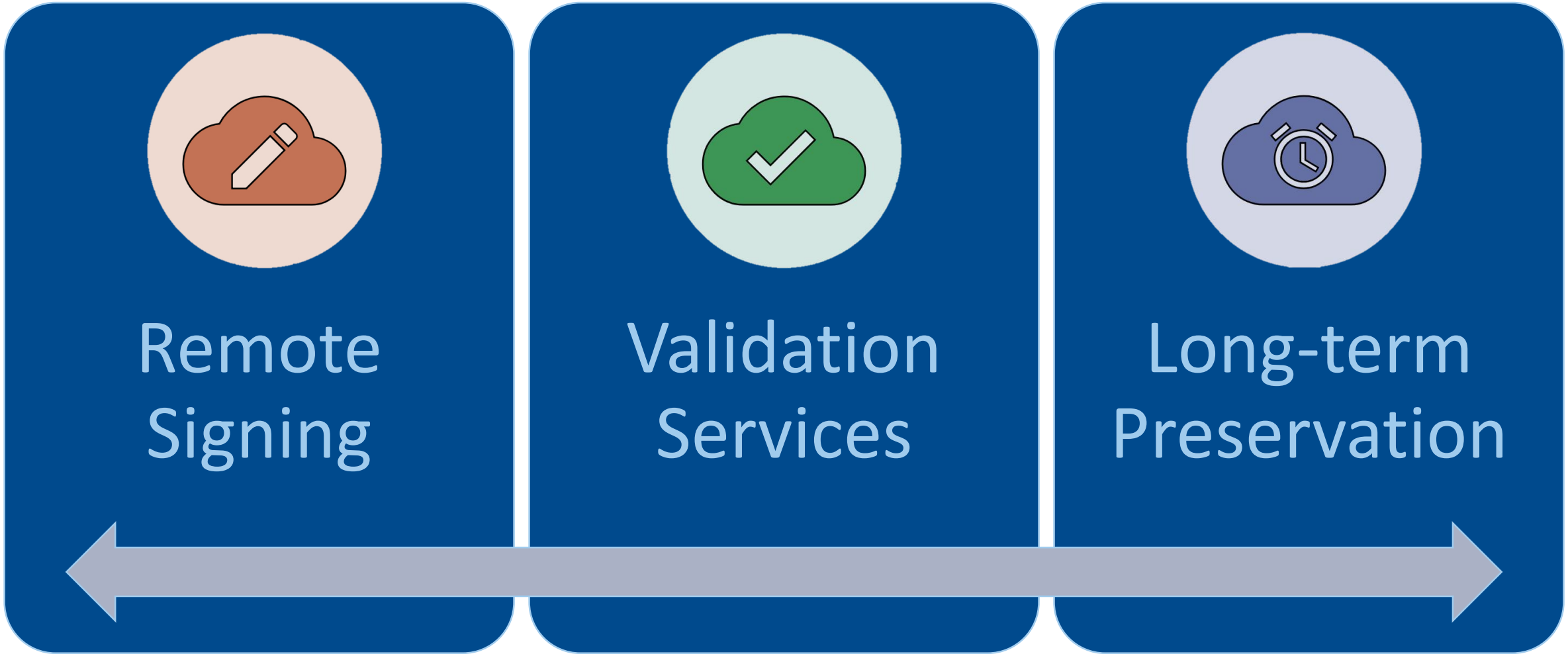
- **ETSI TS 119 102**

Procedures for Creation and Validation of AdES

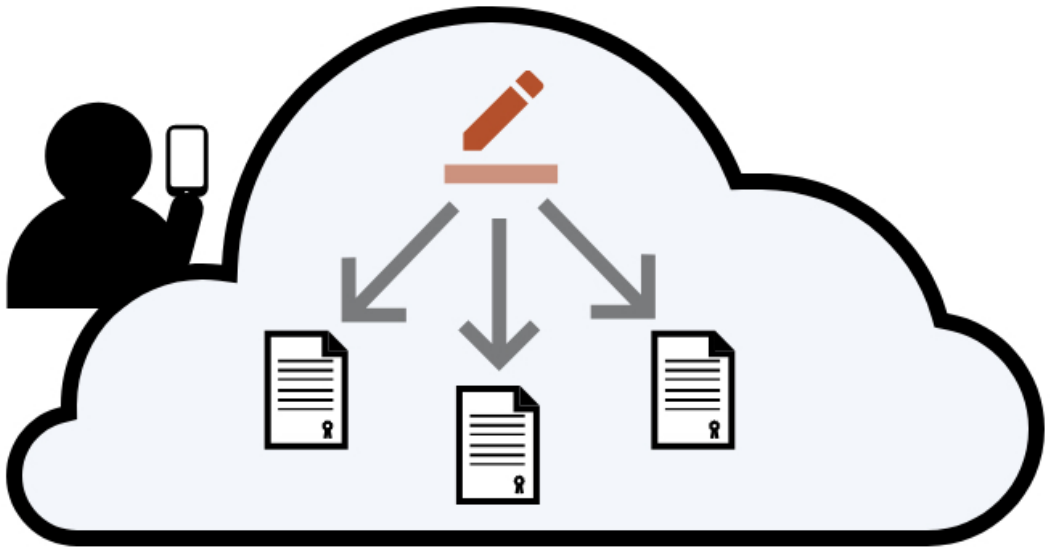
  - Part 1: Signature *c*reation and validation
  - Part 2: Signature Validation Report

Signature Enhanced Services

Signature Enhanced Trust Services



Signatures: Remote Signing



- **ETSI TS 119 431-1**

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

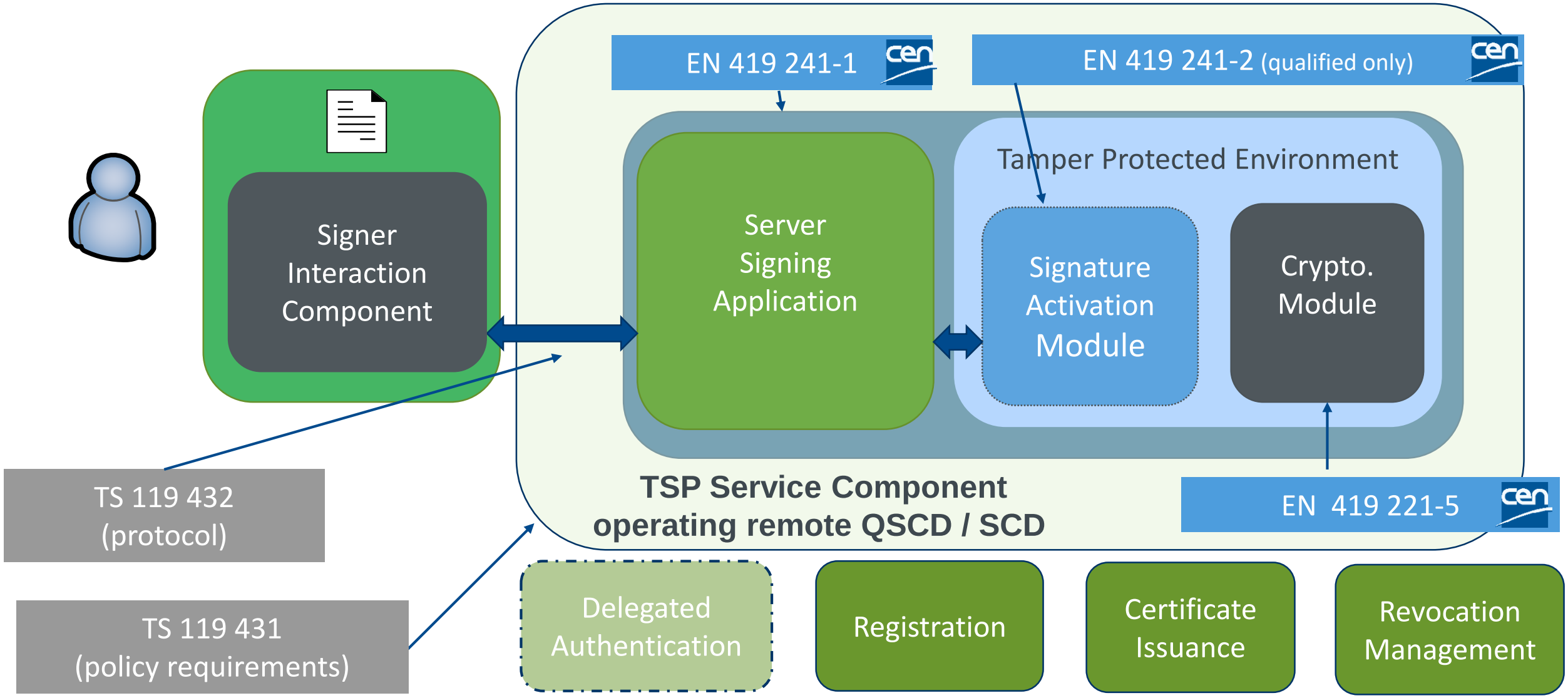
- **ETSI TS 119 431-2**

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

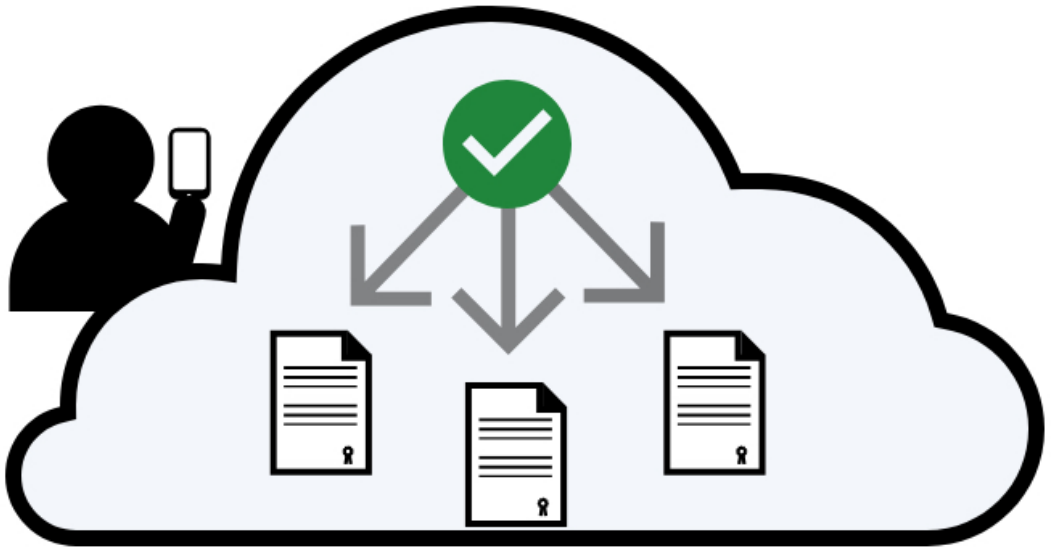
- **ETSI TS 119 432**

Protocols for
Remote Digital Signature Creation

Trust services issuing certificates: Scope of Remote Signing Standards



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

ETSI TS 119 511

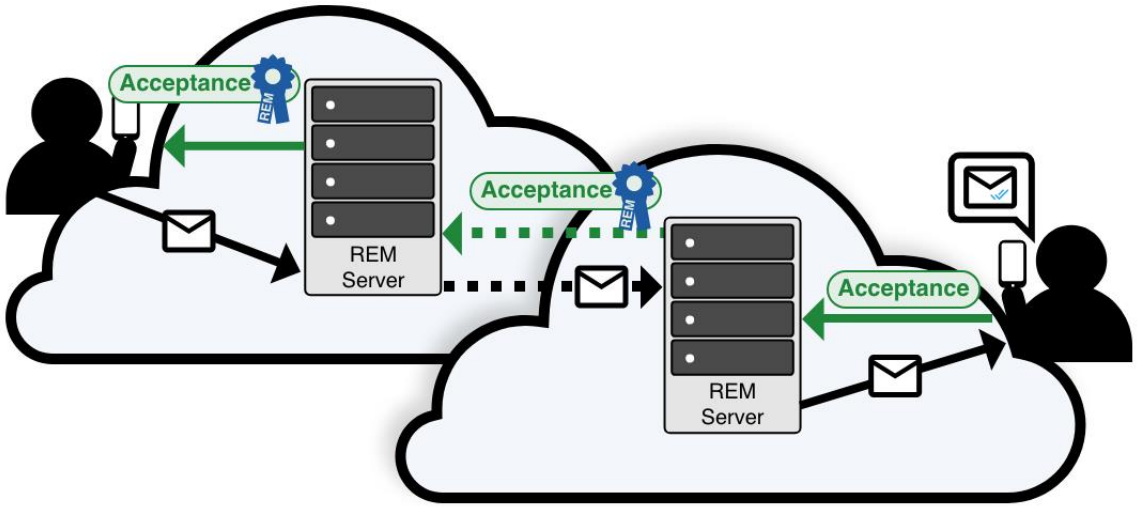
Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques *(draft)*

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**

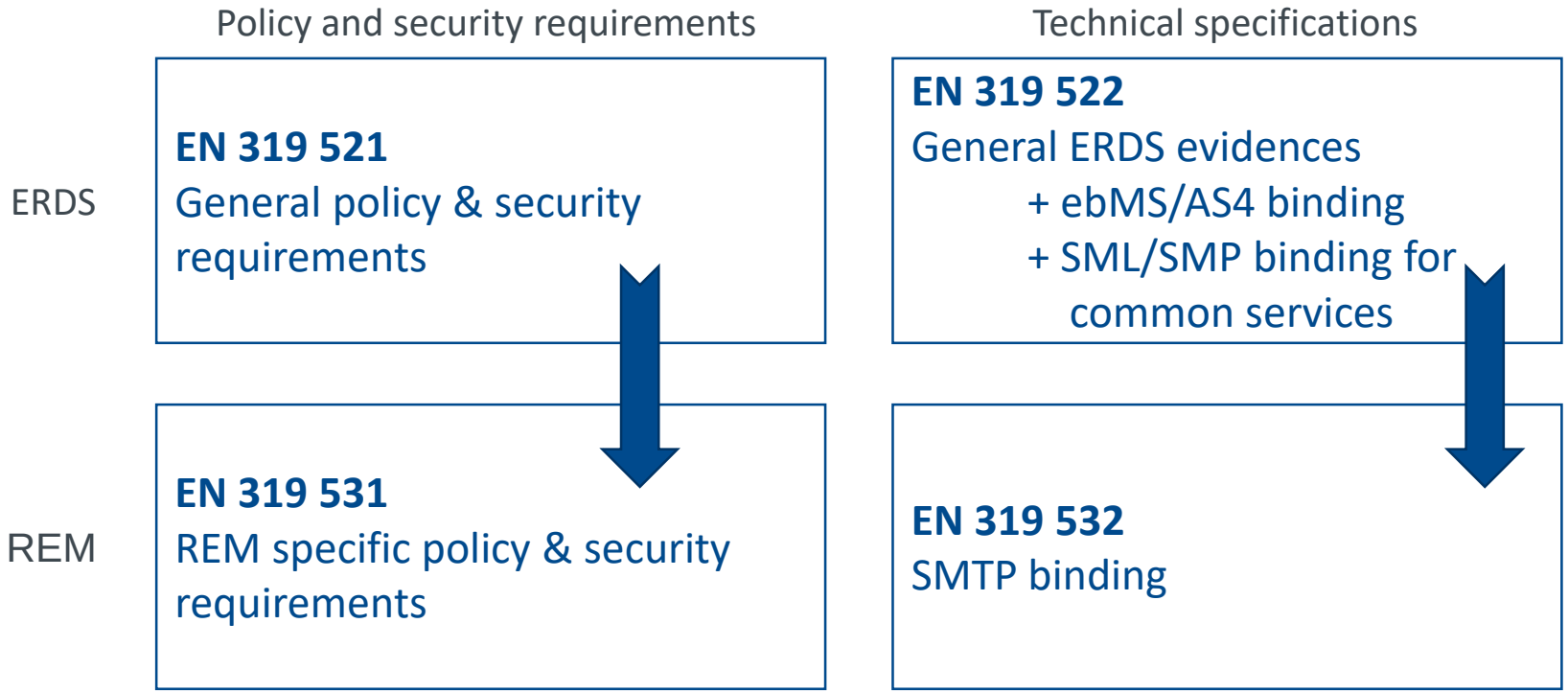
  Policy and Security Requirements for Electronic Registered Delivery Service Providers

- **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.



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

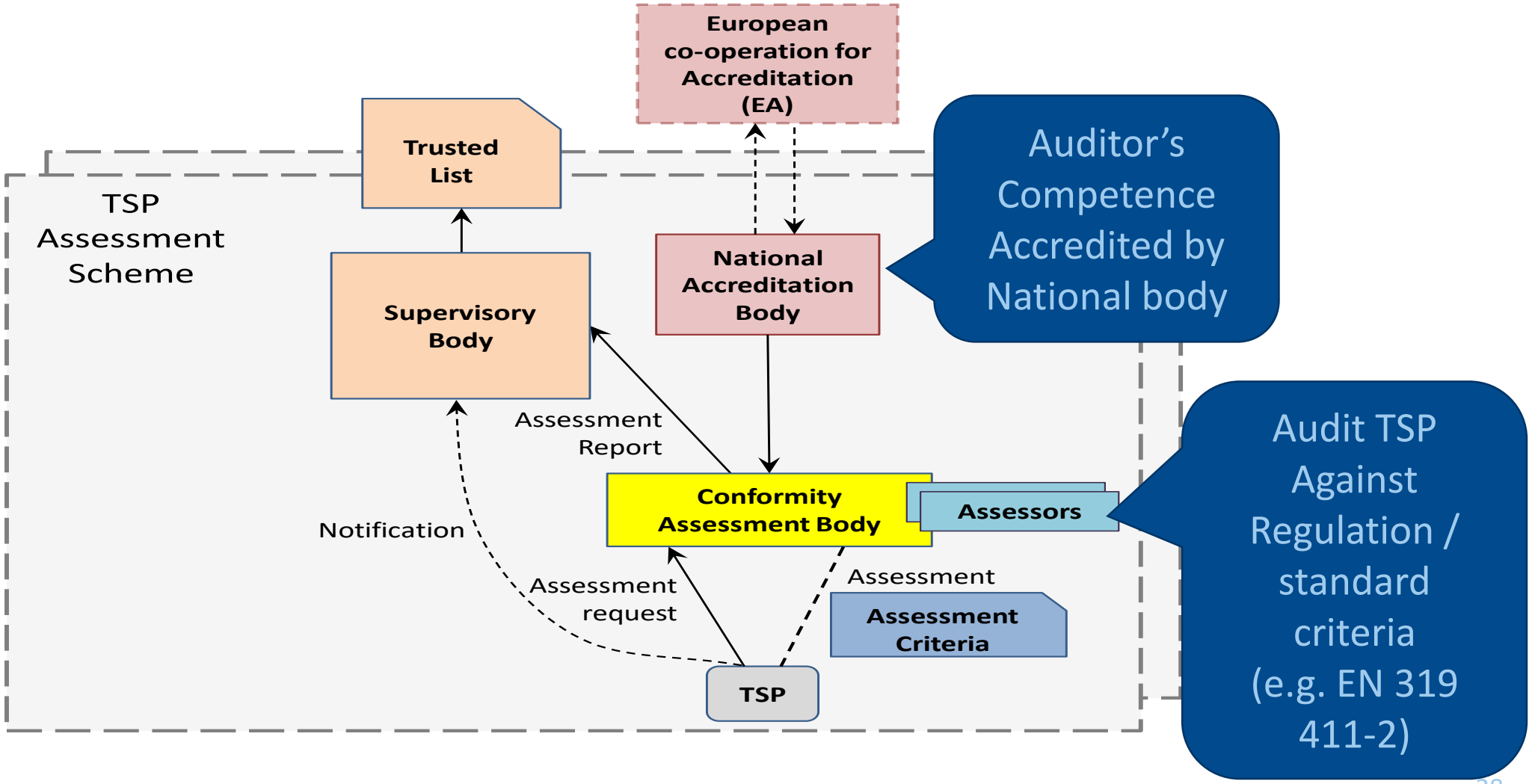
Primary reference:

- ISO 17065 Conformity assessment -- Requirements for bodies certifying products, processes and services
  - 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:

- ISO 17021 Conformity assessment -- Requirements for bodies providing audit and certification of management systems
  - First published in 2006, was created for assessing certification bodies to ensure their competence and conformance to all types of management systems

ETSI EN 319 403: TSP Conformity Assessment Model



New Supplements to EN 319 403 on specific TSP Audit Requirements

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

	Document reference	Technical requirement reference	Severity	CABF Requirement	NCP	NCP+	LCP	OVCP	EVCP	QCP-n	QCP-l	QCP-w (legal person)	QCP-w (natural person)	QCP-n with device	QCP-l with device	QCP-n-qscd	QCP-l-qscd	TSP Overall	Registration services	Certificate generation services	Dissemination services	Revocation management services	Revocation status services	Subject device provisioning services	eIDAS Regulation (sub)article supported by the requirement-applicable to Qualified Certificate policies defined in EN 319 411-2	Guidance	Claimed compliant status	Assessed compliant status	Comments	Actions required
2	[ETSI 319 411-2]	OVR-5.1-01	shall							y	y	y	y	y	y	y	y	y												
3	[ETSI 319 411-1]	OVR-5.1-01	shall					y		y								y												
4	[ETSI 319 411-1]	OVR-5.1-02	shall		y	y	y	y										y												
5	[ETSI 319 411-1]	OVR-5.1-03	should		y	y	y	y	y	y	y	y	y	y	y	y	y	y												
6	[ETSI 319 411-2]	OVR-5.1-02	shall							ch	ch			ch	ch			y												
7	[ETSI 319 411-2]	OVR-5.1-03	shall									ch	ch					y												
8	[ETSI 319 411-2]	OVR-5.1-04	shall													y		y												
9	[ETSI 319 411-2]	OVR-5.1-05	shall														y	y												
10	[ETSI 319 411-2]	OVR-5.2-01	shall							y	y	y	y	y	y	y	y	y												
11	[ETSI 319 411-1]	OVR-5.2-01	shall		y	y	y	y	y	y	y	y	y	y	y	y	y	y												
12	[ETSI 319 401]	REQ-6.1-01	shall		y	y	y	y	y	y	y	y	y	y	y	y	y	y												
13	[ETSI 319 401]	REQ-6.1-02	shall		y	y	y	y	y	y	y	y	y	y	y	y	y	y												
14	[ETSI 319 401]	REQ-6.1-03	shall		y	y	y	y	y	y	y	y	y	y	y	y	y	y												
15	[ETSI 319 401]	REQ-6.1-04	shall		y	y	y	y	y	y	y	y	y	y	y	y	y	y												
16	[ETSI 319 401]	REQ-6.1-05	shall		y	y	y	y	y	y	y	y	y	y	y	y	y	y												
17	[ETSI 319 401]	REQ-6.1-06	shall		y	y	y	y	y	y	y	y	y	y	y	y	y	y												
18	[ETSI 319 401]	REQ-6.1-07	shall		y	y	y	y	y	y	y	y	y	y	y	y	y	y												
19	[ETSI 319 401]	REQ-6.1-08	shall		y	y	y	y	y	y	y	y	y	y	y	y	y	y												
20	[ETSI 319 401]	REQ-6.1-09	shall		y	y	y	y	y	y	y	y	y	y	y	y	y	y												
21	[ETSI 319 401]	REQ-6.1-10	shall		y	y	y	y	y	y	y	y	y	y	y	y	y	y												
22	[ETSI 319 401]	REQ-6.1-11	shall		y	y	y	y	y	y	y	y	y	y	y	y	y	y												
23	[ETSI 319 411-1]	OVR-5.2-02	should		y	y	y	y	y	y	y	y	y	y	y	y	y	y								See IETF RFC 3647					
	[ETSI 319 411-1]		shall		y	y	y	y	y	y	y	y	y	y	y	y	y	y												

Trusted Lists

Trusted Lists defined by eIDAS

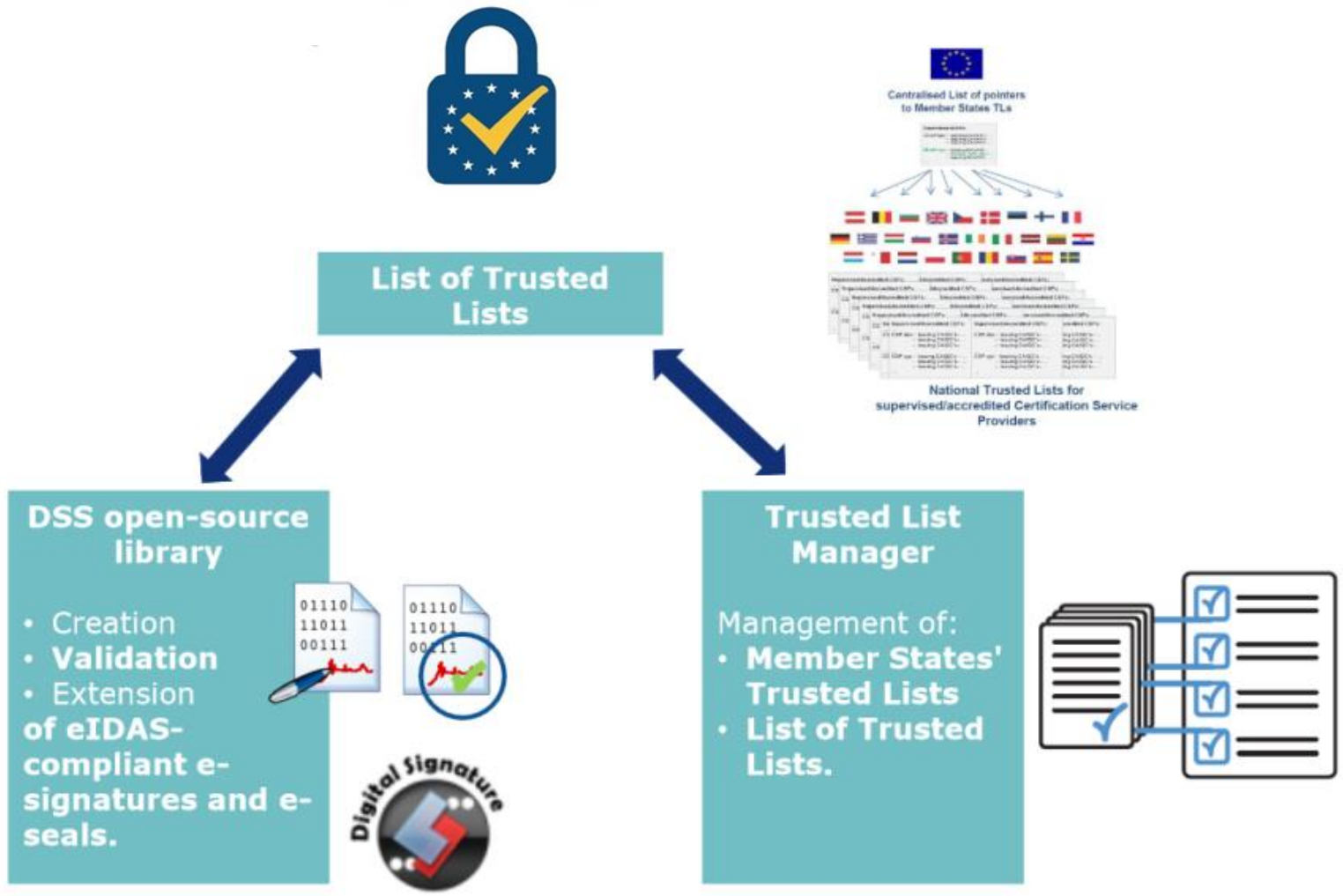
eIDAS Section 3 Article 22

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.

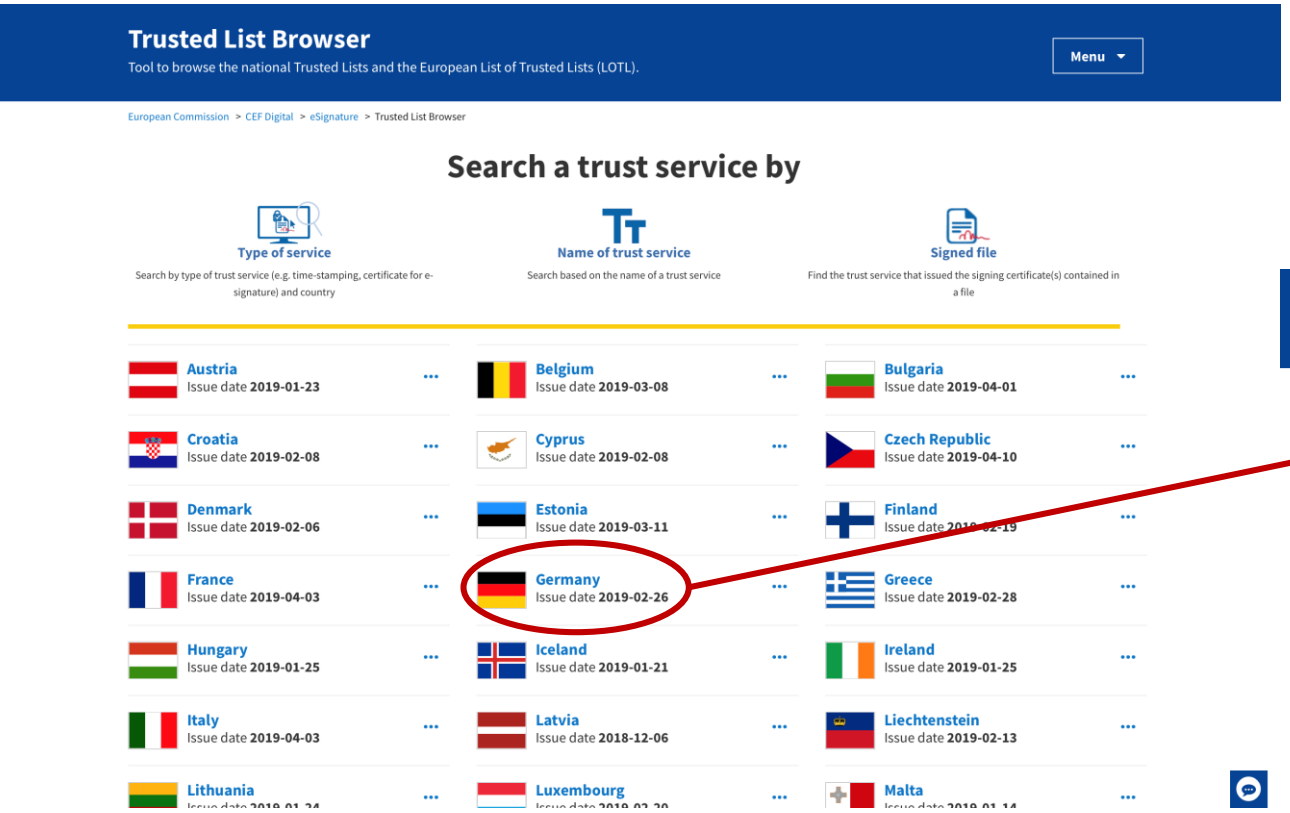
ec.europa.eu/digital-single-market/en/eu-trusted-lists-trust-service-providers

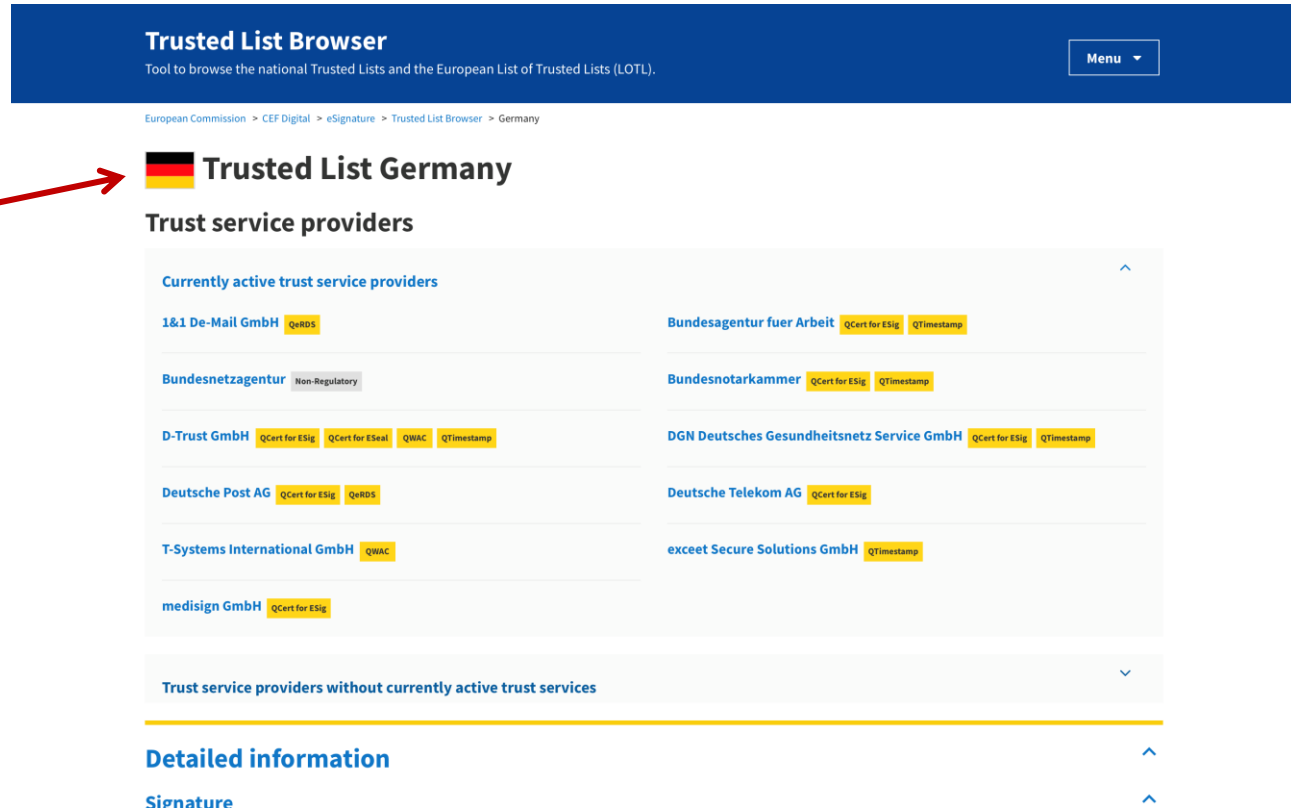
Please see: **ETSI TS 119 612:** Trusted lists

The EU “List of the 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