European standardisation framework for trust services

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

For: **CA/B-Forum Thessaloniki**

12.06.2019

TC CYBER and CA/B Forum collaboration

TC CYBER has a broad array of products and work items for global use, including quantum safe cryptography

- ✓ Its dashboard portal can be found here
- ✓ Freely-available Technical Specifications and Reports that can be found here
- ✓ Work items in progress can be found here and here (quantum)

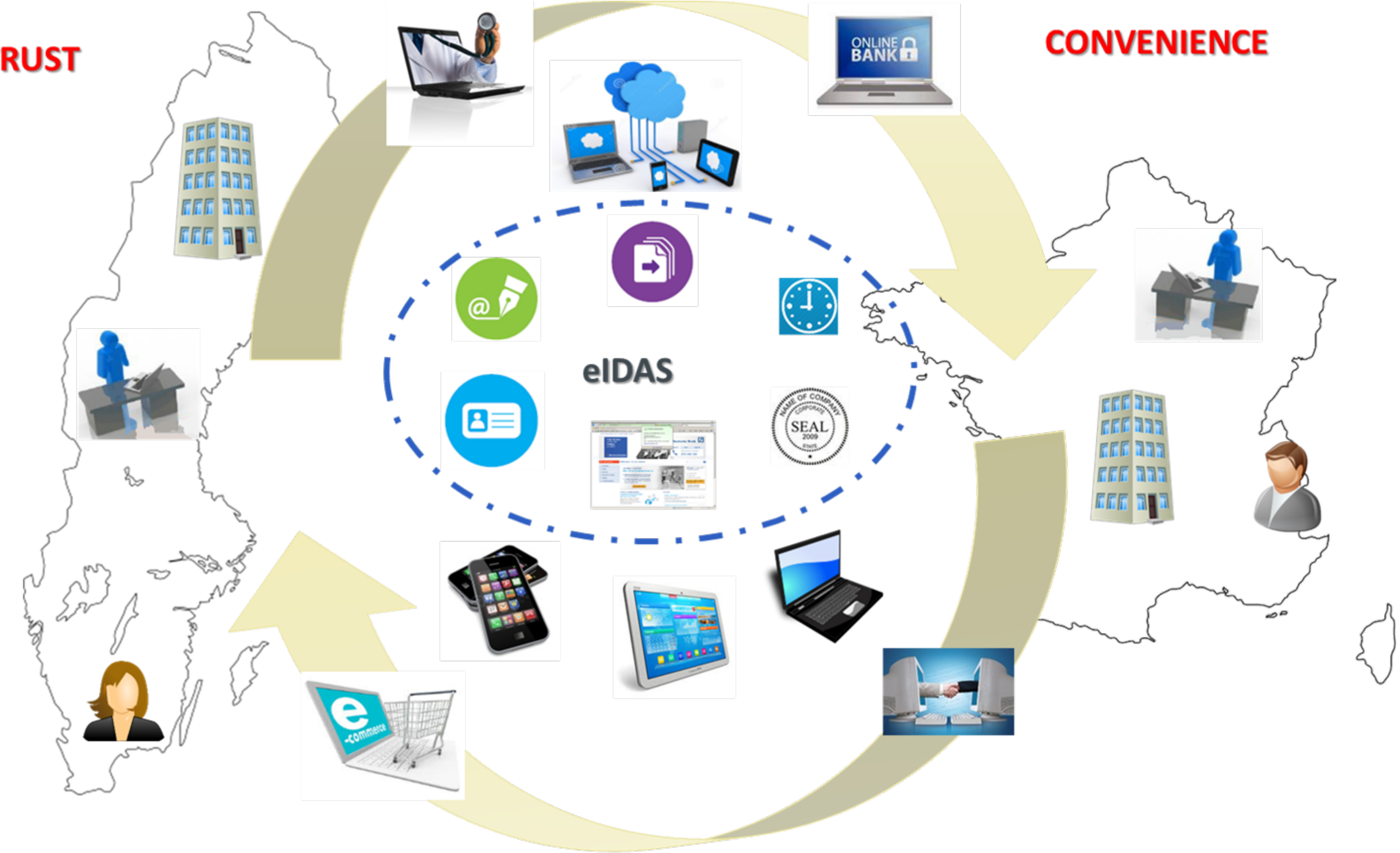
CA/B's work is closely followed and specific future collaboration is envisioned for

- ✓ Critical Security Control technical specifications referring to and including Code Signing Certificates to enhance cybersecurity trust generally
- ✓ Making use of the Subject Information and Certificate Policy Identification fields in conjunction with Middlebox Security Protocol specifications
- ✓ Contact is Tony Rutkowski,tony.Rutkowski@cisecurity.org

eIDAS Standards Roadmap

eIDAS Strategic Goals

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



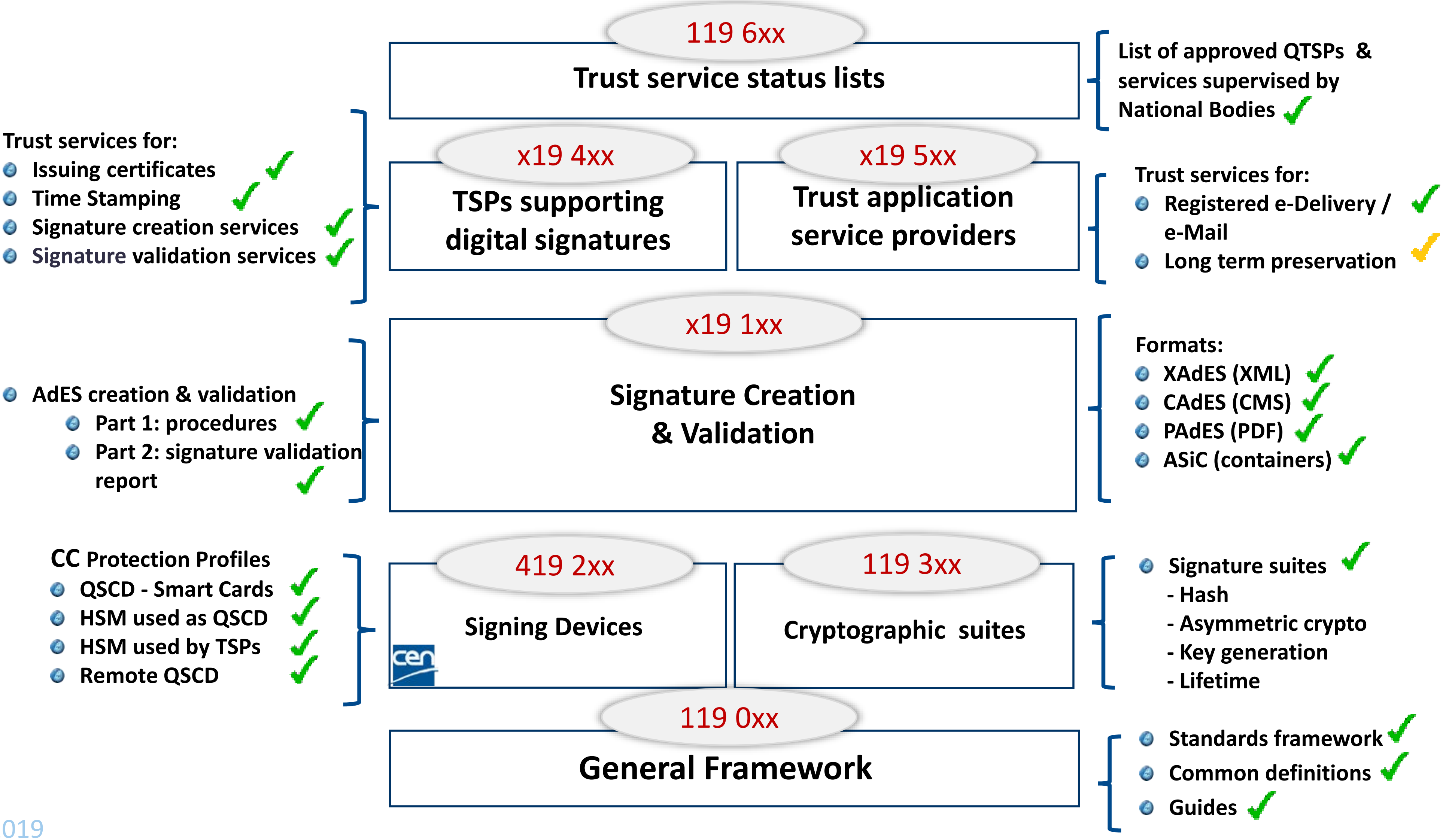
TRUST

CONVENIENCE

CROSS-BORDER

SEAMLESS

eIDAS Standards Framework: Published Standards



119 6xx
Trust service status lists

List of approved QTSPs & services supervised by National Bodies ✓

x19 4xx
TSPs supporting digital signatures

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

x19 5xx
Trust application service providers

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

x19 1xx
Signature Creation & Validation

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

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

419 2xx
Signing Devices

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

119 3xx
Cryptographic suites

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

119 0xx
General Framework

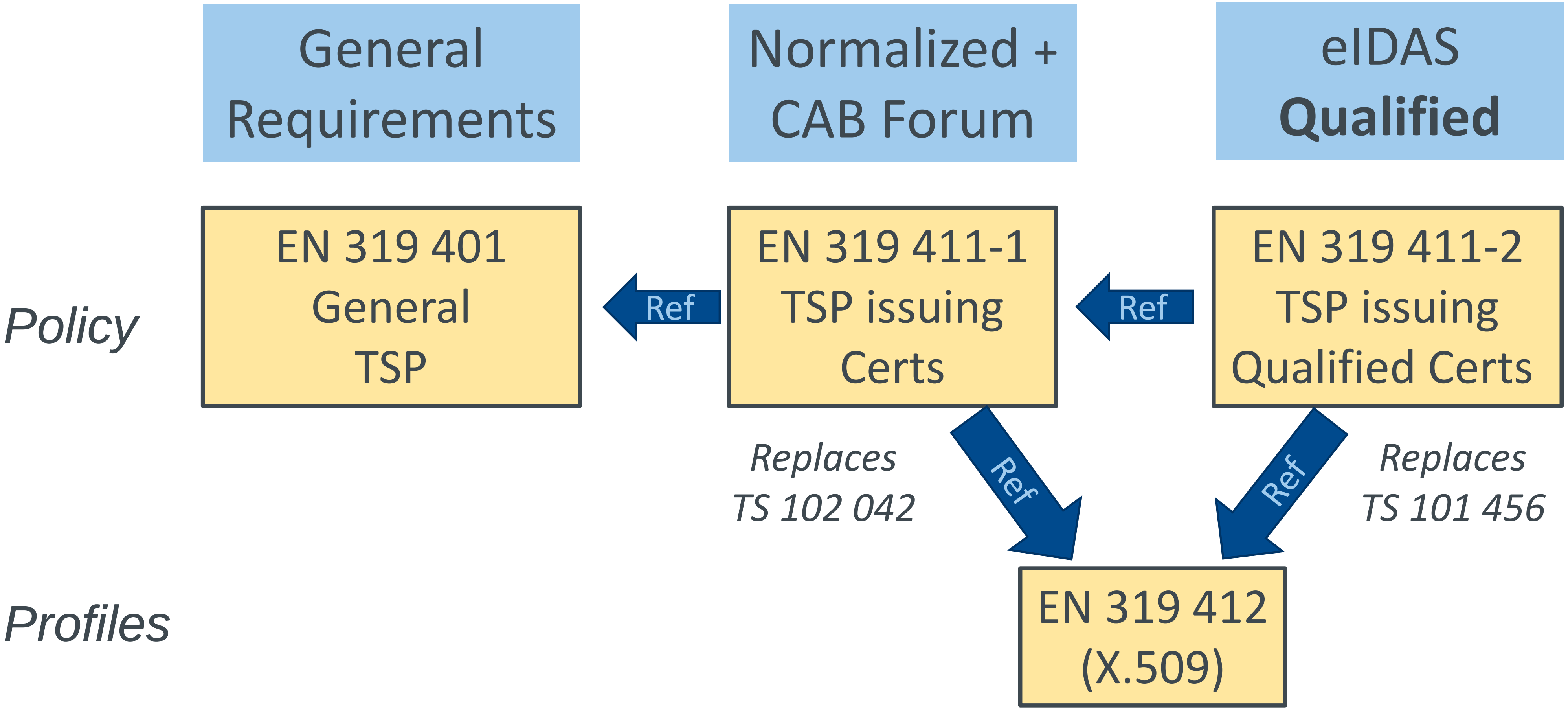
- Standards framework ✓
- Common definitions ✓
- Guides ✓

Trust services issuing certificates

Trust service issuing certificates

e-Signatures	For use by natural persons
e-Seals	For use by legal 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

Ref

Ref

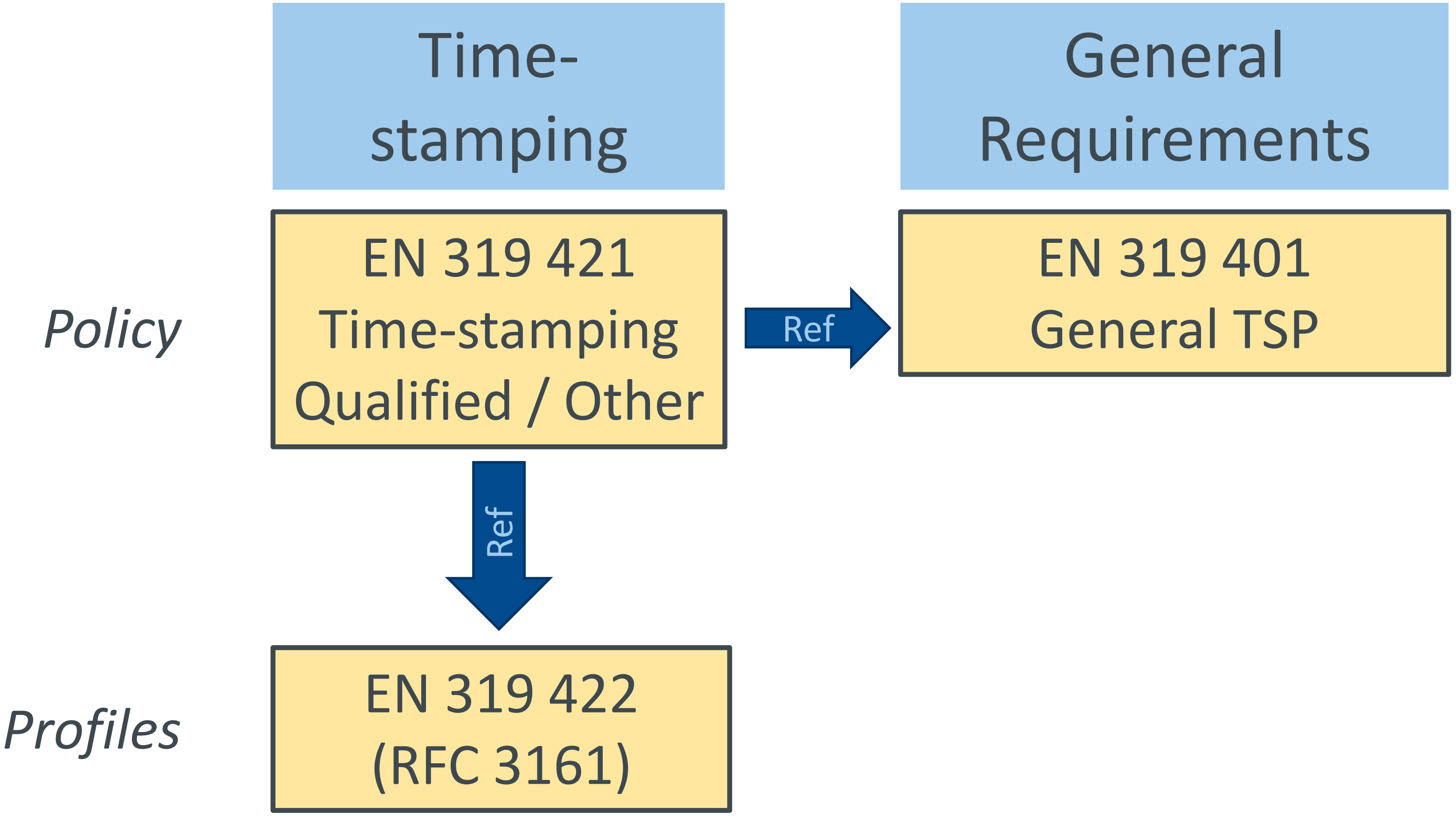
Replaces TS 101 456

Profiles

EN 319 412 (X.509)

Timestamping

ETSI Time-Stamping Standards



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

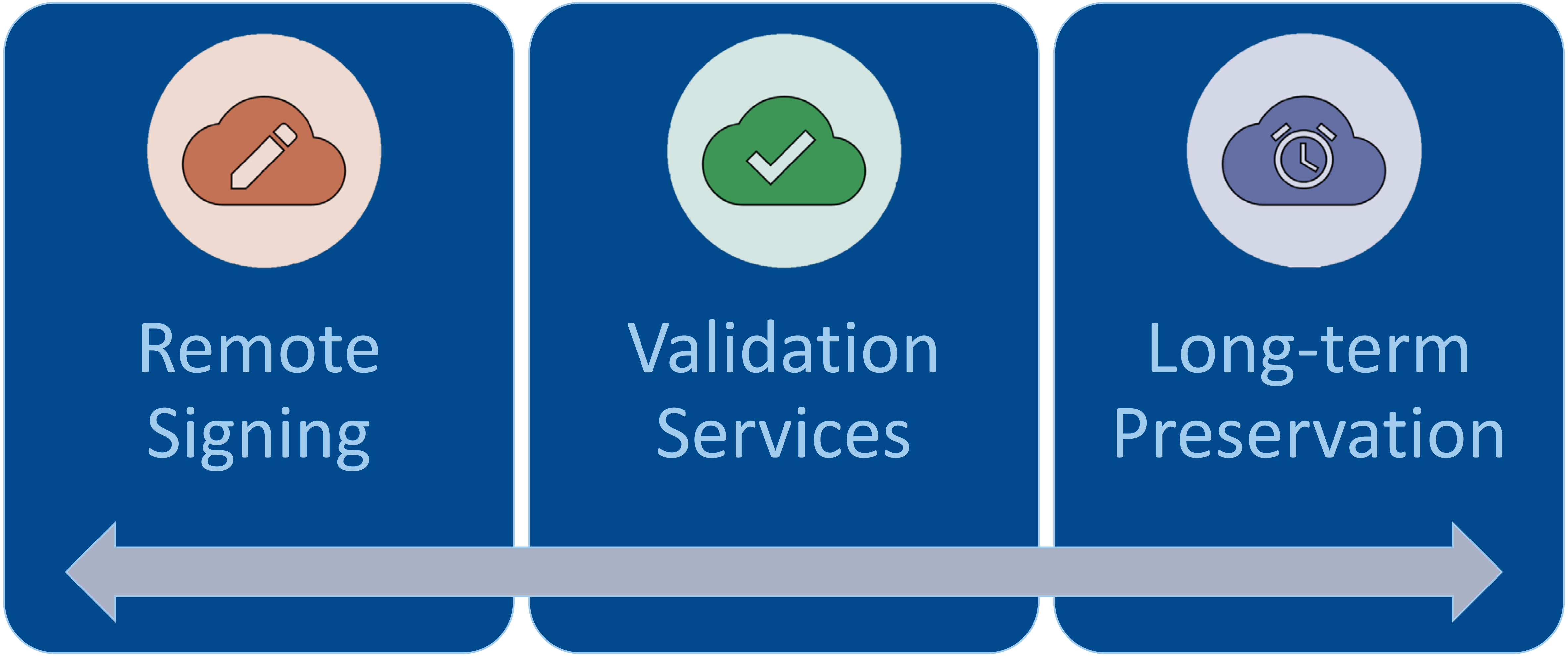
(d) linked […] in such a way that any subsequent change in the data is detectable.

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

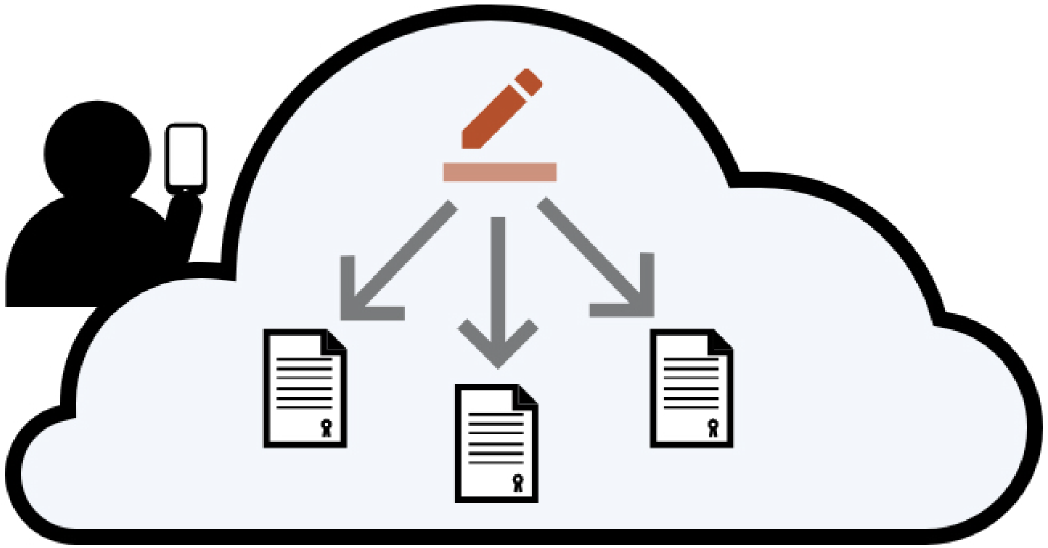


Remote Signing

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

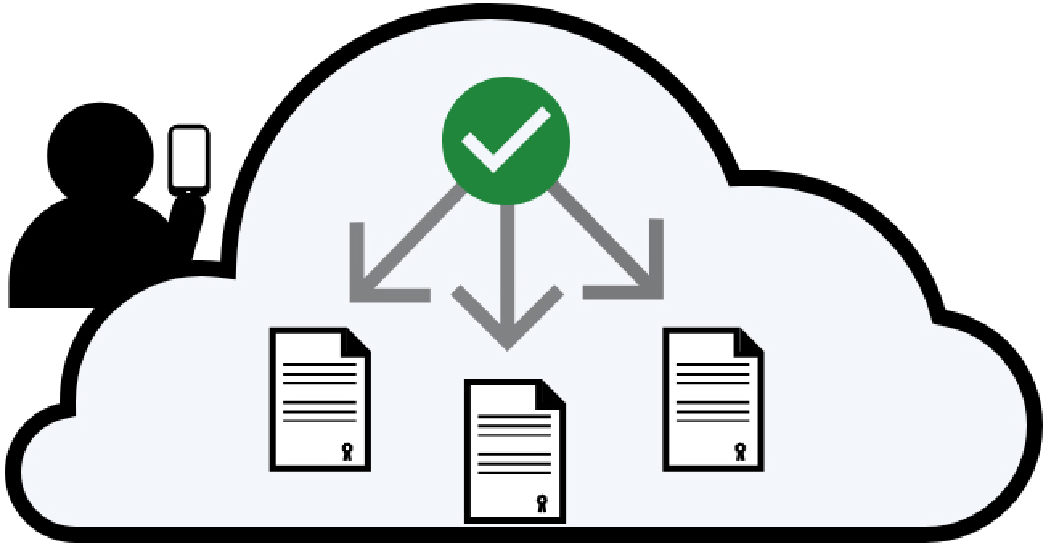
- **ETSI TS 119 431-2**

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

- **ETSI TS 119 432**

  Protocols for
  Remote Digital Signature Creation

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)*

Conformity Assessment

Basis for EN 319 403 TSP Audit Requirements

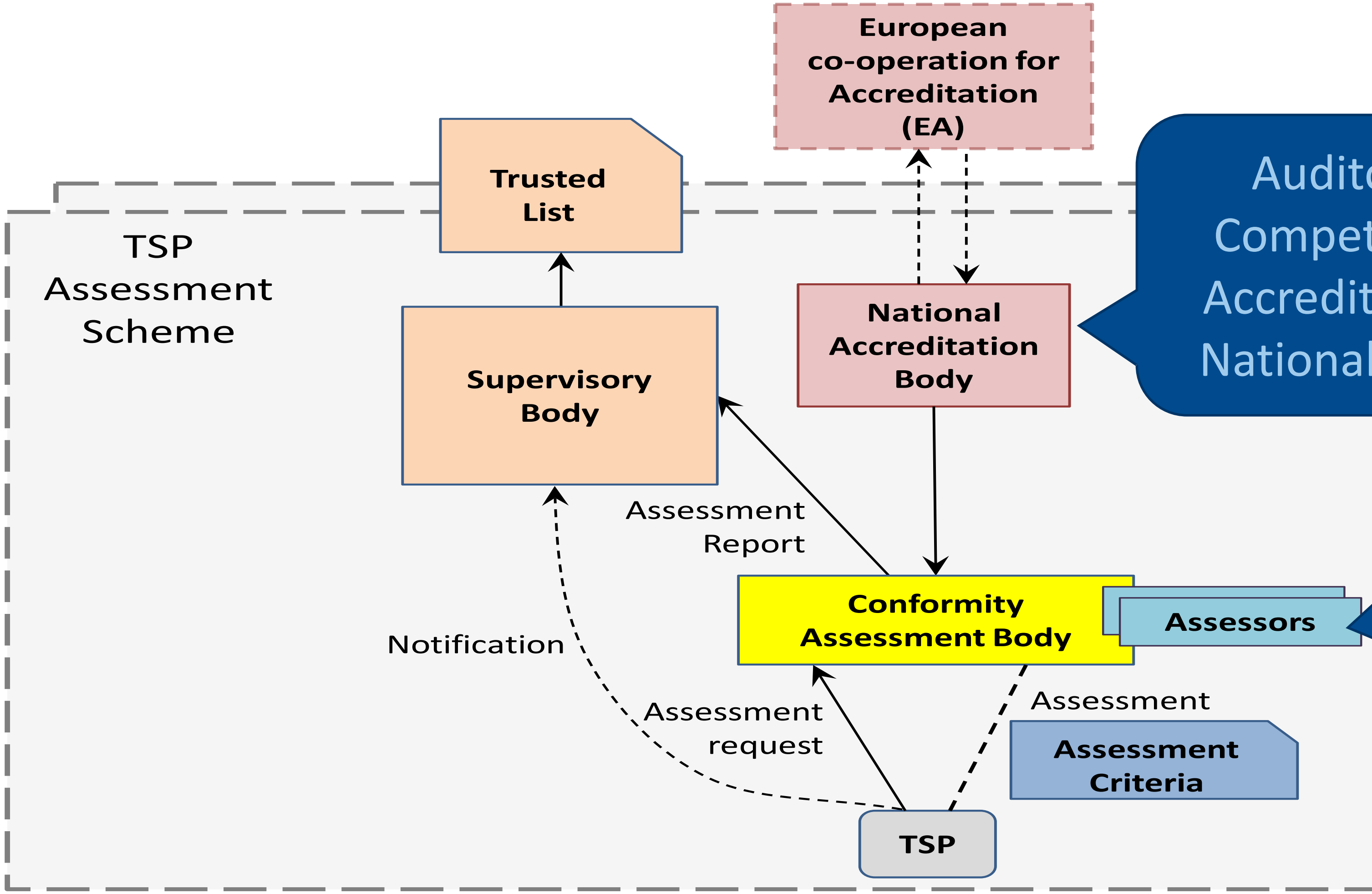
Primary reference:

- 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



Auditor’s Competence Accredited by National body

Audit TSP Against Regulation / standard criteria (e.g. EN 319 411-2)

New Supplements to EN 319 403 on specific TSP Audit Requirements

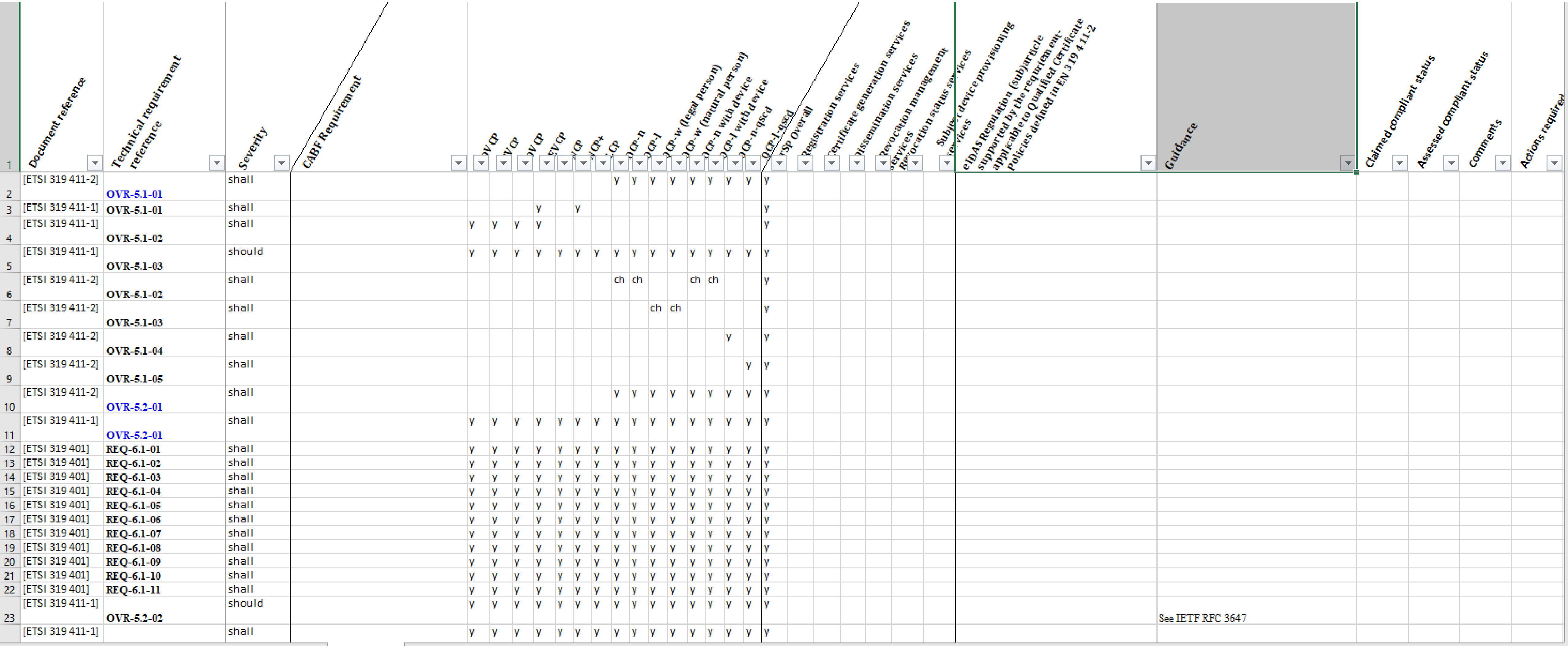
TS 119 403-2: Part 2: Additional requirements for Conformity Assessment Bodies auditing Trust Service Providers that issue Publicly-Trusted Certificates (e.g. as in CA/Browser Forum)

- 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	ov CP	v CP	ov CP	ev CP	CP	CP+	CP	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 ent- applicable to Qualified Certificate Policies defined in EN 319 411-2	Guidance	Claimed compliant status	Assessed compliant status	Comments	Actions required
1																																
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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	y	y												

Trusted Lists

Trusted Lists defined by eIDAS

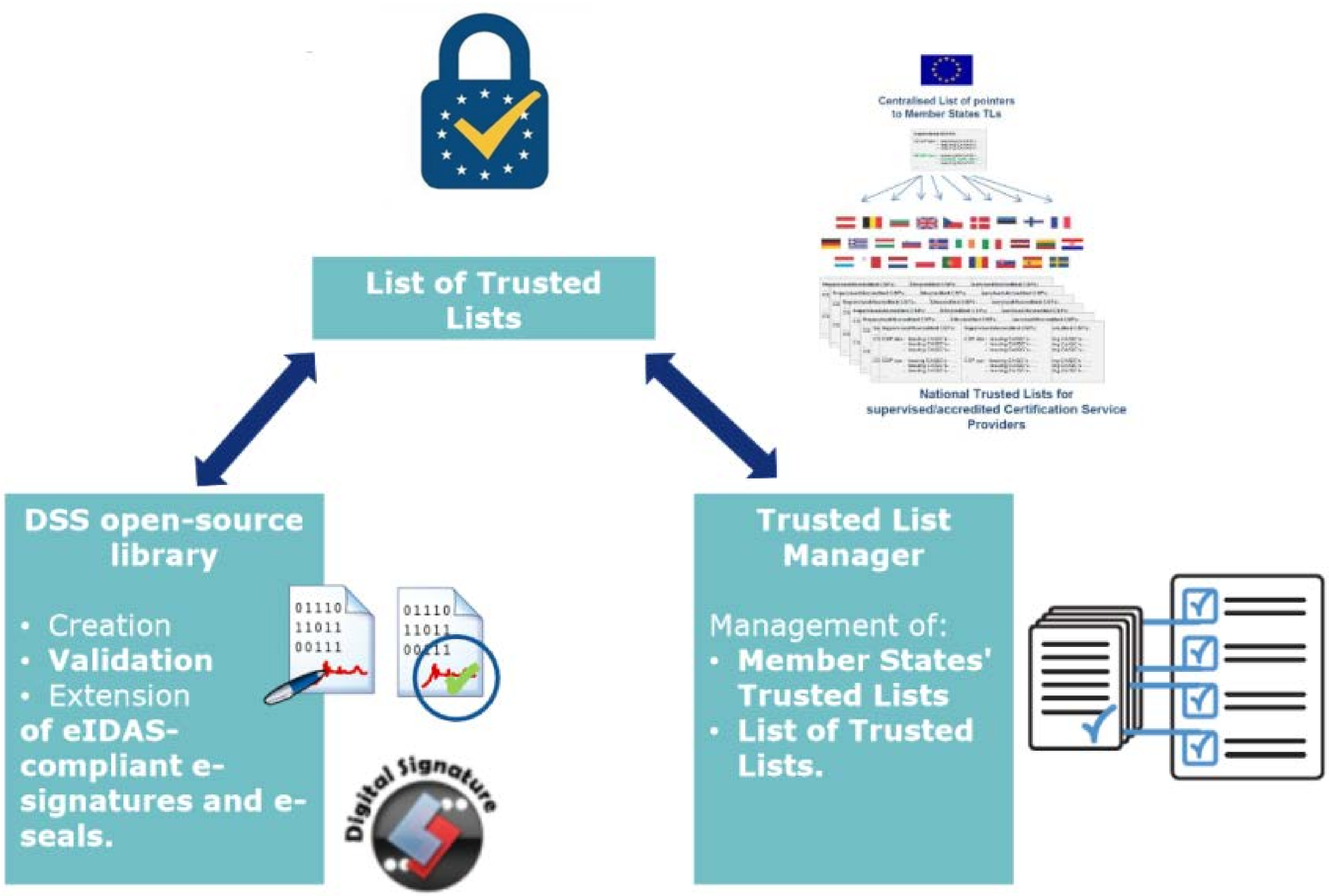
eIDAS Section 3 Article 22

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”



List of Trusted Lists

DSS open-source library

- Creation
- **Validation**
- Extension

of eIDAS-compliant e-signatures and e-seals.

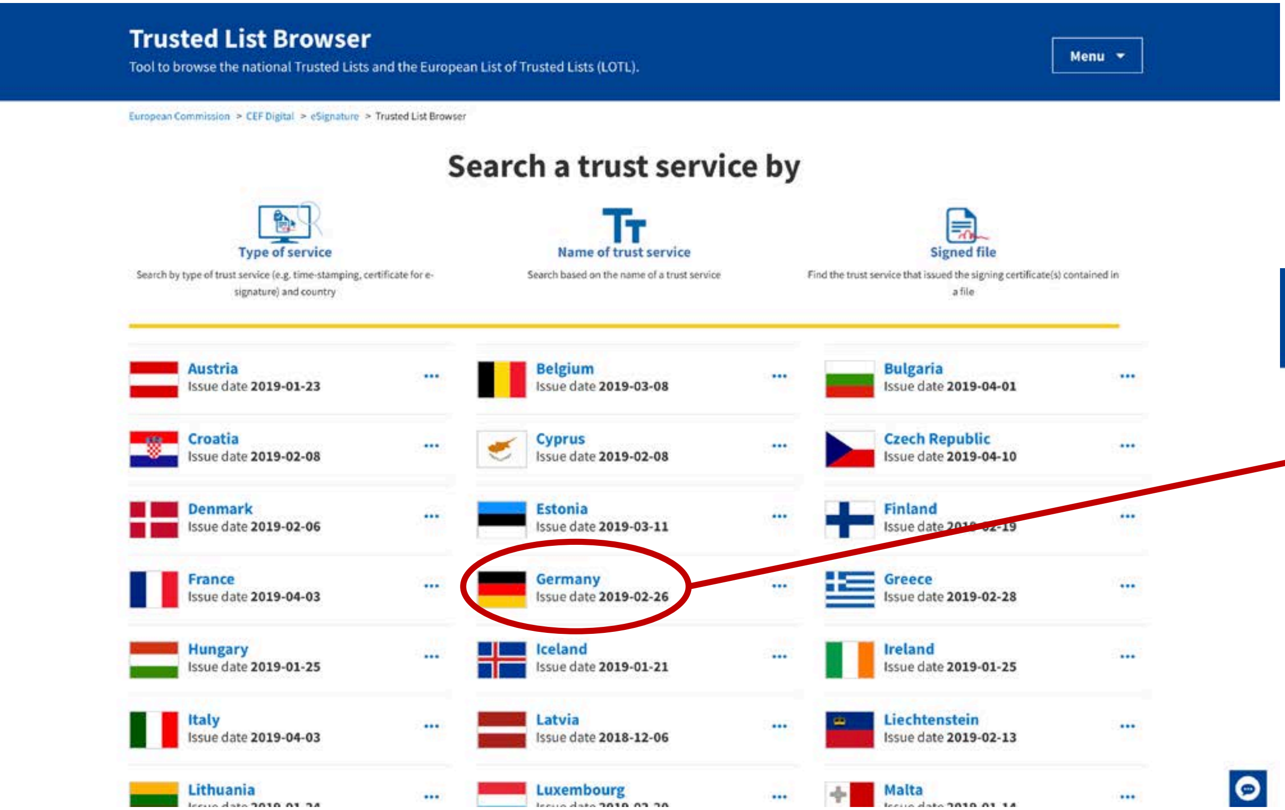
Trusted List Manager

Management of:

- **Member States' Trusted Lists**
- **List of Trusted Lists.**

Centralised List of pointers to Member States TLs
National Trusted Lists for supervised/accredited Certification Service Providers
01110
11011
00111
Digital Signature

Browsing the EU Trusted Lists



Trusted List Browser

Tool to browse the national Trusted Lists and the European List of Trusted Lists (LOTL).

European Commission > CEF Digital > eSignature > Trusted List Browser

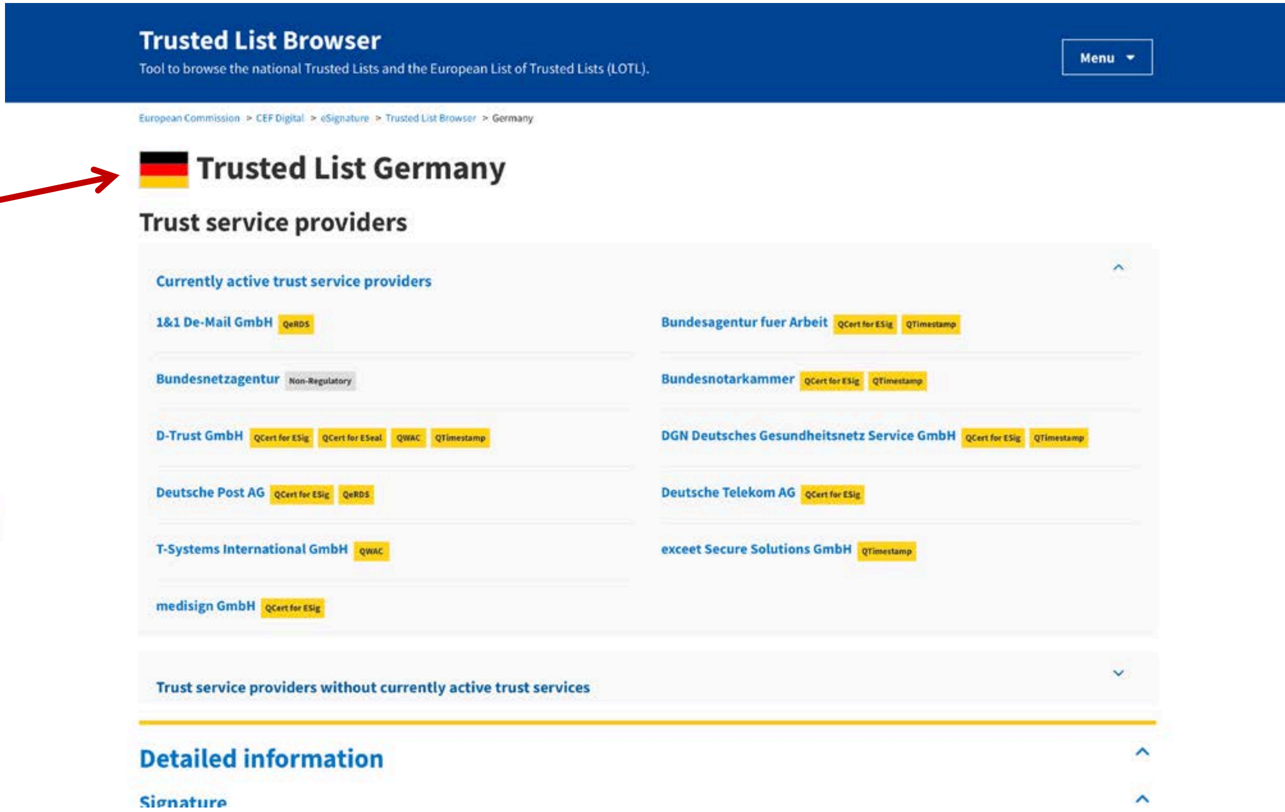
Search a trust service by

Type of service
Search by type of trust service (e.g. time-stamping, certificate for e-signature) and country

Name of trust service
Search based on the name of a trust service

Signed file
Find the trust service that issued the signing certificate(s) contained in a file

Austria Issue date 2019-01-23	Belgium Issue date 2019-03-08	Bulgaria Issue date 2019-04-01
Croatia Issue date 2019-02-08	Cyprus Issue date 2019-02-08	Czech Republic Issue date 2019-04-10
Denmark Issue date 2019-02-06	Estonia Issue date 2019-03-11	Finland Issue date 2019-02-19
France Issue date 2019-04-03	Germany Issue date 2019-02-26	Greece Issue date 2019-02-28
Hungary Issue date 2019-01-25	Iceland Issue date 2019-01-21	Ireland Issue date 2019-01-25
Italy Issue date 2019-04-03	Latvia Issue date 2018-12-06	Liechtenstein Issue date 2019-02-13
Lithuania Issue date 2019-01-24	Luxembourg Issue date 2019-02-20	Malta Issue date 2019-01-14



Trusted List Browser

Tool to browse the national Trusted Lists and the European List of Trusted Lists (LOTL).

European Commission > CEF Digital > eSignature > Trusted List Browser > Germany

Trusted List Germany

Trust service providers

Currently active trust service providers

- 1&1 De-Mail GmbH QeRDS
- Bundesagentur fuer Arbeit QCert for ESig QTimestamp
- Bundesnetzagentur Non-Regulatory
- Bundesnotarkammer QCert for ESig QTimestamp
- D-Trust GmbH QCert for ESig QCert for ESeal QWAC QTimestamp
- DGN Deutsches Gesundheitsnetz Service GmbH QCert for ESig QTimestamp
- Deutsche Post AG QCert for ESig QeRDS
- Deutsche Telekom AG QCert for ESig
- T-Systems International GmbH QWAC
- exceet Secure Solutions GmbH QTimestamp
- medisign GmbH QCert for ESig

Trust service providers without currently active trust services

Detailed information

Signature

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

STF 560
Globalisation of Trust Services

Presented by: **Nick Pope**

For: **Report to ESI #67**

05.06.2019

Agenda

- Workshops

- Draft Report

STF 560 Workshops on Globalisation of Trust Services

- Middle-east and Africa
- Asia
- Central and South America
- North America

Middle-east & Africa

General information

- Date: 2 May 2019
- Location: Dubai
- Attendance: 25 + 3 STF members
- Hosted by: Telecommunications Regulatory Authority (TRA) of the United Arab Emirates

Presentations

- STF - EU Study and standards framework
- EU Commission - eIDAS
- TRA - UAE National Trust service framework
- TRA – UEAPASS: First national digital identity
- Oman National PKI
- Arab-African e-Certification Authorities Network (AAECA)

Key Points

- Keen to work with EU
- AAECA: Maintain close liaison and suggest invite to ESI #68
- Make workshop slides available

Asia

General information

- Date: 23 May 2019
- Location: Tokyo
- Attendance: 120 (mainly Japanese + 2 from India)
- Hosted by: Keio University JIPDEC

Presentations

- STF - EU Study and standards framework
- EU Commission - eIDAS
- Ministry of Internal Affairs & Communications(MIC) & Ministry of Economy Trade and Industry (METI)
- JCAN Trusted Service Registration
- Japan Trust Technology Association (JT2A) Activities: Authenticity Guarantee & Remote Signatures
- Japan Trust Service Forum Society5.0 and Trust Services
- Japan Use cases: eContracts, Docusign, Spread of e-Contracting
- Asia Pacific Countries adoption of Trust Services (confidential)
- US Comparison with EU and Japan

Key Points

- Very keen to work with EU
- Need to justify Trust Services
- General METI model of Cyber security may provide useful context for Trust Services

Asia cont’d

Key Points

- Very keen to work with EU
- Need to justify Trust Services
- General METI model of Cyber security may provide useful context for Trust Services (also could be of interest to TC Cyber)
- ASIA PKI Forum
  - Report of Asia PKI when released should provide useful input to study report
  - Suggest establish ongoing liaison
- JIPDEC JT2A looking closely at adoption of ETSI & CEN standards for remote signing
- Workshop presentations: https://itc.jipdec.or.jp/20190523_shiryou.html

Central & South (Latin) America

General information

- Date: 27 June 2019
- Location: Mexico City
- Hosted by: Logalty

North America

General information(to be confirmed)

- Date: 1st week in September
- Location: New York
- Hosted by: EU UN Delegation Office

Technical Report on Global Acceptance of EU Trust Services
4 Pillars of Trust

Trust Services

Legal context

- Regulation vs contract
- Community
- Trust services
- Legal effect
- Legal requirements on TSP

Supervision & audit

- Oversight activities
- Verification against legal provisions
- Audit requirements
- Approval

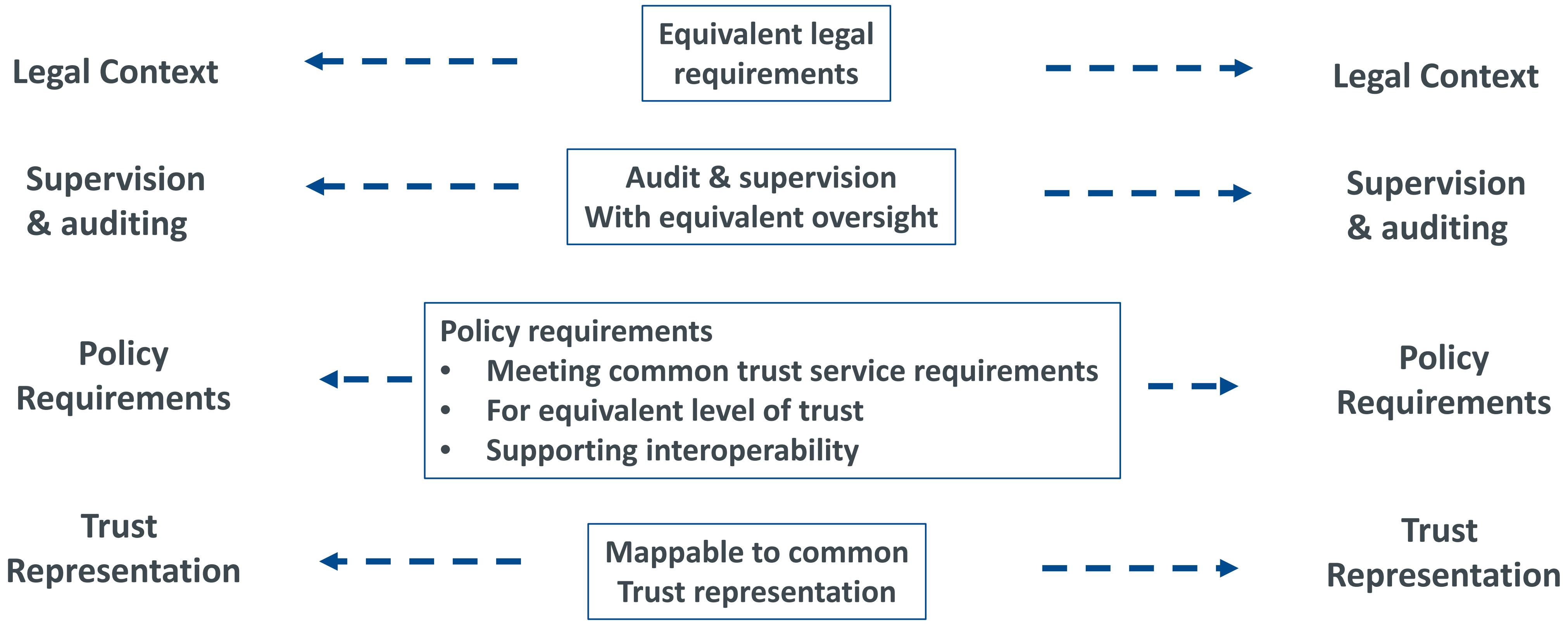
Policy requirements

- Security & policy requirement
- Technical criteria
- Interoperable protocols and formats

Trust representation

- Trusted List
- Root store
- Bridge certificates

Main points of comparison



Legal Context

Equivalent legal requirements

Legal Context

Supervision & auditing

Audit & supervision
With equivalent oversight

Supervision & auditing

Policy Requirements

Policy requirements
- Meeting common trust service requirements
- For equivalent level of trust
- Supporting interoperability

Policy Requirements

Trust Representation

Mappable to common Trust representation

Trust Representation

Information Collection

- International Legal Framework: UNCITRAL
- Industry : Adobe, Aerospace, Certipath, Safe-biopharma, Webtrust, ISO 27099…..
- South America: Argentina, Bolivia, Brazil. Chile, Columbia, Paraguay, Peru, Uruguay
- Middle-east & Africa: Arab-African eCA, Israel, ….
- Asia: Asia PKI Consortium, China, India, Japan, …
- Other: Russia, Switzerland

Analysis

Legal Context:

- General approach: regulatory vs contractual
- Enablers: non-qualified and advanced electronic signatures, specific level requirements for qualification.
- Barriers: Different trust services, cross border recognition

Supervision and audit:

- General approach:17065 + EN 319 403 vs Webtrust
- Enablers: International accreditation (EA & IAF)
- Barriers: Lack of accreditation framework for trust services

Policy requirements

- General approach: X.509, RFC 3647
- Enablers: Use of EN 319 411-x or earlier equivalents, CA/B Forum, ISO standards (21188 -> 27009)
- Barriers: Lack of common basis for policy requirements

Trust representation

- General approach: National root, root stores, Trusted lists, cross certification
- Enablers: Trusted lists
- Barriers: Mapping between different approval levels

Cooperation with CA/B-Forum:

- ETSI ESI has adopted SR 119 403-3 (extended Audit Rules for PTC) as requested by Mozilla, official version is published

https://www.etsi.org/deliver/etsi_ts/119400_119499/11940302/01.02.01_60/ts_11940302v010201p.pdf

- ETSI ESI is still discussing the comments on EN 319 403 (Audit Rules) , no quick win at last meeting, new round ongoing, Key Lifecycle; matching ISO 17065
- ETSI has set up a new work item on updating EN 319411-1 (Certification Policy) update on BR/EVG Links,
- New ETSI secretariat eMail-Adress to communicate with CA/B-Forum