ETSI — The Standards People

EU standards for Certification Authorities and Cross Recognition

Presented by: **Arno Fiedler - Nimbus**
Vice Chair ETSI TC on Electronic signatures and (Trust) Infrastructures (ESI)

For: **International Workshop on Cross Border Recognition of Certifying Authorities**

07.09.2022

Agenda

- ➢ - Introduction to eIDAS and Trust Services in Europe

- ➢ - Standards for Trust Service Providers Issuing Certificates

- ➢ - Audit and supervision of Trust Services

- ➢ - Trusted lists

- ➢ - International cross recognition

- ➢ - Q&A

EU Directive on electronic identification and trust services for electronic transactions 910 2014: (eIDAS)
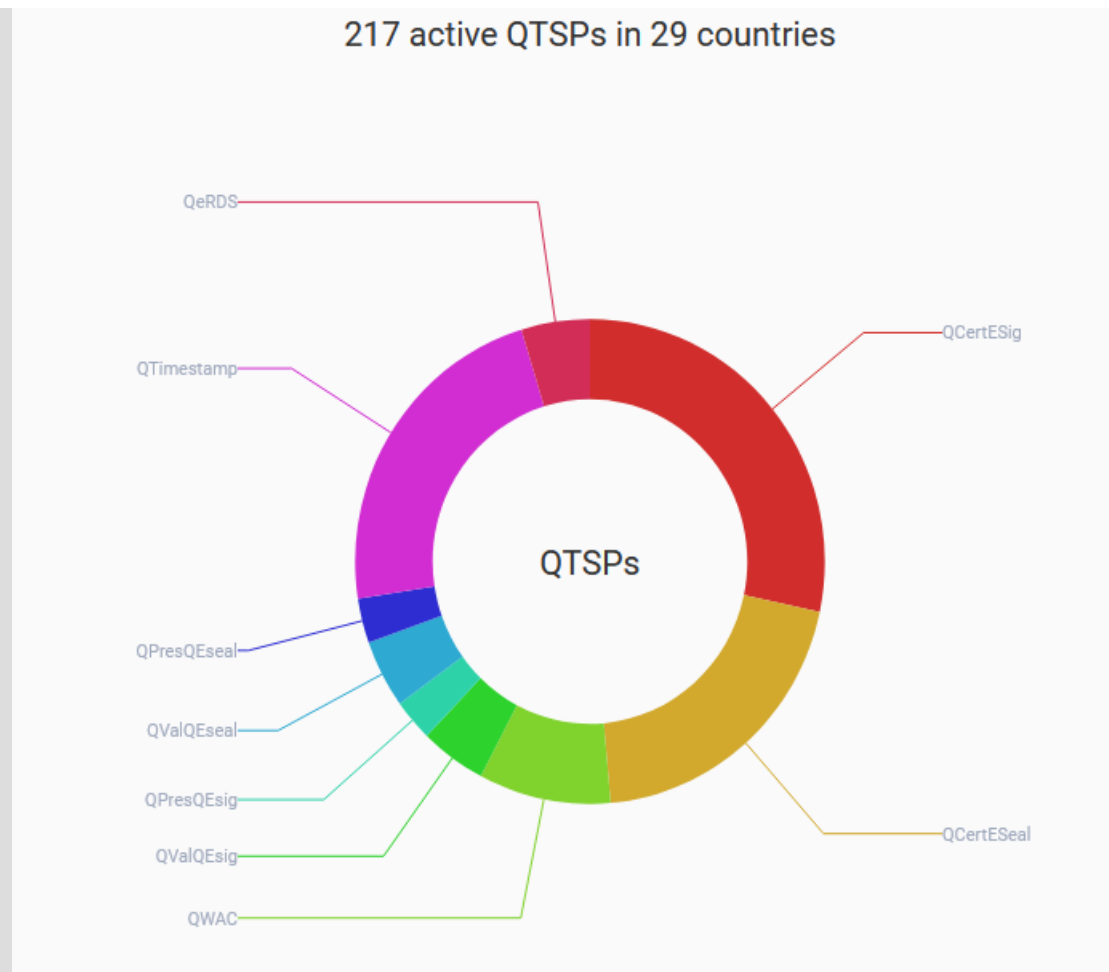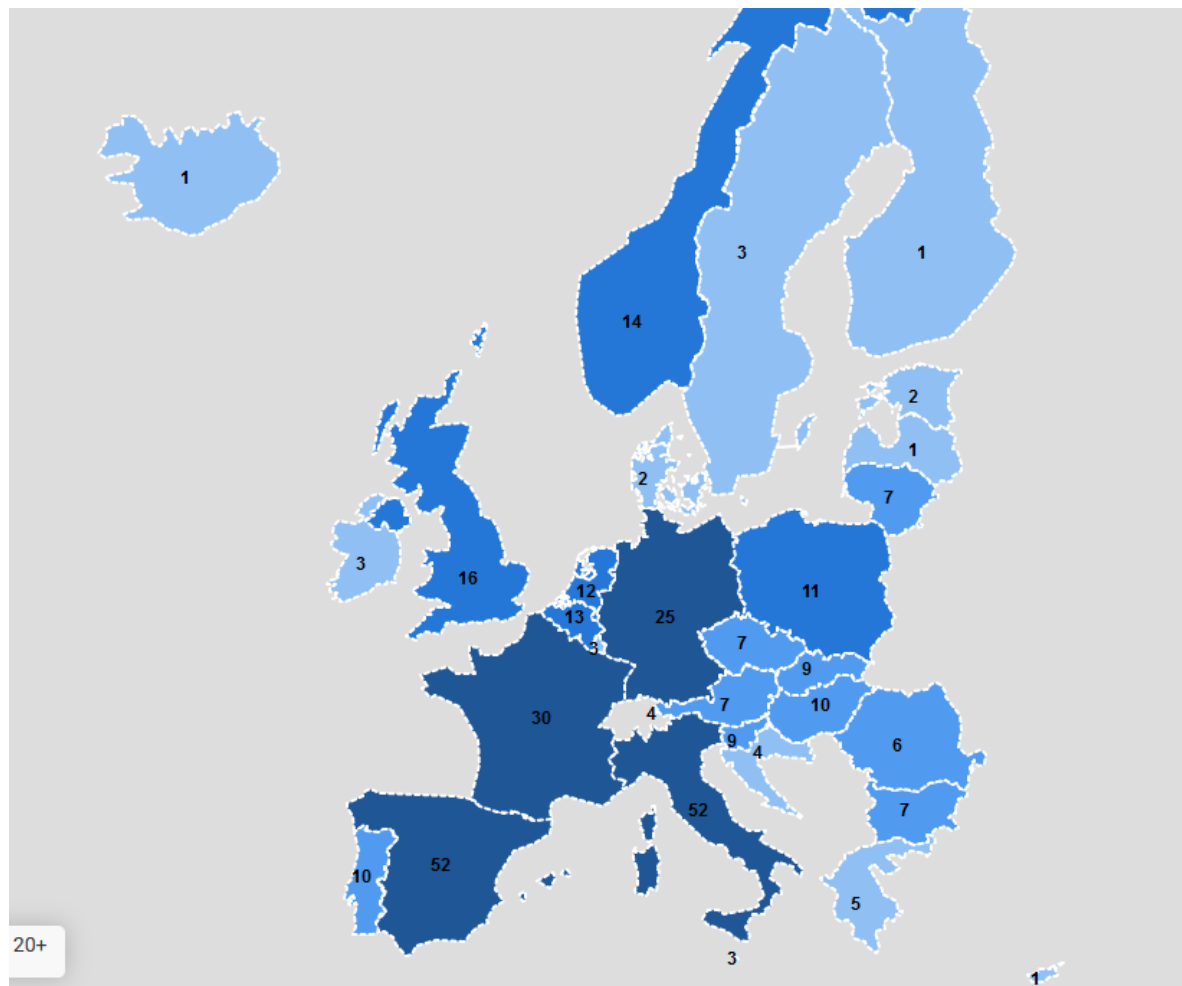
Provides regulatory framework for support for provision of Trust Services across Europe

➢ Trust Services issuing certificates (i.e. Certificate Authorities) for:

- ➢ Electronic Signatures for Natural Persons
- ➢ Electronic Seals for legal persons
- ➢ Website Authentication

➢ + Other trust services e.g. Registered e-Mail, Signature Validation
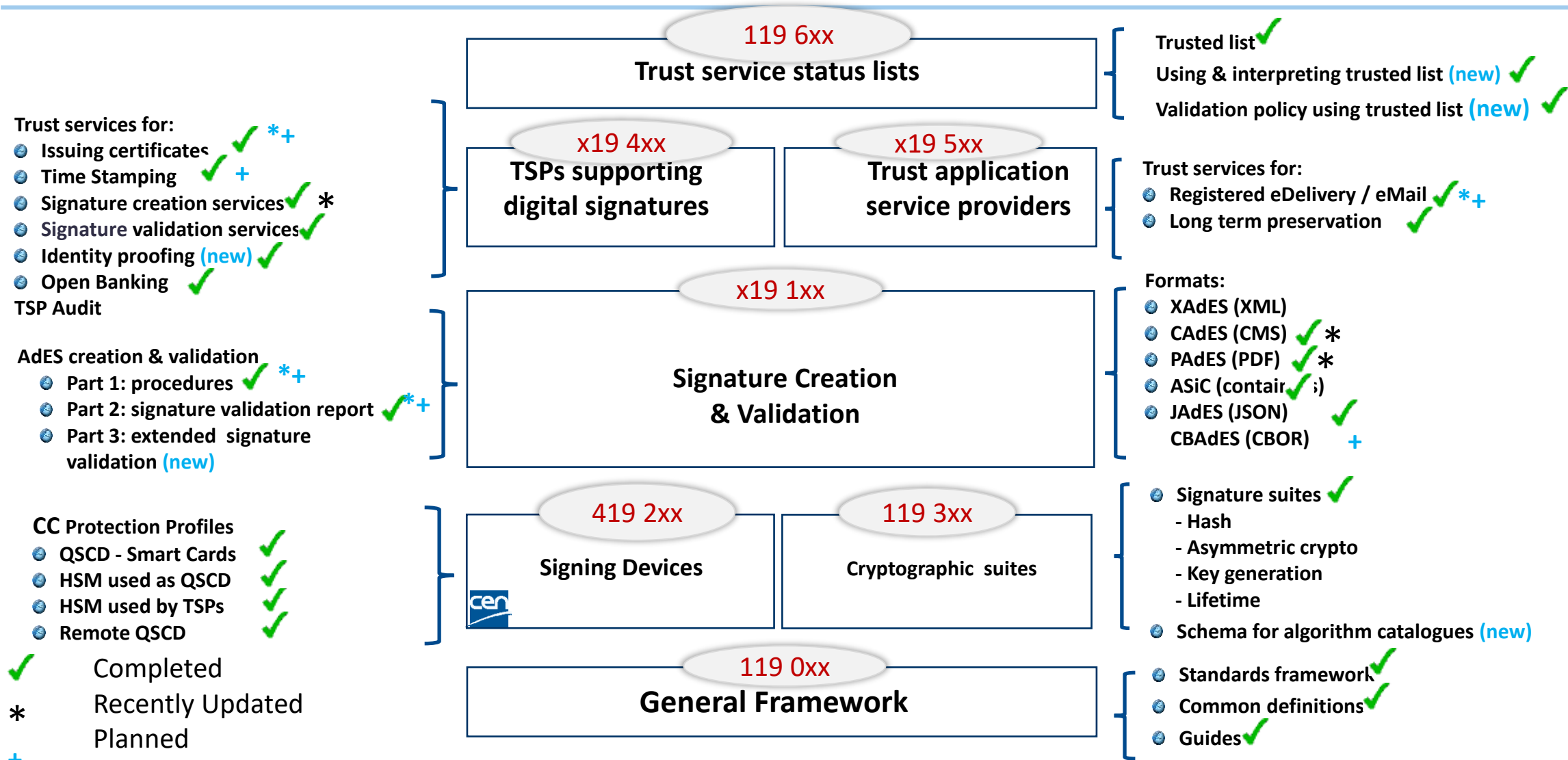
Defines specific requirements for "Qualified" Trust Services

➢ Functional and certificate content requirements

➢ Third Party Audit against best practices based on eIDAS regulatory requirement

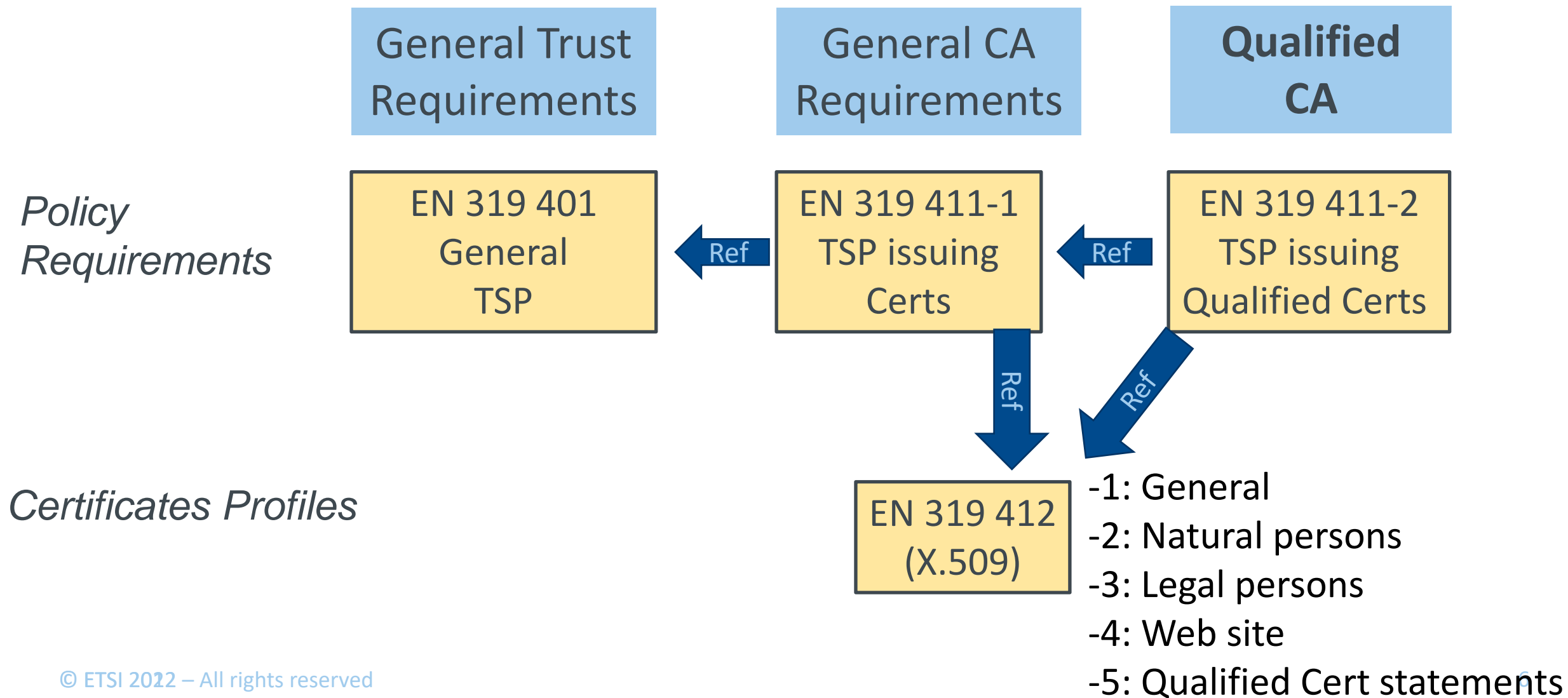➢ Nations issue Trust Lists of "Qualified Trust Service Providers"

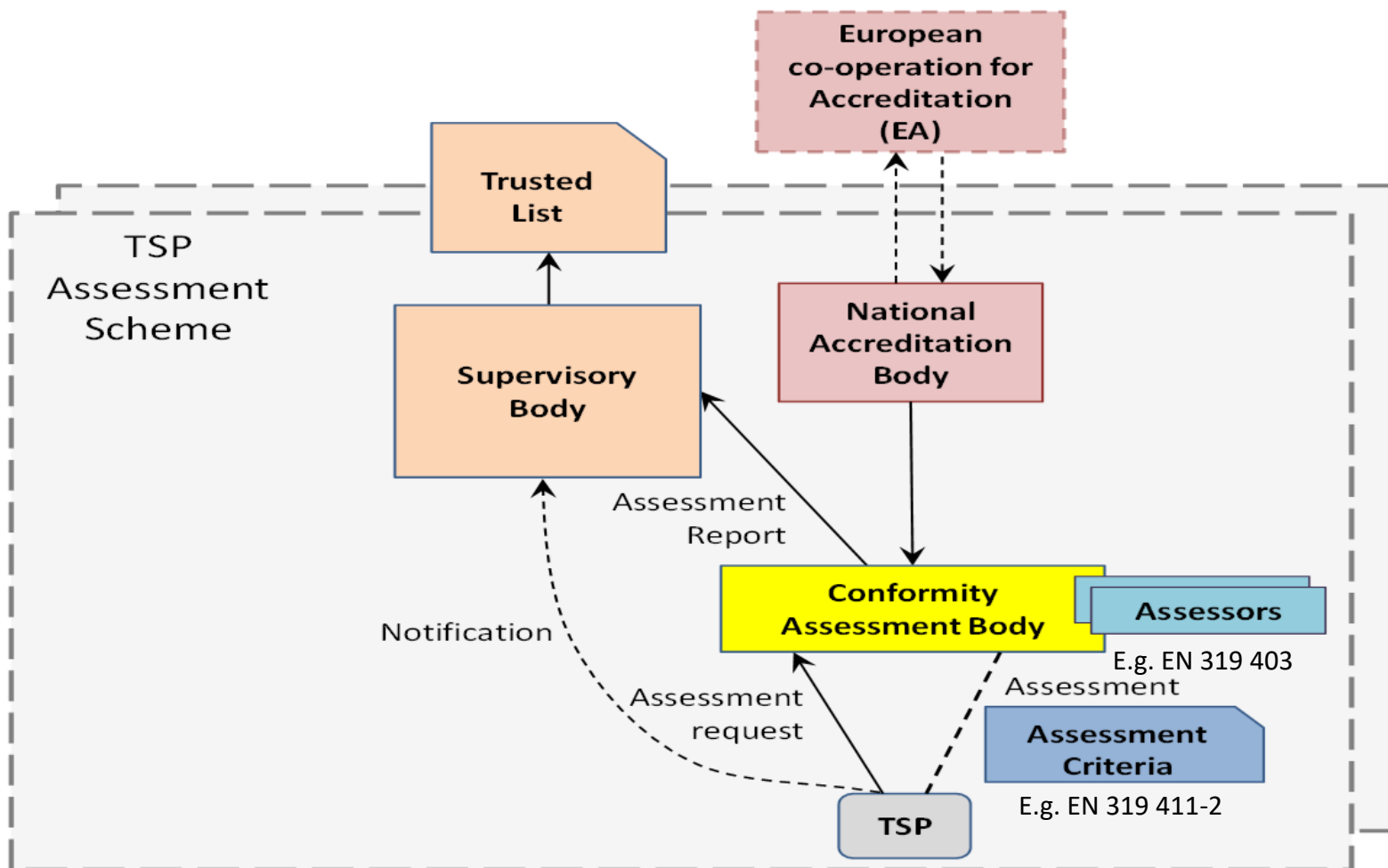# QTSP in Europe Sept. 2022, see: EU Trust Services Dashboard:

217 active QTSPs in 29 countries

ETSI & CEN Standards supporting eIDAS – the overall picture

119 6xx
Trust service status lists

Trusted list ✔
Using & interpreting trusted list (new) ✔
Validation policy using trusted list (new) ✔

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

TSP Audit

x19 4xx
TSPs supporting digital signatures

x19 5xx
Trust application service providers

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

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

x19 1xx
Signature Creation & Validation

Formats:
- XAdES (XML)
- CAdES (CMS) ✔ *
- PAdES (PDF) ✔ *
- ASiC (containers) ✔
- JAdES (JSON) ✔
- CBAdES (CBOR) +

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

419 2xx
Signing Devices

119 3xx
Cryptographic suites

- Signature suites ✔
  - Hash
  - Asymmetric crypto
  - Key generation
  - Lifetime
- Schema for algorithm catalogues (new)

✔ Completed
* Recently Updated
+ Planned

119 0xx
General Framework

- Standards framework ✔
- Common definitions ✔
- Guides ✔

Trust services issuing certificates: ETSI standards overview

General Trust Requirements	General CA Requirements	**Qualified CA**

Policy Requirements

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

Ref ← (EN 319 411-1 → EN 319 401)

Ref ← (EN 319 411-2 → EN 319 411-1)

Ref ↓ (EN 319 411-1 → EN 319 412)

Ref ↘ (EN 319 411-2 → EN 319 412)

Certificates Profiles

EN 319 412 (X.509)

-1: General
-2: Natural persons
-3: Legal persons
-4: Web site
-5: Qualified Cert statements
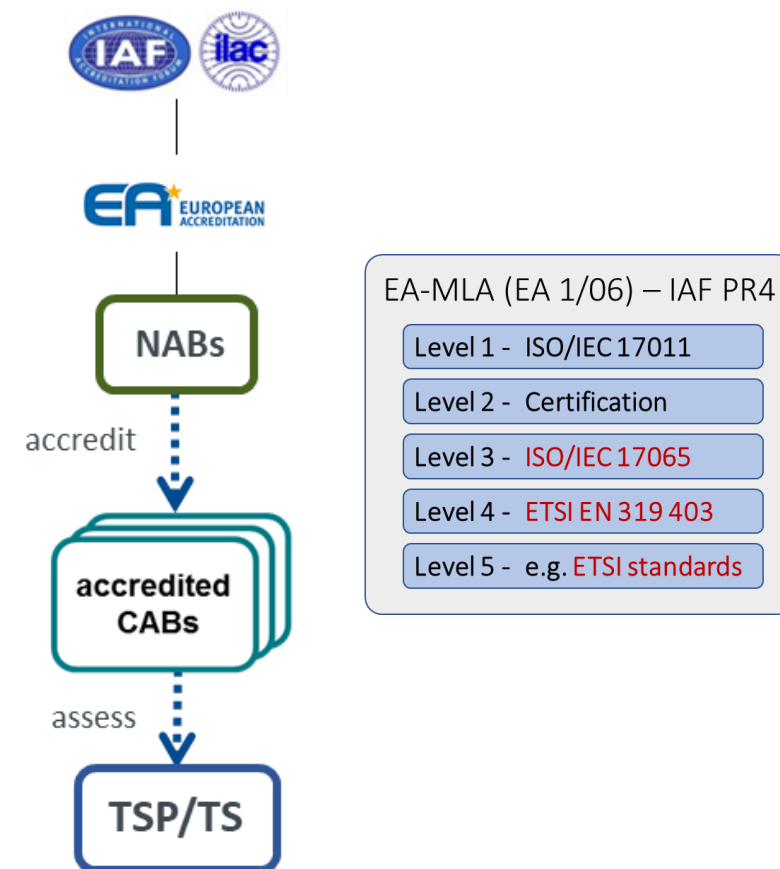
TSP+CAB+SB=>TSL

ETSI Best practise audit framework

EN 319 403-1 on requirements for bodies auditing TSPs

- ➢ Primary reference: **ISO/IEC 17065** specifying general requirements for conformity assessment bodies (CABs) performing certification of products, processes, or services

- ➢ Supplements ISO/IEC 17065 to provide additional dedicated requirements for CABs performing certification of TSPs

- ➢ Incorporates additional requirements on CABs relating to the audit of a TSP's management system, as defined in **ISO/IEC 17021** and in **ISO/IEC 27006**

New supplements on additional requirements for CABs auditing

- ➢ Part 2: TSPs issuing PTC (e.g. as in CA/Browser Forum)
- ➢ Part 3: QTSPs against eIDAS Regulation

EA-MLA (EA 1/06) – IAF PR4

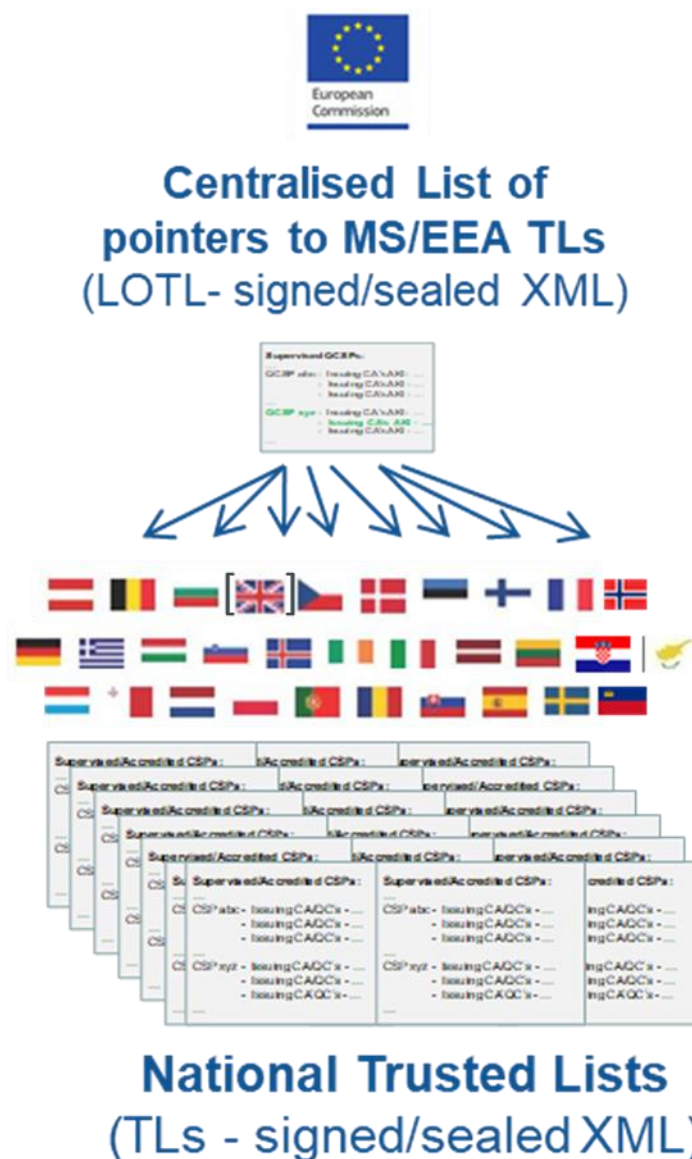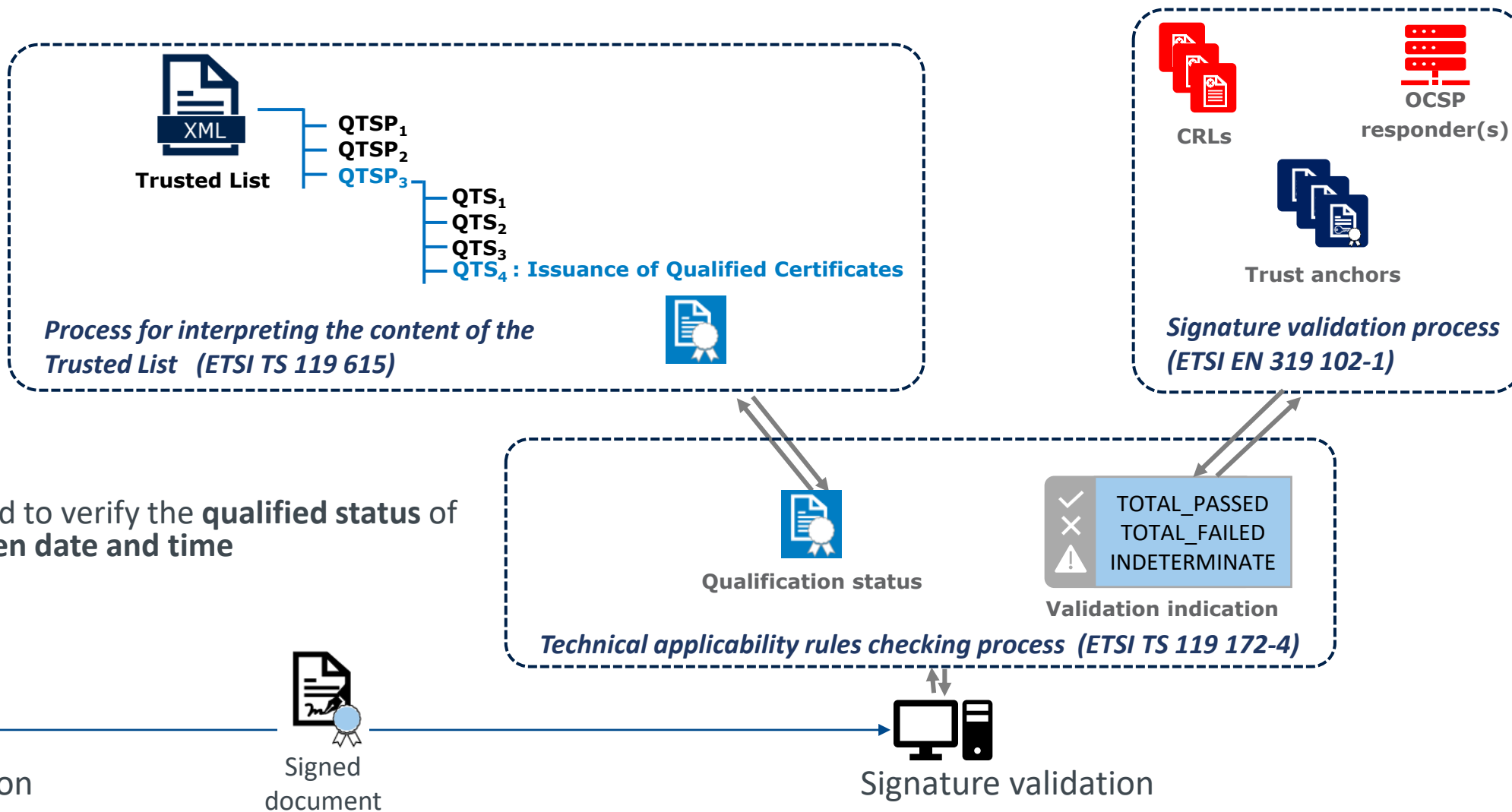| Level 1 - | ISO/IEC 17011 |
Level 2 -	Certification
Level 3 -	ISO/IEC 17065
Level 4 -	ETSI EN 319 403
Level 5 -	e.g. ETSI standards

Trusted List – what it is

ETSI TS 119 612 (Trusted List)

Regional – Multi-country schemes

- List of the Lists (LOTL)
- Facilitating discovery, authentication and grouping of trusted lists pertaining to a common ecosystem / approval scheme

e.g. European LOTL whose authenticity and integrity can be verified via a publication in the Official Journal of the EU and the concept of pivot-LOTL
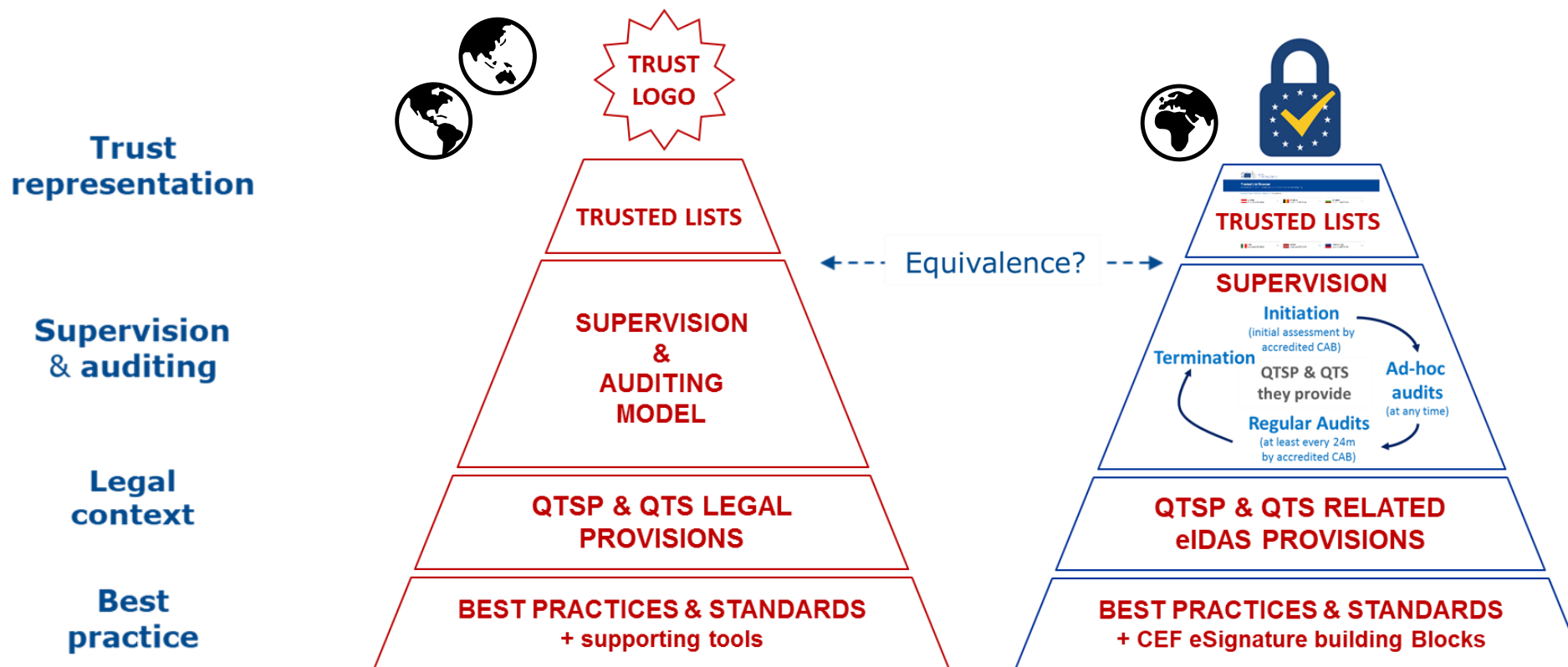

Centralised List of pointers to MS/EEA TLs
(LOTL- signed/sealed XML)

National Trusted Lists
(TLs - signed/sealed XML)

Trusted List – usage by relying parties

Process for interpreting the content of the Trusted List (ETSI TS 119 615)

- QTSP₁
- QTSP₂
- QTSP₃
  - QTS₁
  - QTS₂
  - QTS₃
  - QTS₄ : Issuance of Qualified Certificates

Trusted List

CRLs

OCSP responder(s)

Trust anchors

Signature validation process (ETSI EN 319 102-1)

Trusted Lists are used to verify the **qualified status** of trust tokens at a **given date and time**

Qualification status

TOTAL_PASSED
TOTAL_FAILED
INDETERMINATE

Validation indication

Technical applicability rules checking process (ETSI TS 119 172-4)

Signature creation

Signed document

Signature validation

Mutual recognition of electronic trust services

∨ Four-pillar methodology

Further information

Information on Signatures and Trust Services standards :
   https://portal.etsi.org/TBSiteMap/ESI/ESIActivities.aspx

ETSI standards: available for free download: http://www.etsi.org/standards-search

News list on Signatures and trust services:
   https://list.etsi.org/scripts/wa.exe?SUBED1=e-signatures_news&A=1

The slides & a recording of the training session on eIDAS trust Services:

https://www.etsi.org/events/1926-webinar-etsi-standards-for-trust-services-and-digital-signatures

ENISA Study: Towards global acceptance of eIDAS audits
https://www.enisa.europa.eu/publications/towards-global-acceptance-of-eidas-audits

https://esignature.ec.europa.eu/efda/home/#/screen/home

12