The Standards People

Trusted Lists & Mutual Recognition of non-EU Trust Services

Presented by: **Olivier Delos**
Sealed

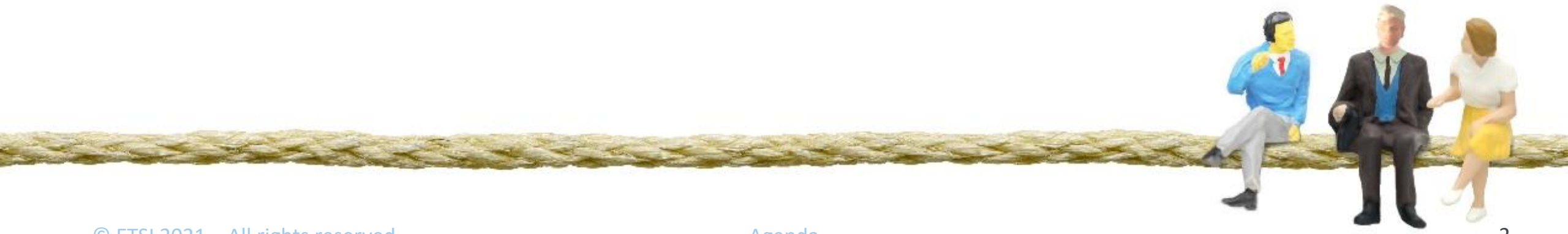
For: **ETSI Standards Training Webinar**

01.06.2021

© ETSI 2021 – All rights reserved

Agenda

- Subject 7 – Trusted lists



© ETSI 2021 – All rights reserved

Trusted List – what it is

EU Member States Trusted Lists are **constitutive** instruments on:

- Who is **QTSP** for what type of **QTS**
- Legal certainty with regards to QTS

Mandatory listing of QTSP/QTS

Optional listing of non-Q TSP and non-Q TS on a national basis based on national approval scheme

The Trusted List (TL) format is specified in CID (EU) 2015/1505 building upon ETSI TS 119 612 (v2.1.1):

- **Hierarchical** structure: TL – TSP – TS – TS history
- **Signed** XML file
- **Machine-processable** information

Standard guidance for the **interpretation** of the EU MS Trusted Lists is specified in ETSI TS 119 615

© ETSI 2021 – All rights reserved

(Q)TSP: (Qualified) Trust Service Provider
(Q)TS: (Qualified) Trust Service

Trusted List – what it is

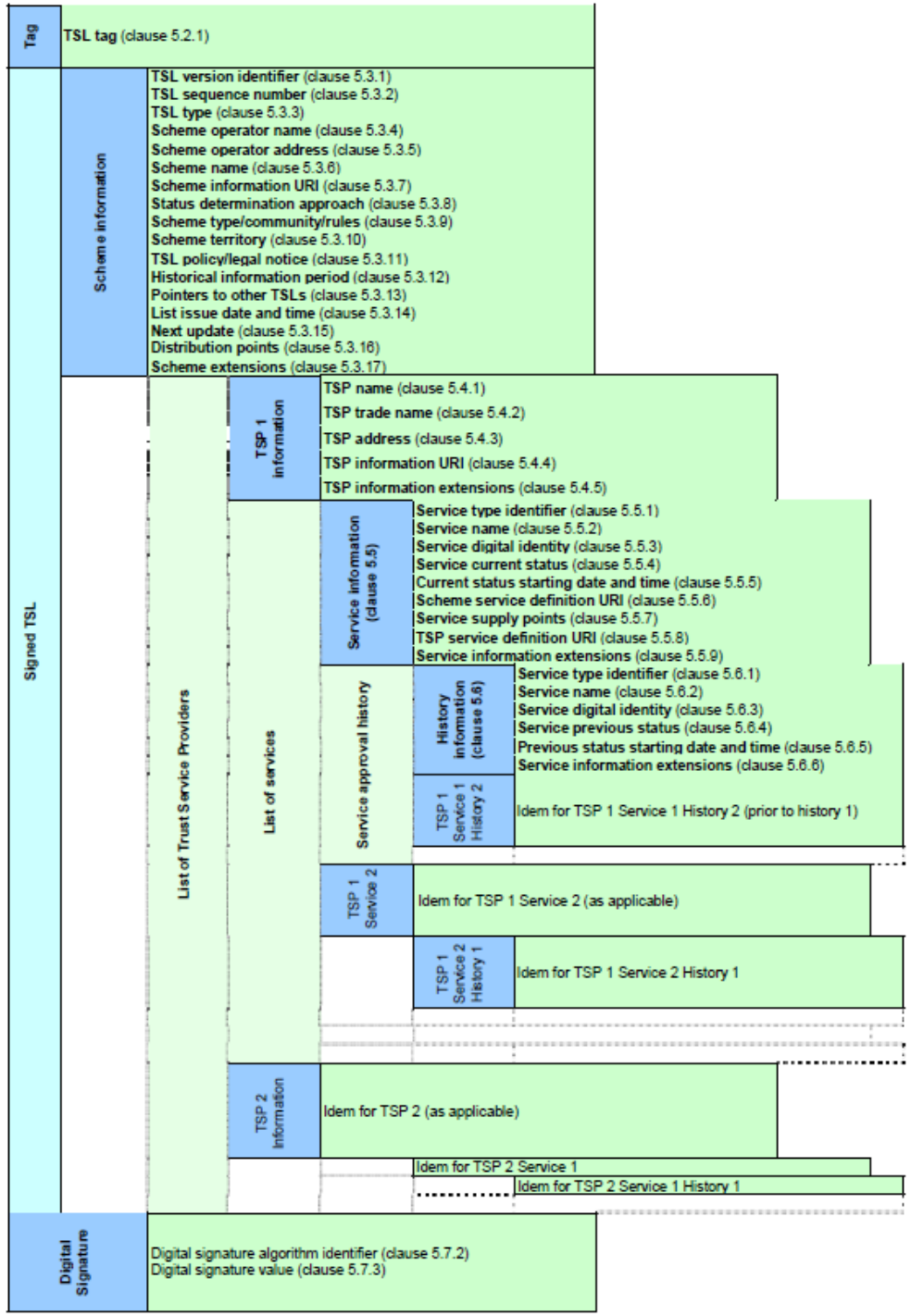
Information on the TL **scheme** and TL **operator**:

- TLSO (issuer – operator of the TL)
  - Name
  - Postal and electronic address
- Information on scheme:
  - Territory
  - URI pointing to information on supervision scheme
  - Type of the list, scheme name, legal notice
  - Date of issuance and expiry
  - Info on status values, Usage rules: how to use/interpret the TL

Pointer to other TLs (e.g. EC **LOTL**)

List of (Q)TSPs and the (Q)TSs they provide

- (Q)TSP (Name, postal and electronic address)
- URI pointing to information on QTSP practices (e.g. CP/CPS, GTC, legal info, etc.)
- (Q)TS service entries (per service entry)
  - "Digital Identity" (trust anchor)
  - "Service type" (and additional service information)
  - Current status (and service information extensions)
  - Full history (at least one history entry per status change)



© ETSI 2021 – All rights reserved

Trusted List – what it is

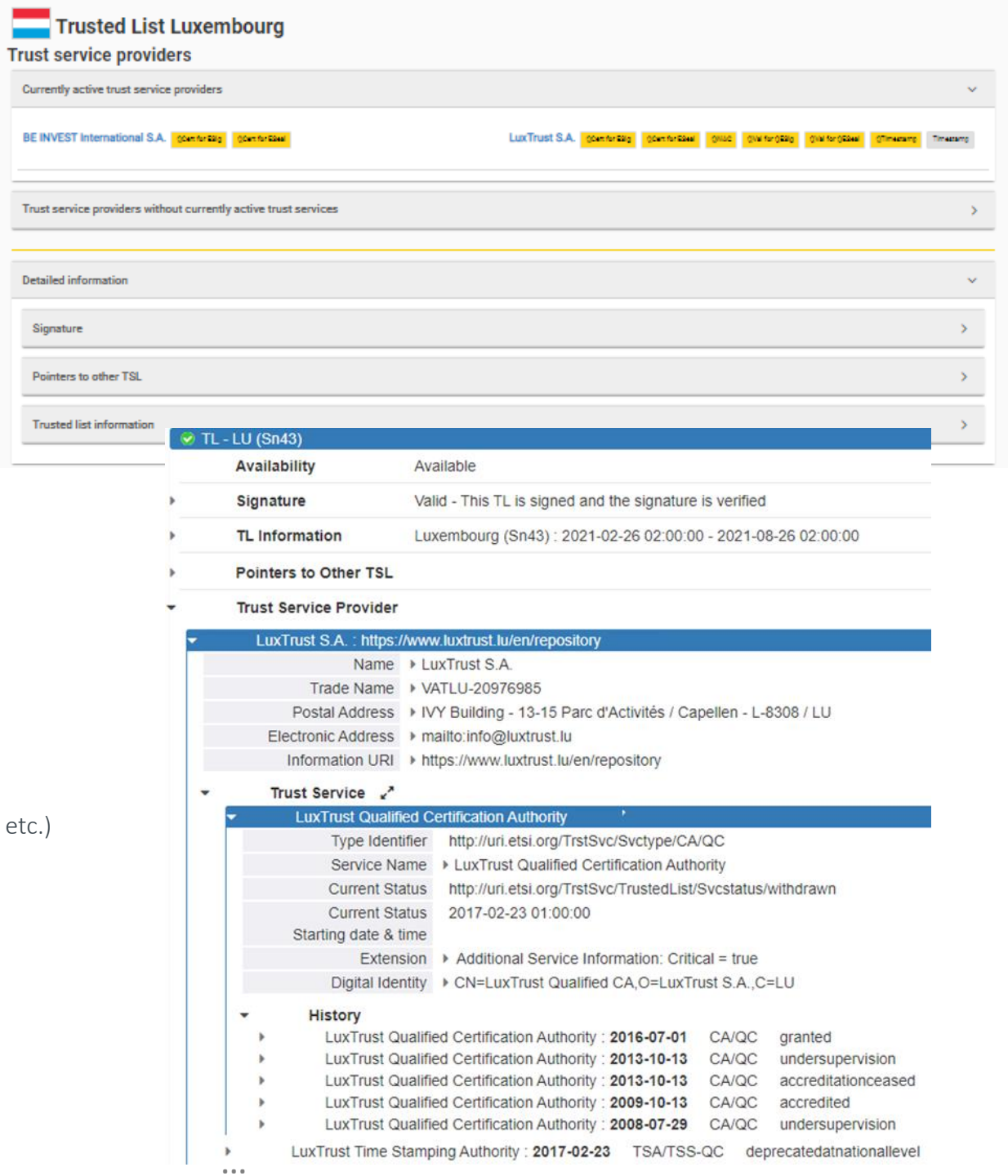
Information on the TL **scheme** and TL **operator**:

- TLSO (issuer – operator of the TL)
  - Name
  - Postal and electronic address
- Information on scheme:
  - Territory
  - URI pointing to information on supervision scheme
  - Type of the list, scheme name, legal notice
  - Date of issuance and expiry
  - Info on status values, Usage rules: how to use/interpret the TL

Pointer to other TLs (e.g. EC **LOTL**)

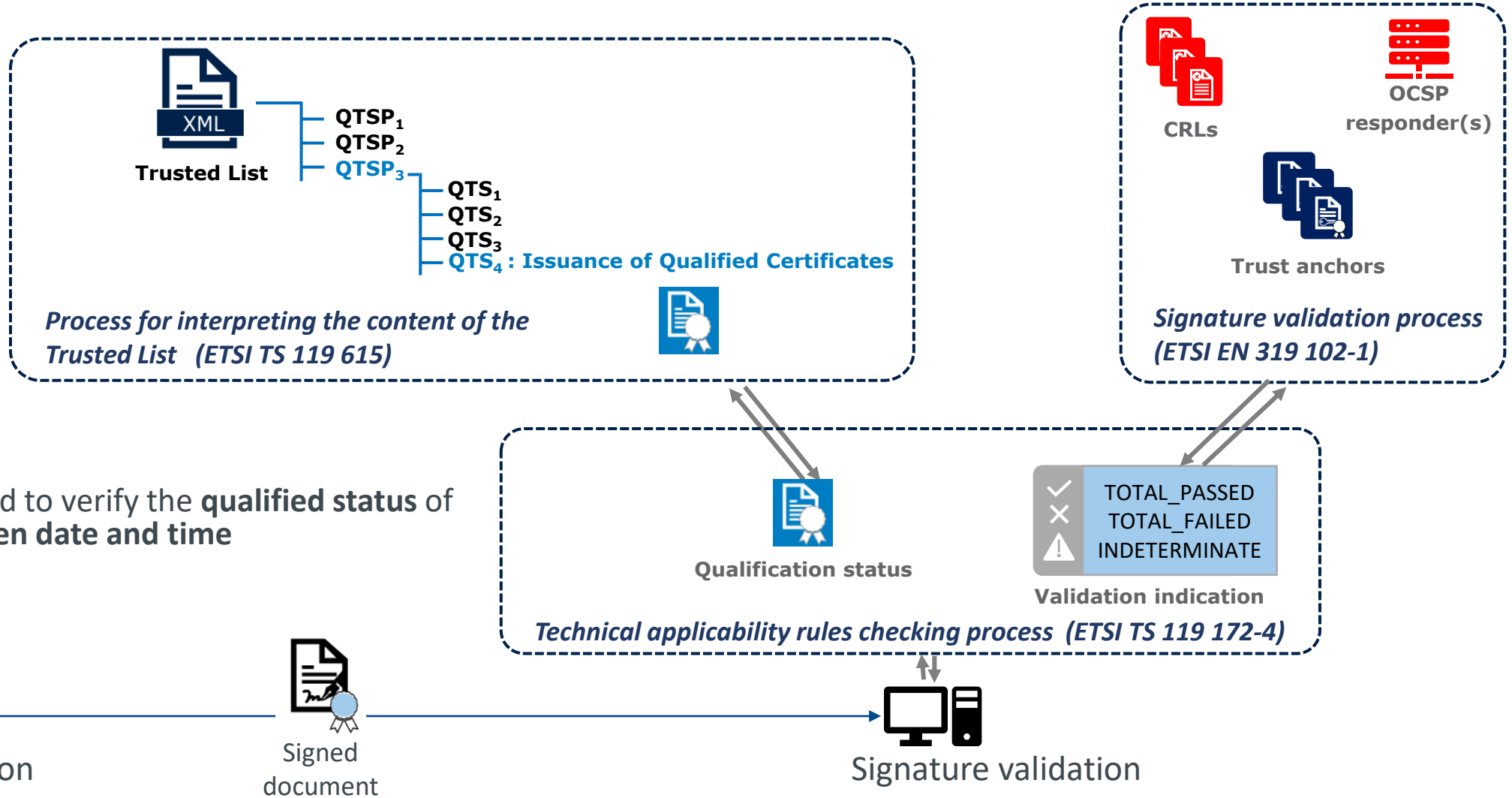
List of (Q)TSPs and the (Q)TSs they provide

- (Q)TSP (Name, postal and electronic address)
- URI pointing to information on QTSP practices (e.g. CP/CPS, GTC, legal info, etc.)
- (Q)TS service entries (per service entry)
  - "Digital Identity" (trust anchor)
  - "Service type" (and additional service information)
  - Current status (and service information extensions)
  - Full history (at least one history entry per status change)



© ETSI 2021 – All rights reserved

Trusted List – usage by relying parties



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

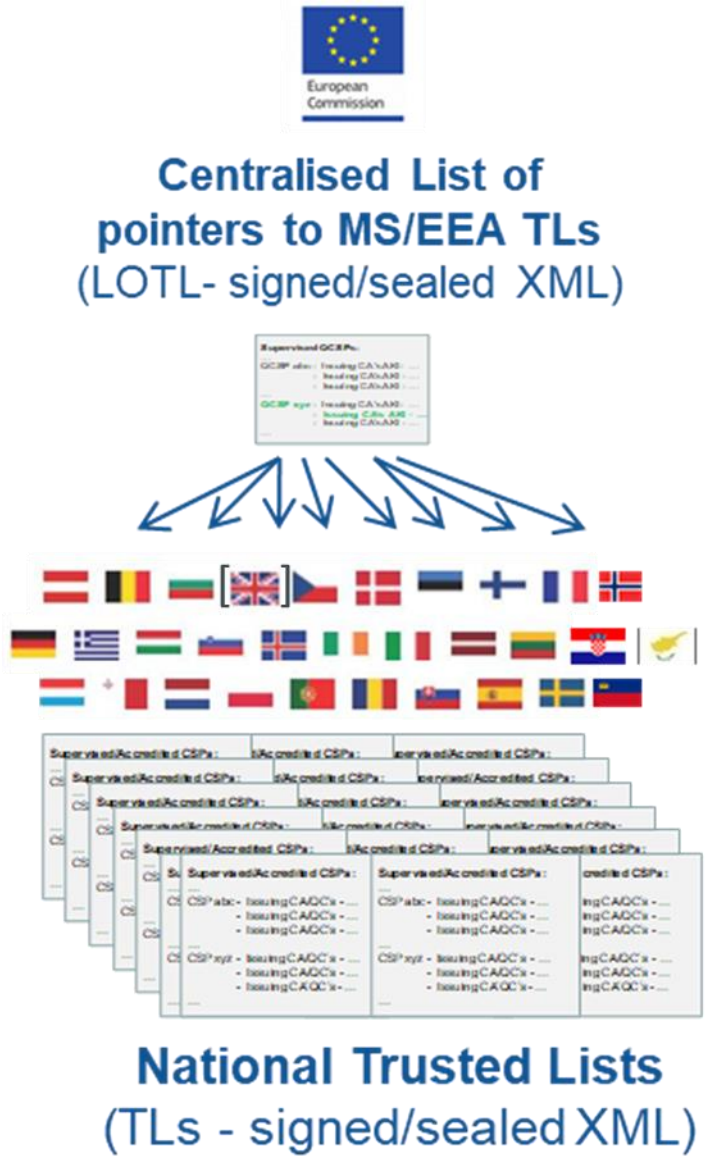
© ETSI 2021 – All rights reserved

Trusted List – what it is

ETSI TS 119 612 allows for 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



© ETSI 2021 – All rights reserved

Trusted List – what for non EU countries

ETSI TS 119 612 may be used by nonEU countries and (international) organisations to determine:

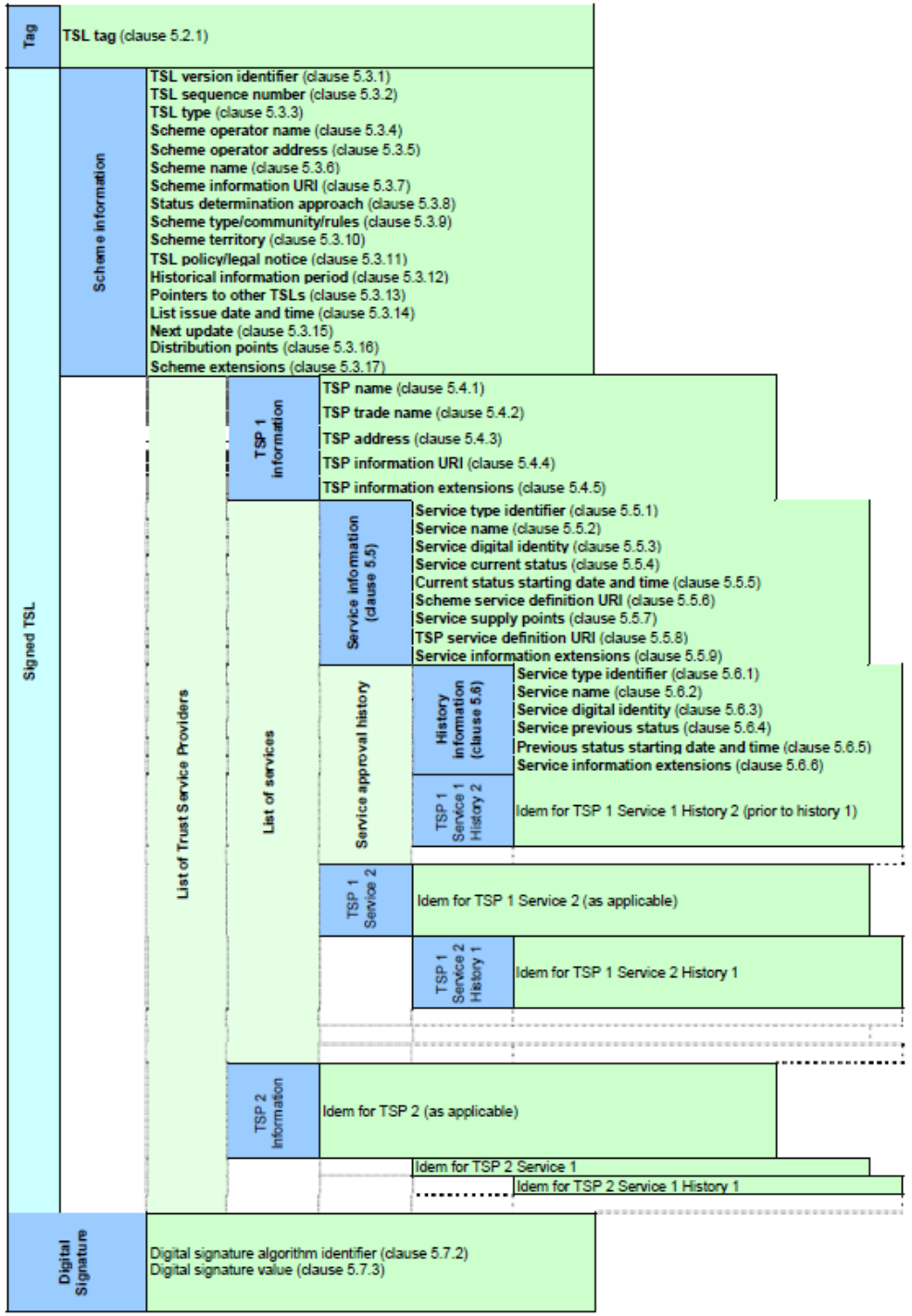
- whether a trust service is or was operating in compliance with relevant requirements,
- currently or at a given time in the past (e.g. provision time, transaction time)

Facilitates the declaration of mutual recognition between trust services and their outputs, e.g.:

- within or between groups of nations/organisations outside the EU
- Between EU and other nations/organisations outside the EU (actually use of trusted lists is a pre-requisite in this case)

Tips/requirements

- Make use of nonEU country or organisation specific URIs for Service type identifiers, Service statuses, qualification extensions and qualifiers – Do not use eIDAS Regulation specific URIs
- Define benchmark or require use of EN 319 412-5 statements applicable to nonEU context in nonEU "qualified" certificates

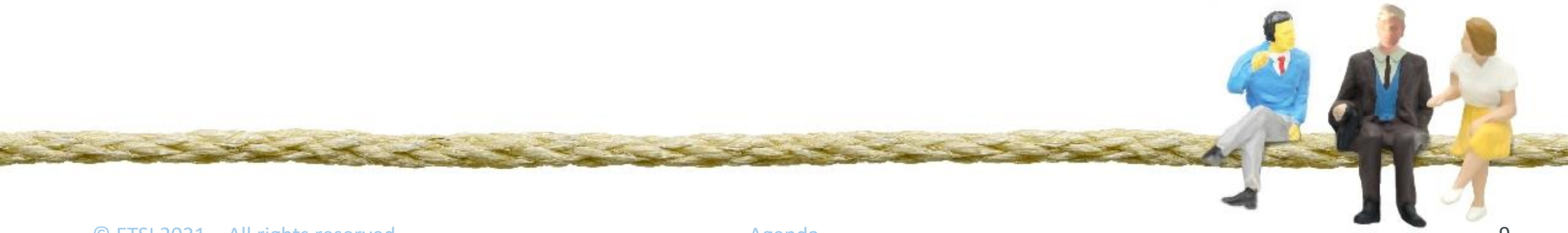


© ETSI 2021 – All rights reserved

Cf. CEF International Preparedness Project

Agenda

- Subject 8 – Mutual recognition of electronic trust services



© ETSI 2021 – All rights reserved

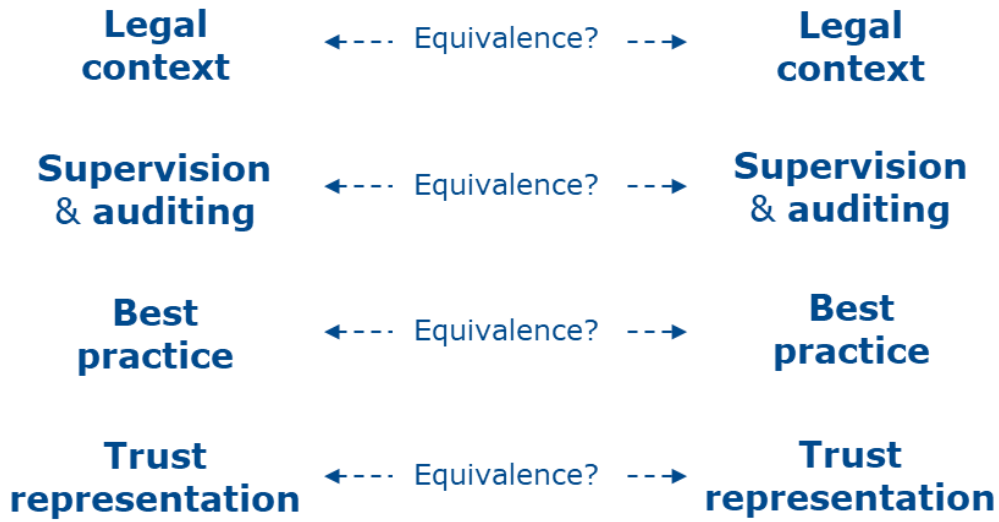
Mutual recognition of electronic trust services

- Various types
  - eSignatures, eSeals, time stamps, electronic delivery services, website authentication, preservation / archiving, validation, …
  - Key building block / commodity supporting electronic transactions and digital economy
- Benefits of harmonization of
  - Laws
  - Supervision
  - Technical (best) practices
  - Trust representation
  - … for cross-border electronic transactions and digital economies

© ETSI 2021 – All rights reserved

Mutual recognition of electronic trust services

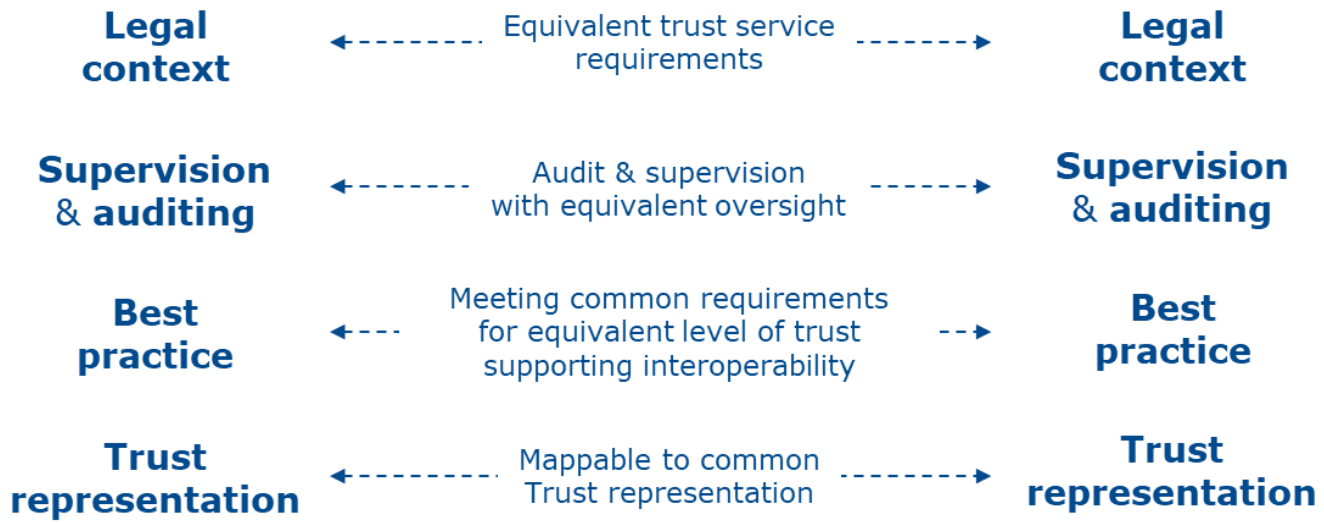
- Looking for harmonization, interoperability & mutual recognition of electronic trust services …
- … Four-pillar methodology reveals useful for comparing (PKI-based) trust services frameworks (cf. ETSI TR 103 684 report)
  - in a view establishing a benchmark
  - in a view establishing a national / regional framework
  - in a view of establishing recognition



© ETSI 2021 – All rights reserved

Mutual recognition of electronic trust services

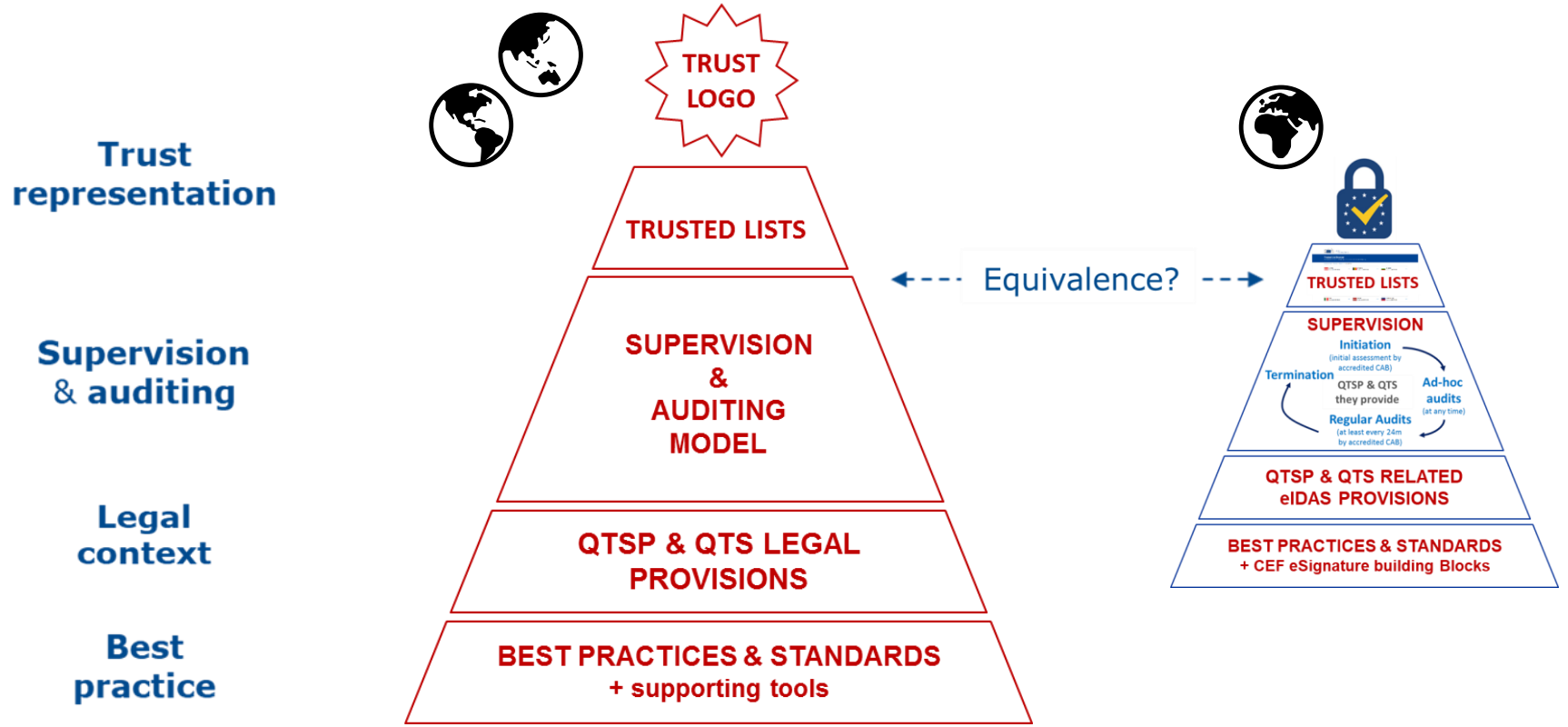
- Looking for harmonization, interoperability & mutual recognition of electronic trust services …
- … Four-pillar methodology reveals useful for comparing (PKI-based) trust services frameworks (cf. ETSI TR 103 684 report)
  - in a view establishing a benchmark
  - in a view establishing a national / regional framework
  - in a view of establishing recognition



© ETSI 2021 – All rights reserved

Mutual recognition of electronic trust services

- Four-pillar methodology
  - in a view establishing a national / regional framework



Mutual recognition as per eIDAS Art.14:

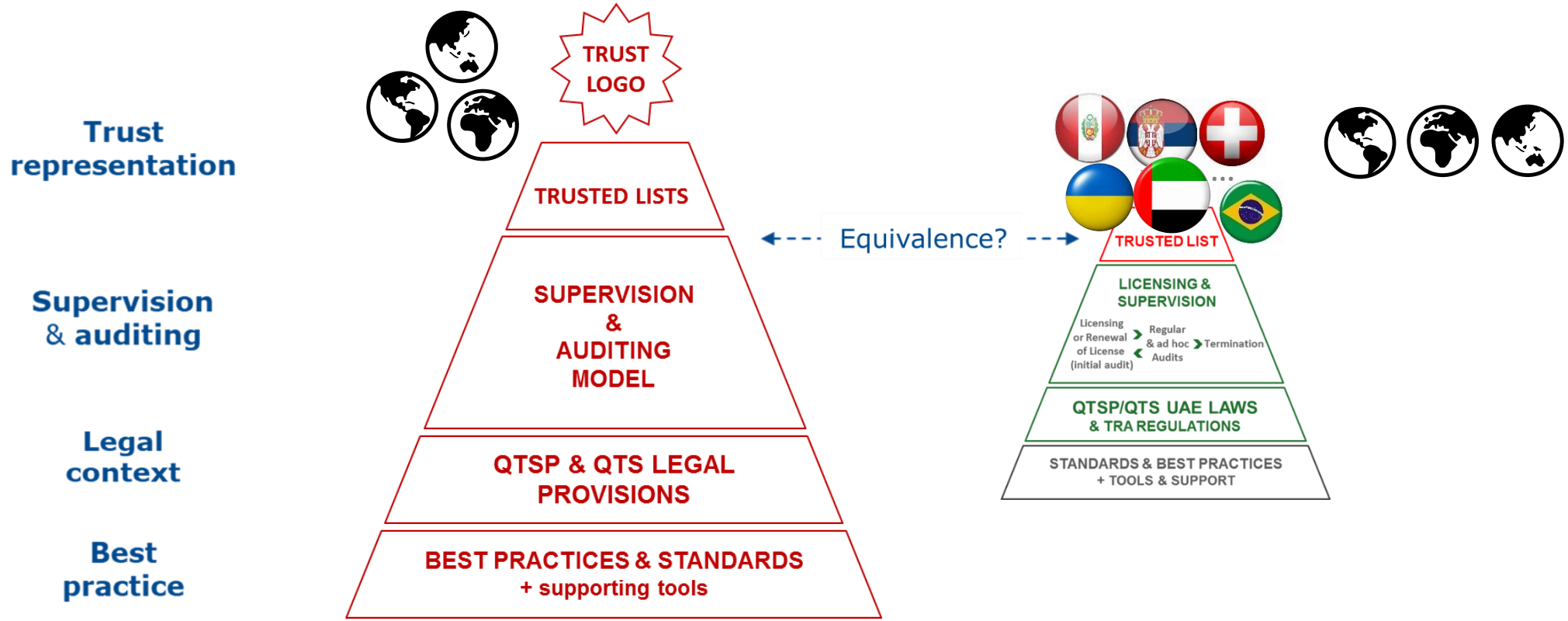
- Trade agreement
- QTS equivalence only
- Foreign TSP/TS must meet eIDAS QTSP/QTS requirements
- Reciprocity

Sources: ENISA, TRA presentation @ ETSI Dubai workshop (May 2019)

© ETSI 2021 – All rights reserved

Mutual recognition of electronic trust services

- Four-pillar methodology
  - in a view establishing a national / regional framework



© ETSI 2021 – All rights reserved

Sources: ENISA, TRA presentation @ ETSI Dubai workshop (May 2019)

Mutual recognition of electronic trust services

Legal context

Equivalence?

Facilitators / Benchmarks

- Regulatory vs contractual
- General principles
  - Non-discrimination against the use of electronic means
  - Technology neutrality

  (does not prevent being prescriptive with regards to a particular technology)
  - Functional equivalence, etc.
- Trust services, e.g.
  - Provision of certificates for signatures, seals or website/device
  - Creation / Preservation / Validation of electronic signatures / seals
  - Electronic time stamps; Electronic delivery services
  - Electronic archiving
- TSP/TS Levels of reliability
  - e.g. qualified vs non-qualified / licensed vs registered …

UNITED NATIONS COMMISSION ON INTERNATIONAL TRADE LAW

Working Group IV: Electronic Commerce

Use and Cross border Recognition of Identity Management and Trust Services

→ **Towards a Model Law in 2021 !**

eIDAS Regulation (EU) 910/2014

Benchmark/leading example

→ EU harmonisation

→ Secondary legislation pointing to electronic trust services reference standards not adopted (yet)

© ETSI 2021 – All rights reserved

Mutual recognition of electronic trust services

Legal context

Equivalence?

Facilitators / Benchmarks

- Obligations of TSPs
  - Liability & burden of proof,
  - Accessibility for persons with disabilities,
  - supervision/audits,
  - Correct operations,
  - Security risks management,
  - Security/Personal data breach notifications,
  - Personal Data protection,
  - Staff,
  - Operations changes and termination,
  - Insurances/Financial resources,
  - Data recording, …
- User obligations
- Recognition by public online services / private platforms
- International aspects (mutual recognition)

UNITED NATIONS COMMISSION ON INTERNATIONAL TRADE LAW

Working Group IV: Electronic Commerce

Use and Cross border Recognition of Identity Management and Trust Services

→ **Towards a Model Law in 2021 !**

eIDAS Regulation (EU) 910/2014

Benchmark/leading example

- → EU harmonisation
- → Secondary legislation pointing to electronic trust services reference standards not adopted (yet)

© ETSI 2021 – All rights reserved

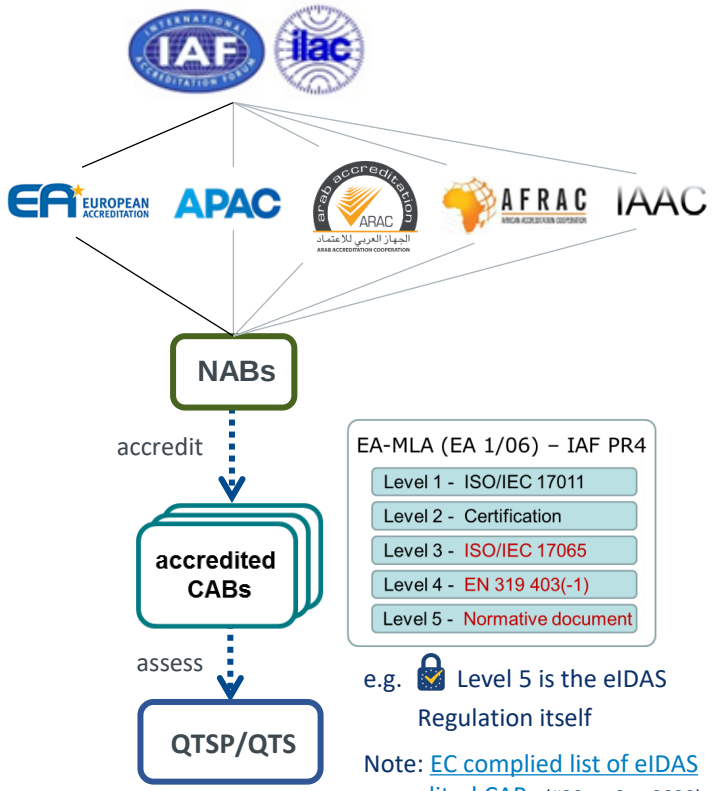
Mutual recognition of electronic trust services

Supervision & auditing

- Authorities approving (accrediting) auditing bodies
- Schemes to approve (accredit) auditing bodies
- Requirements on auditing bodies
  - Type of bodies
  - Conduct of assessment
  - Skills / competences
- Auditing (certification) scheme
- Assessment against what “normative document”
  - Regulation (legal requirements)
  - Technical standard
  - Mix
- Conformity assessment report
- Supervision decision
- Links into trust representation

Equivalence?

Facilitators / Benchmarks



© ETSI 2021 – All rights reserved

Mutual recognition of electronic trust services

Supervision & auditing

EA-MLA (EA 1/06) – IAF PR4

- Level 1 - ISO/IEC 17011
- Level 2 - Certification
- Level 3 - ISO/IEC 17065
- Level 4 - EN 319 403(-1)
- Level 5 - Normative document

Level 1: ISO/IEC 17011 "Conformity assessment — Requirements for accreditation bodies accrediting conformity assessment bodies"

- It specifies requirements for the competence, consistent operation and impartiality of accreditation bodies assessing and accrediting conformity assessment bodies

Level 2: Product Certification ***(including processes and services)***

- CABs needs to be certification bodies

Level 3: ISO/IEC 17065 "Conformity assessment — Requirements for bodies certifying products, processes and services"

- It specifies requirements relating to the competence, consistency of activities and impartiality of certification bodies for products, processes and services.

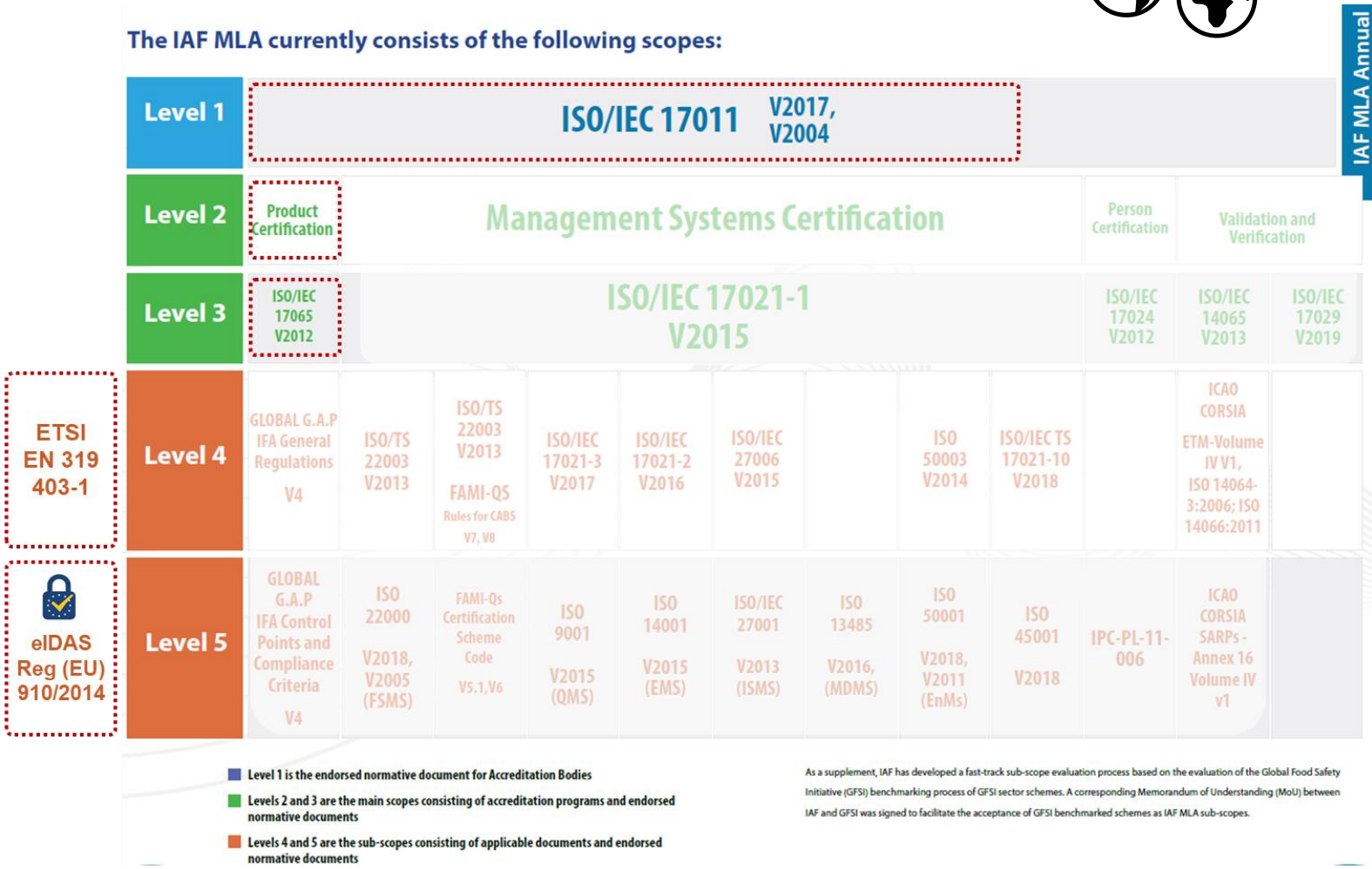
Level 4: ETSI EN 319 403-1 "Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers"

- It supplements ISO/IEC 17065 on requirements for certification bodies assessing trust service providers and the trust services they provide

Level 5: eIDAS Regulation (EU) 910/2014

- Normative document against which the trust service providers and the trust services they provide are certified compliant (i.e. eIDAS compliance)

Equivalence?



© ETSI 2021 – All rights reserved

Mutual recognition of electronic trust services

Supervision & auditing

Equivalence?

Facilitators / Benchmarks

- Promotion of the ISO/IEC 17065 / ETSI EN 319 403(-1) at the regional and global levels
  - Common existing framework for the recognition of certified evaluation of TSP/TS conformity against normative documents
    - Peer-review at the level of national accreditation bodies
    - "Certified once, accepted everywhere"
  - Normative documents may be
    - Regulatory documents (e.g. eIDAS Regulation)
    - Standards
    - Other types of (national, regional, industry) technical specifications
  - Available from (most) existing National Accreditation Bodies
  - Immediately available from most of the eIDAS accredited CABs

    (cf. EC compiled list of eIDAS accredited CABs)
  - Last milestones in context of mutual recognition
    - Equivalence of Normative documents' requirements for specific type of TSP/TS (Legal context & Best practices pillars)
    - Equivalence / Harmonisation of conformity assessment schemes (Best practices pillar)

© ETSI 2021 – All rights reserved

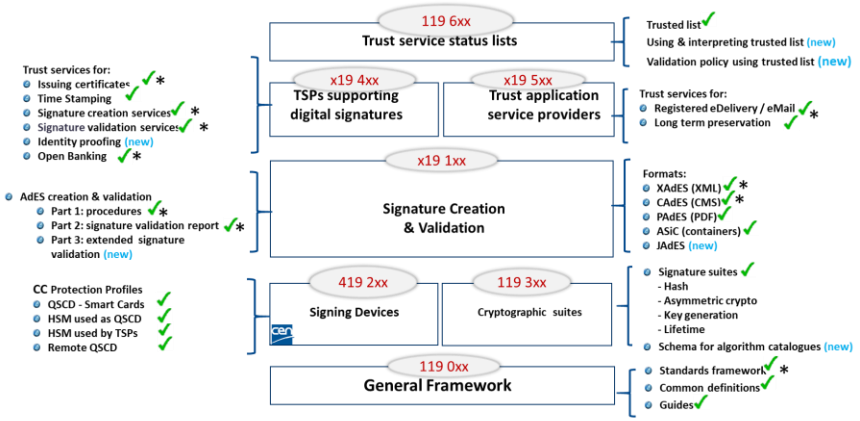
Mutual recognition of electronic trust services

Best practice

Equivalence?

Facilitators / Benchmarks

- Common technical basis makes easier mutual recognition
  - Best practices
  - Interoperability
  - Structuring of requirements
    - RFC 3647 for TSP issuing certificates
    - For other types of trust services ?
  - Mapping of technical requirements versus legal requirements, when "normative documents" are not standards but laws
  - ETSI standards for trust services
    - Truly "global" standards



ISO
CENELEC
ETSI
WebTrust
CAB CA/BROWSER FORUM
IETF
OASIS Open standards. Open source.
W3C
NIST National Institute of Standards and Technology
...

© ETSI 2021 – All rights reserved

Mutual recognition of electronic trust services

Trust representation

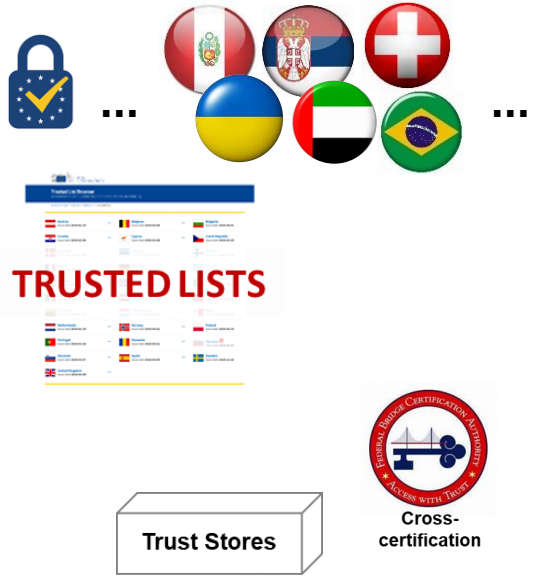
Equivalence?

Facilitators / Benchmarks

- Different models for representing trust
  - Trusted lists
  - Trust anchor stores
  - Bridging /cross-certification
- Easy to technically map between different trust representations but only meaningful when mapping other pillars

→ Trusted list is a key instrument when seeking MR with EU

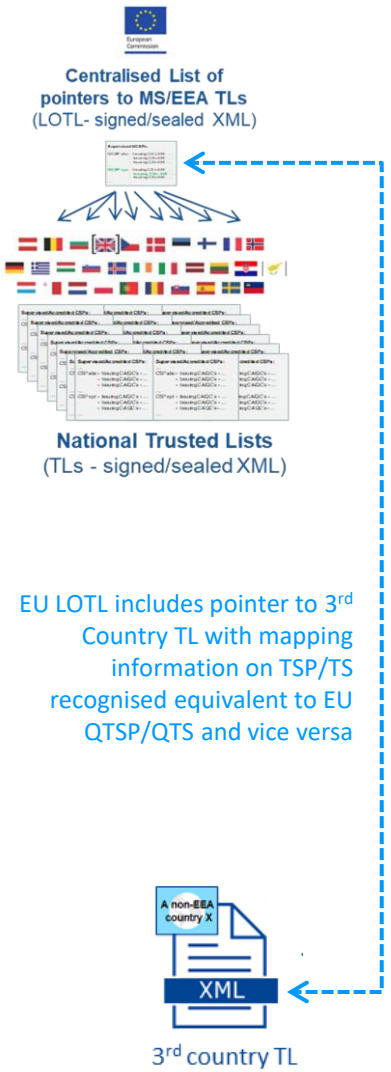
(cf. CEF Pilot for the International Compatibility of Trust Services)



© ETSI 2021 – All rights reserved

CEF Pilot for the International Compatibility of Trust Services

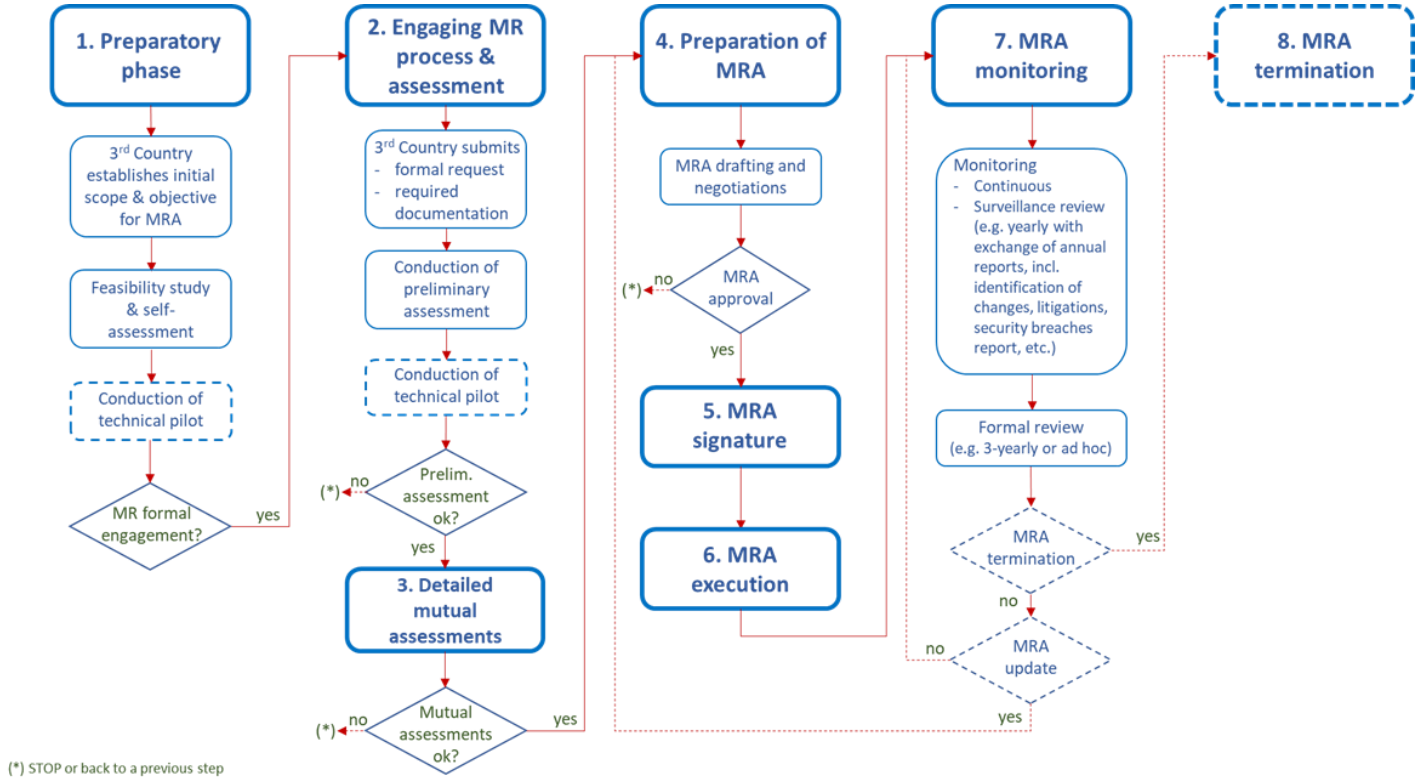
- A **generic model** to ensure 3rd Country TL compatibility with EU TLs under eIDAS *(applicable to any 3rd Country)*
- Builds upon the four-pillar equivalence assessment model of ETSI TR 103 684, focussing on technical aspects:
  - **Cookbook** with requirements for 3rd countries' alignment with EU TLs
  - **eIDAS Article 14 (self) Assessment Check-List** presenting a structured approach covering the four pillars (legal context, supervision and auditing, best practice, trust representation) for 3rd countries to perform a self-assessment on eIDAS compliance
  - **MRA element specification** (and XML Schema Definition), i.e. a "Pointer to other TSLs" including a MRAinfo element for:
    - Mapping expression of what 3rd country TS is recognised equivalent to what EU QTS and what means are respectively used to grant/withdraw approval/qualified status
    - Historical information about such recognition of equivalence
  - **MRA element usage description** incl. the necessary adaptation of standards (ETSI TS 119 615) for the validation of 3rd country electronic signatures/seals based on the content of the EU LOTL pointing to the 3rd country TL
- Toolbox for technical pilots
  - LOTL with pointer to 3rd Country TL mapping the 3rd Country TSP/TS trust anchors candidate for mutual recognition
  - Technical specifications and PKI-based samples
  - TL Manager & TL Browser for non-EU countries
  - Validation tool
- **Starting point** towards mutual recognition with EU on QTSP/QTS
  - Needs to be coupled with a legal assessment



© ETSI 2021 – All rights reserved

eIDAS Art.14 International recognition

- Conclusion of a mutual recognition agreement (MRA) under Art.14 of eIDAS can be a long journey
  - Requires a Trade agreement with the Union in accordance with Article 218 TFEU
  - Eligibility of 3rd country / international organization (IO) is not automatic
  - Scope of recognition (currently) limited to eIDAS closed list of 9 types of QTS
  - 3rd country TSP/TS must meet the eIDAS Regulation requirements applicable to EU QTSP/QTS
  - Requires equivalence of 3rd country/IO candidate TSP/TS approval/supervision (including audit) system with EU QTSP/QTS supervision (including audit) system
  - A typical eIDAS Art.14 MRA life-cycle process flow



(source: CEF Pilot for the International Compatibility of Trust Services)

© ETSI 2021 – All rights reserved

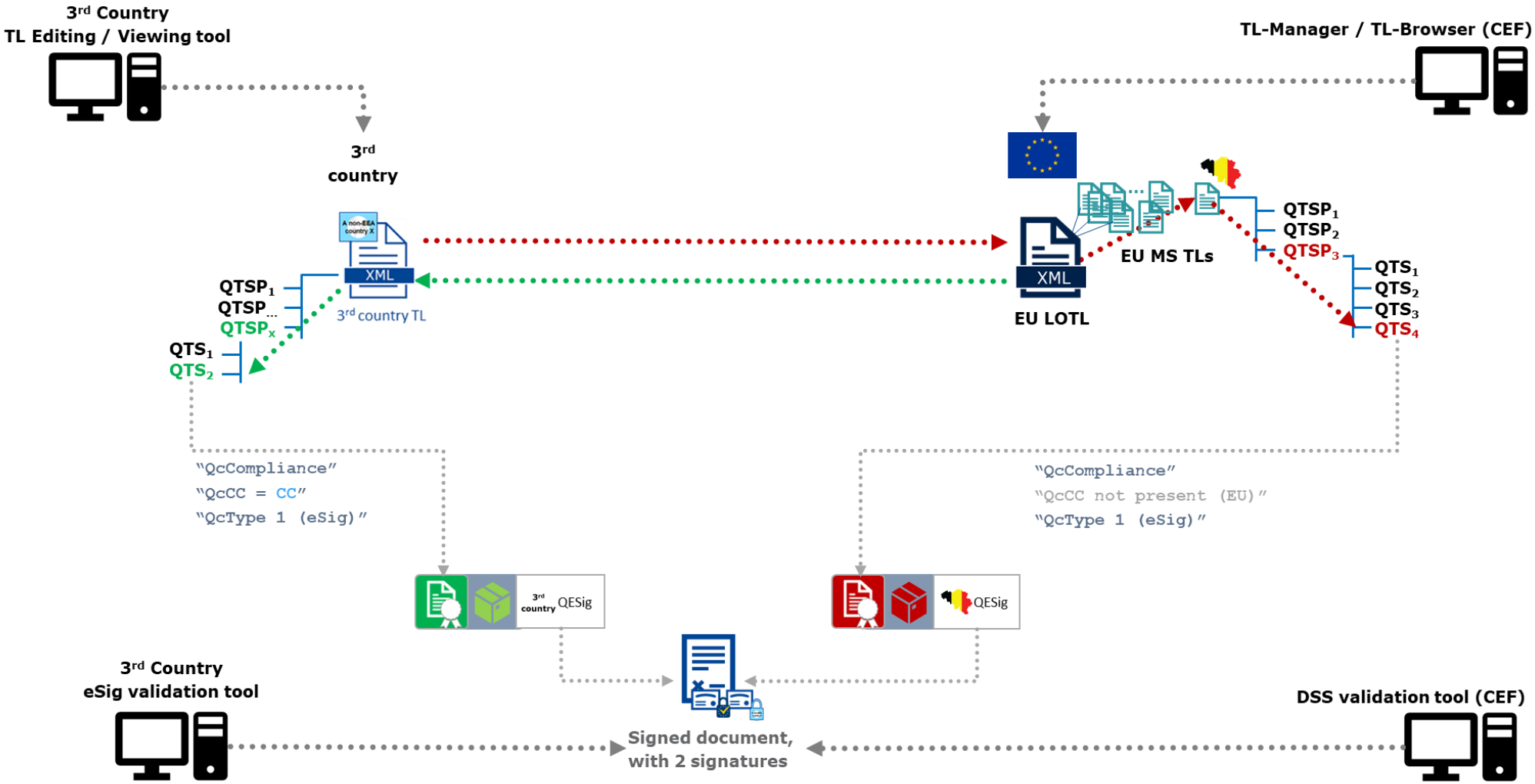
CEF Pilot for the International Compatibility of Trust Services

- **Requirements** *(source: CEF Pilot for the International Compatibility of Trust Services)*
  - 3rd country TSP/TS must meet the eIDAS Regulation requirements applicable to EU QTSP/QTS
  - To be recognised as **QSigCD** (resp. QSealCD), a device (EU or non-EU) must meet the requirements of eIDAS Annex II and be certified in accordance with Art.30 and CID (EU) 2016/650 by a certification body designated by an EU Member State
    - nonEU devices may be certified (+/- 10% today), nonEU bodies might be designated by EU Member States
  - 3rd country to establish and maintain a **trusted list** in accordance with ETSI TS 119 612 and the requirements and recommendations provided in the MRA Cookbook for listing at the least TSP/TS recognised as legally equivalent to EU QTSP/QTS
  - Requirements on use of ETSI defined “QcCompliance”, “QcType” and “QcCClegislation” statements and (optional) ‘Service information extension’ (‘Sie’) ‘Qualification’ extension (‘Sie:Q’) and of the corresponding qualifiers
  - The ETSI defined “QcSSCD” statement (id-etsi-qcs 4) shall not be used by QTSPs established in a 3rd country to declare that the private key related to the certified public key resides in a device that is not an EU-QSCD
  - Requirement on field values for the 3rd country TL with regards to the trust service entries for which an equivalence to EU QTS is expected
    - cf Table 3 of section 3.2.1 of the Cookbook
  - Use in 3rd Country TL of the MRA information element in an MRA pointer to the LOTL

+ a set of **key technical assumptions** and **recommendations** (mostly building upon ETSI satndards)

© ETSI 2021 – All rights reserved

Implementation of the CEF demonstrating technical pilot



© ETSI 2021 – All rights reserved

(source: CEF Pilot for the International Compatibility of Trust Services)

Mutual recognition of electronic trust services
Conclusion

- Facilitators / Benchmarks for paving the way towards an Regional/International framework for electronic trust services:
  - **Legal & Regulatory**, e.g.
    - UNCITRAL Model Law on provisions on the Cross Border recognition of Identity Management and Trust Services
    - EU eIDAS Regulation … benefiting from lessons learned (e.g. importance of secondary legislation for more balance between functional and technical specifications)
  - **Supervision & auditing**
    - Promotion of ISO/IEC 17065 & EN 319 403(-1) at regional and IAF levels

  - **Best practices**
    - Common technical basis (standards) makes easier mutual recognition (e.g. latest versions of CEN CENELEC & ETSI standards)
  - **Trust representation**
    - Trusted lists
- Starting point for MRA with EU → CEF Pilot for the International Compatibility of Trust Services

© ETSI 2021 – All rights reserved