ETSI Study on Globalisation of Trust

Presented by: **Olivier DELOS**   For: **Tokyo Workshop on Globalisation of Trust Services**

23.05.2019

Agenda

- ➢ Background
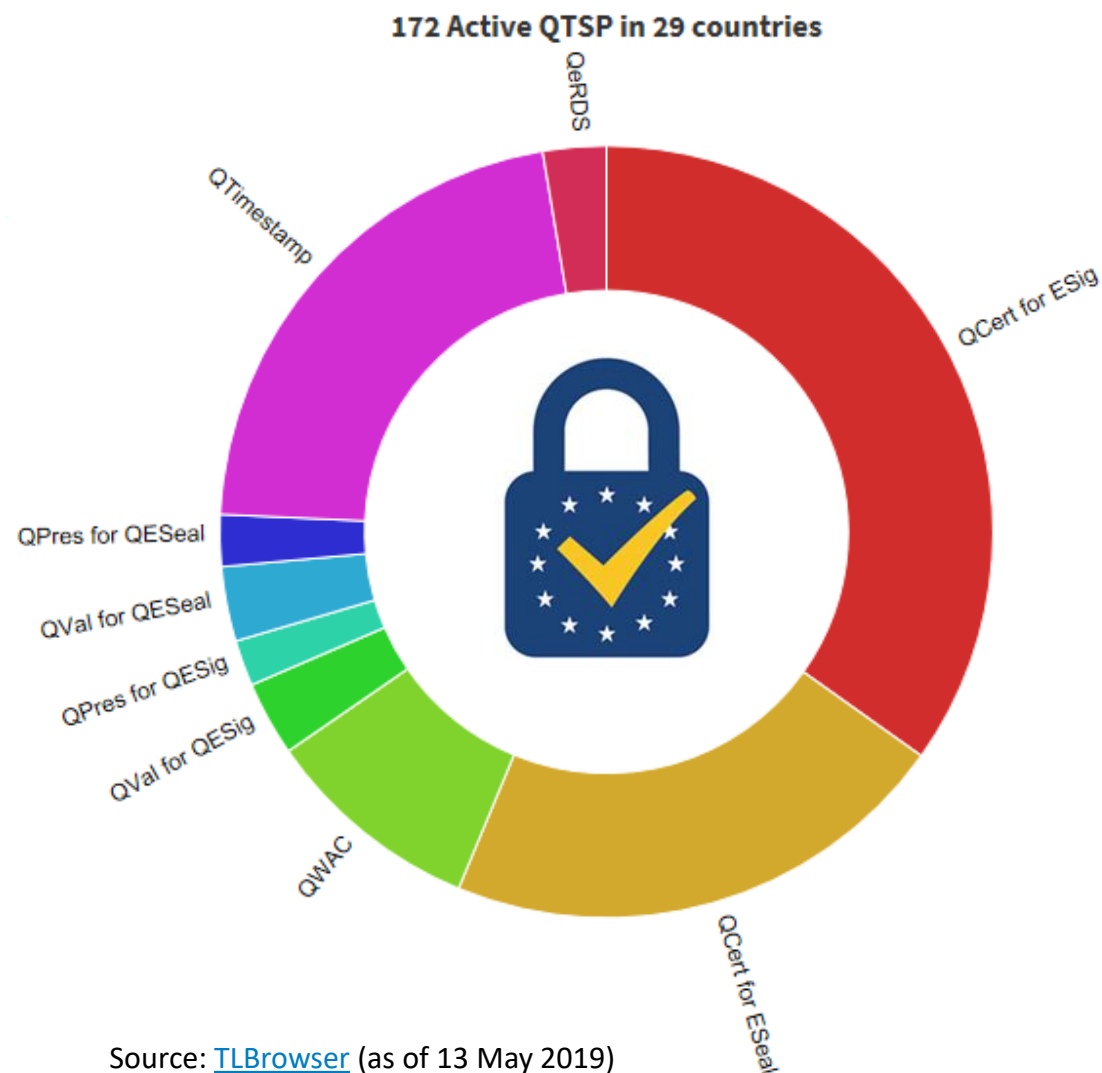
- ➢ Study Aims

- ➢ Methodology

- ➢ Final points

Background EU Trust Services

eIDAS EU Regulation 910/2014

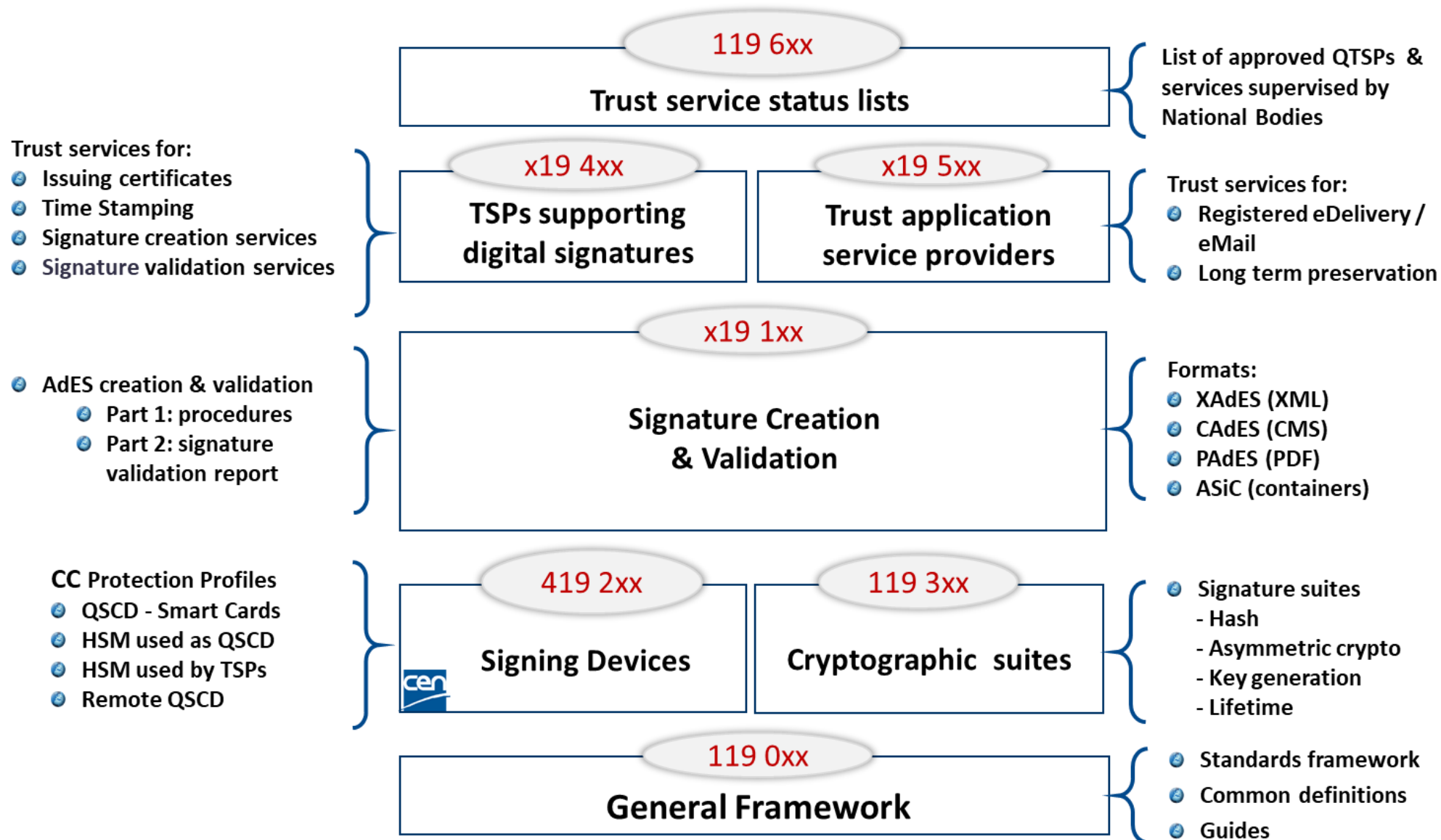➢ Establishes legal framework for (qualified) trust services in the EU

ETSI TC Electronic Signatures and Infrastructures (ESI)
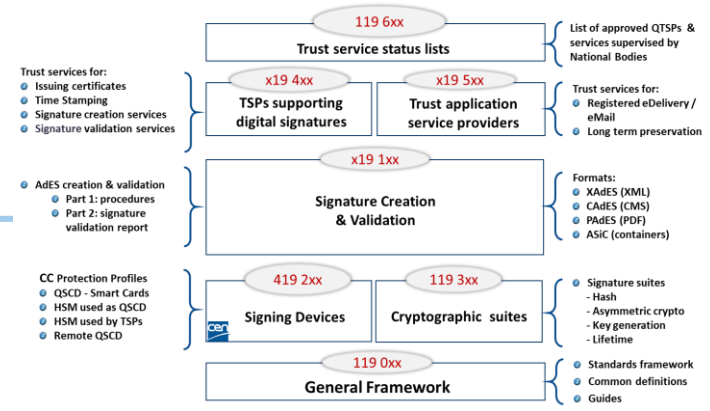
➢ Defines standards for trust services

172 Active QTSP in 29 countries

Source: TLBrowser (as of 13 May 2019)

ETSI Standards for Trust Services

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

119 6xx
Trust service status lists

List of approved QTSPs & services supervised by National Bodies

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

x19 1xx
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

119 3xx
Cryptographic suites

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

119 0xx
General Framework

- Standards framework
- Common definitions
- Guides

4

ETSI Standards for Trust Services

Examples:

➢ Conformity assessment:

➢ EN 319 403: Requirements for conformity assessment bodies assessing Trust Service Providers

(supplements ISO/IEC 17065:2012 Conformity assessment – Requirements for bodies certifying products, processes and services)

➢ TS 119 403-3: Additional requirements for conformity assessment bodies assessing EU qualified trust service providers

(e.g. requirements on conformity assessment reports)

ETSI Standards for Trust Services
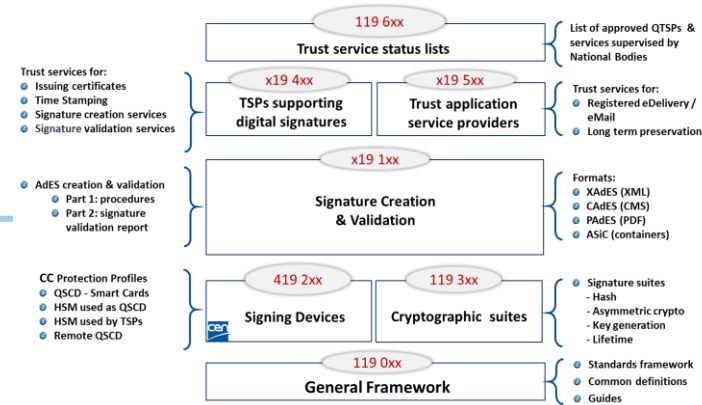
Examples:

➢ Trust Service Providers (TSPs) issuing certificates

   ➢ EN 319 401: Policy requirements for TSPs

   ➢ EN 319 411:

      ➢ Part 1: Policy requirements for TSPs issuing certificates

      ➢ Part 2: Policy requirements for TSPs issuing EU qualified certificates

   ➢ EN 319 412 series (certificate profiles)

➢ TS 119 612: Trusted list of TSPs & Trust Services

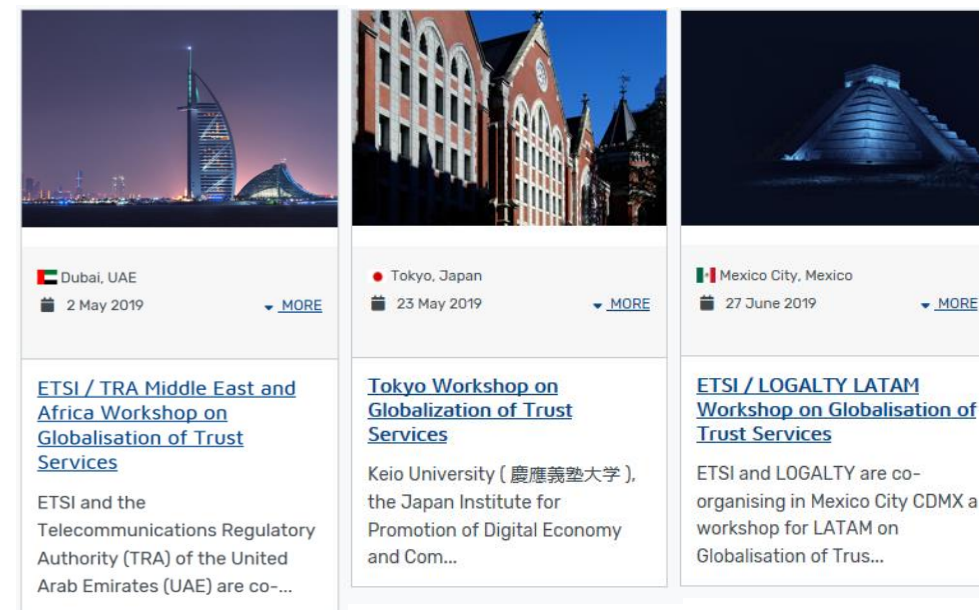# Known Examples of Adoption of ETSI Standards Worldwide

➢ CA/Browser Forum recognises EN 319 403 audit and EN 319 411-1 policy requirements in its guidelines

➢ Japan standards for trust services based on ETSI standards

➢ Several South American countries adopt controls similar or equivalent to ETSI Standards

➢ Some African and Middle Eastern countries have adopted ETSI standards (either at TSP level or at secondary legislation level)

➢ Swiss regulations reference EN 319 411-2 and EN 319 412 series

➢ SAFE-BioPharma equivalence mapping to EN 319 411-1/2

➢ TS 119 612-based Trusted Lists are used on 4 continents …

STF 560 Study Aims

➢ **Investigate PKI-based trust service schemes and their trust model around the world**

  ➢ Questionnaire

  ➢ Desktop research

  ➢ Regional Workshops:
    ➢ Middle East and Africa (02 May – Dubai)
    ➢ Asia (23 May – Tokyo)
    ➢ Central & South America (27 June – Mexico)
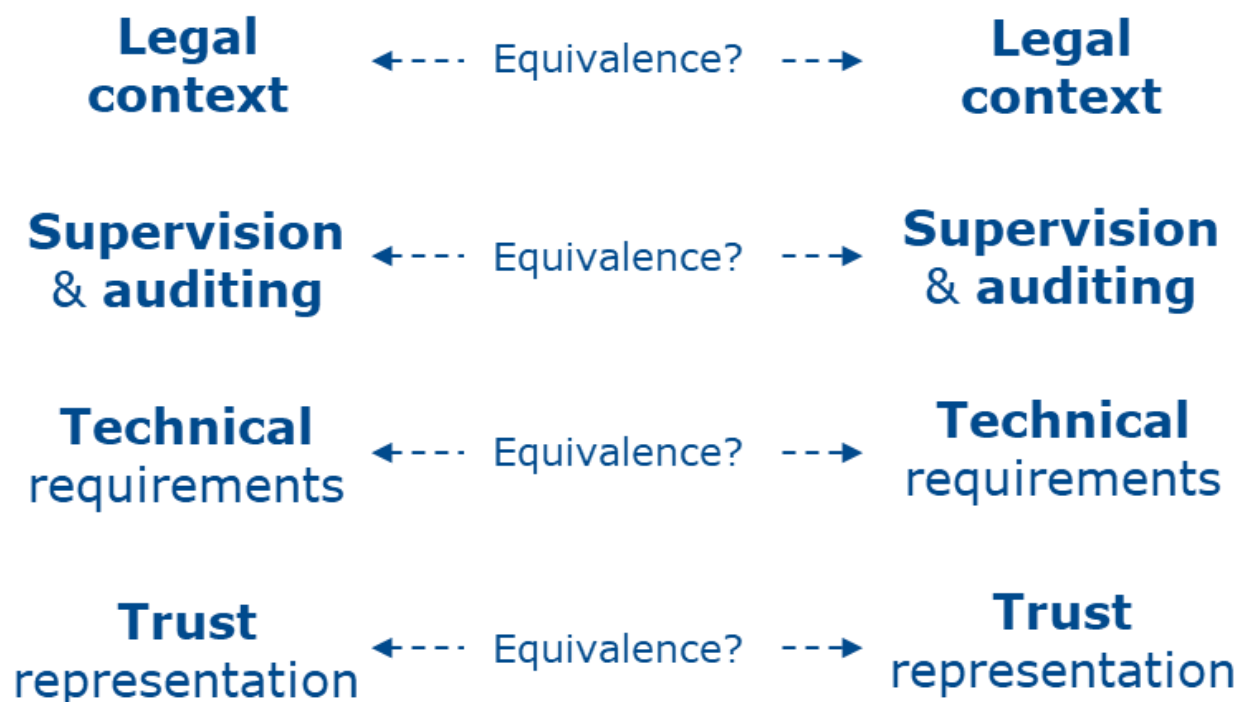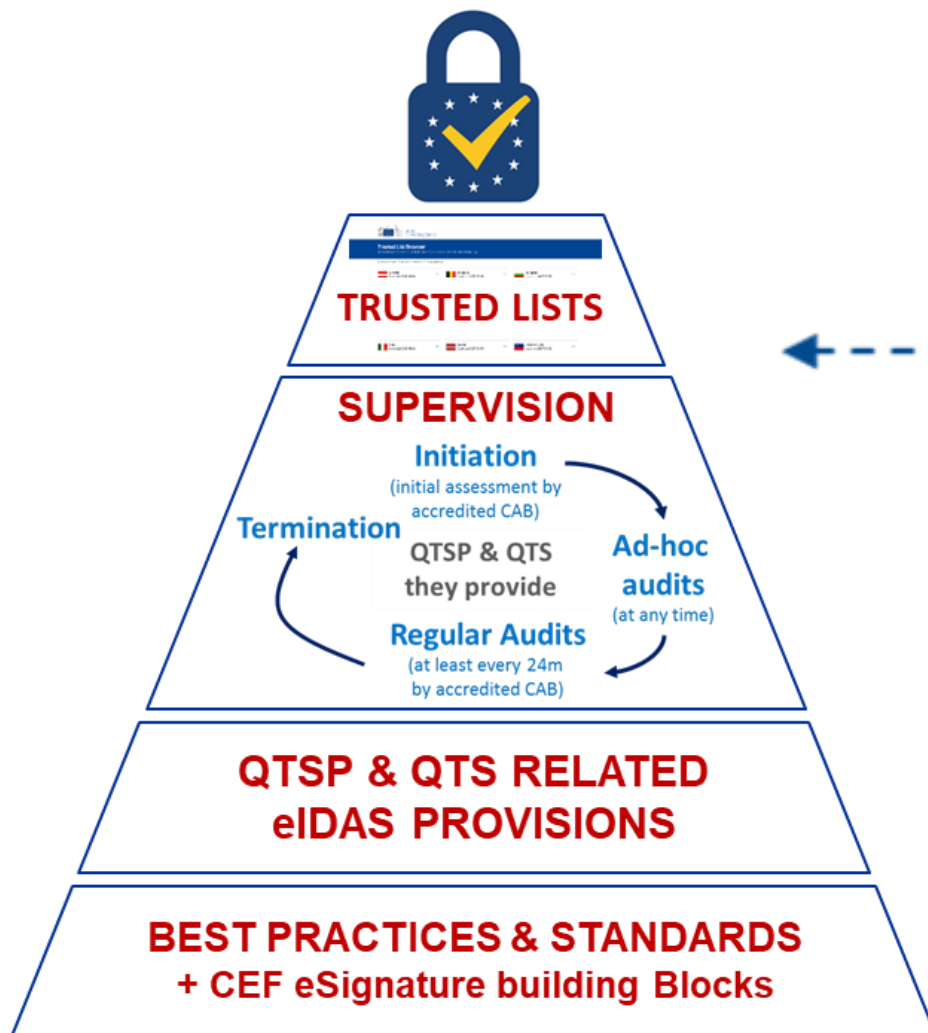
➢ **Identify technical basis for mutual recognition**

  ➢ Incl. model, barriers, solutions

Dubai, UAE
2 May 2019   ▾ MORE

ETSI / TRA Middle East and Africa Workshop on Globalisation of Trust Services

ETSI and the Telecommunications Regulatory Authority (TRA) of the United Arab Emirates (UAE) are co-

Tokyo, Japan
23 May 2019   ▾ MORE

Tokyo Workshop on Globalization of Trust Services

Keio University (慶應義塾大学), the Japan Institute for Promotion of Digital Economy and Com...

Mexico City, Mexico
27 June 2019   ▾ MORE

ETSI / LOGALTY LATAM Workshop on Globalisation of Trust Services

ETSI and LOGALTY are co-organising in Mexico City CDMX a workshop for LATAM on Globalisation of Trus...
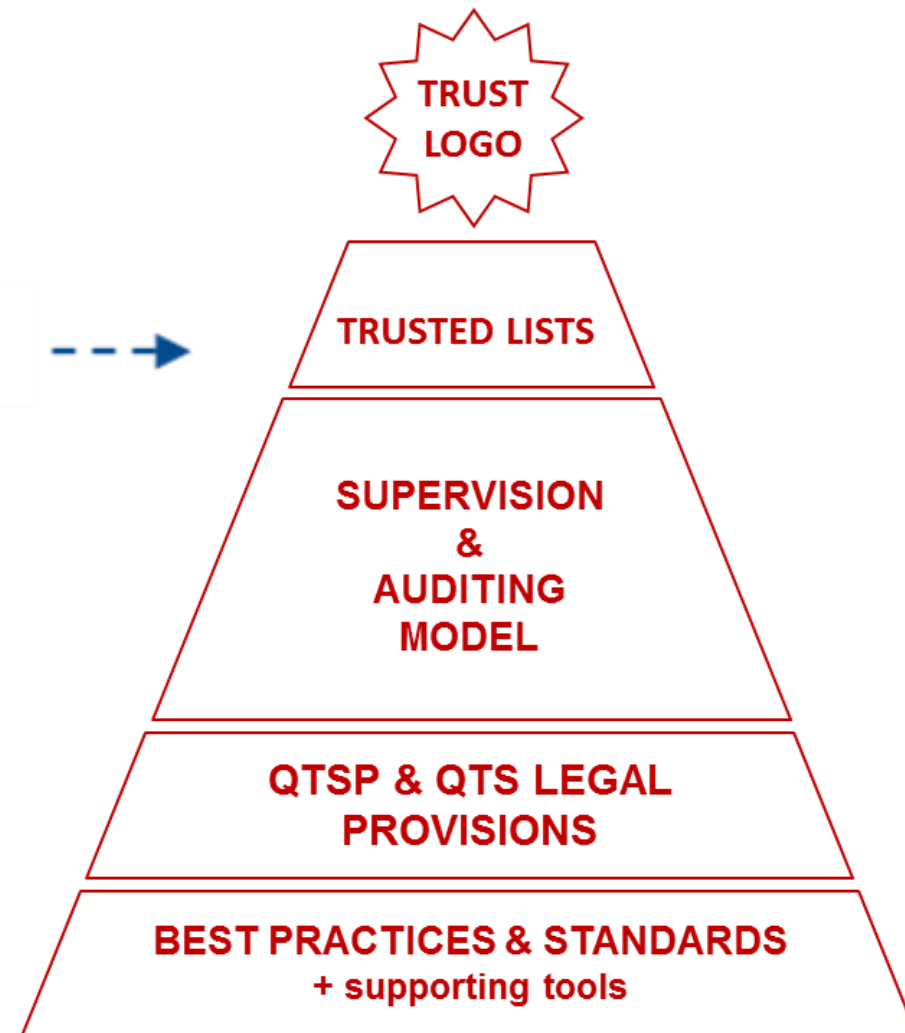
Methodology

Main pillars for comparing PKI-based trust service schemes

(e.g. in a view of establishing recognition)

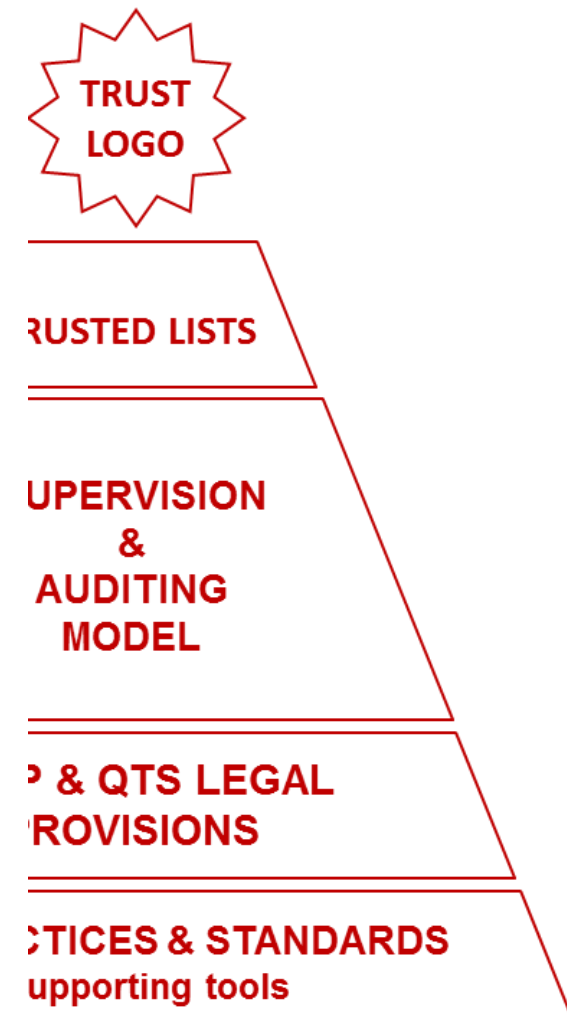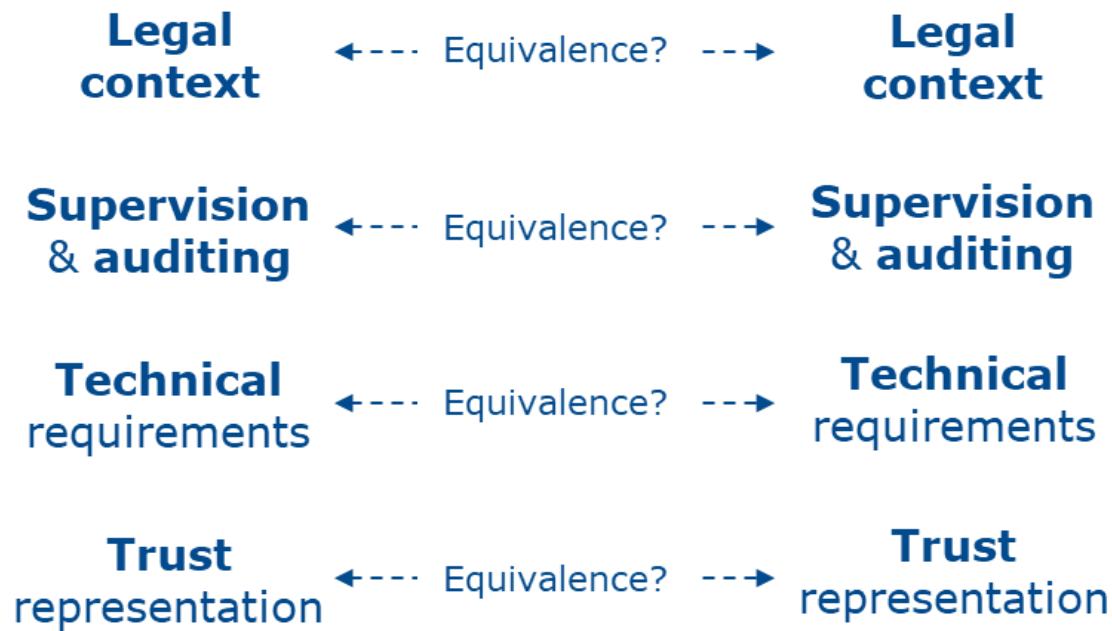| Legal context | ←--- Equivalence? ---→ | Legal context |
Supervision & auditing	←--- Equivalence? ---→	Supervision & auditing
Technical requirements	←--- Equivalence? ---→	Technical requirements
Trust representation	←--- Equivalence? ---→	Trust representation

Methodology
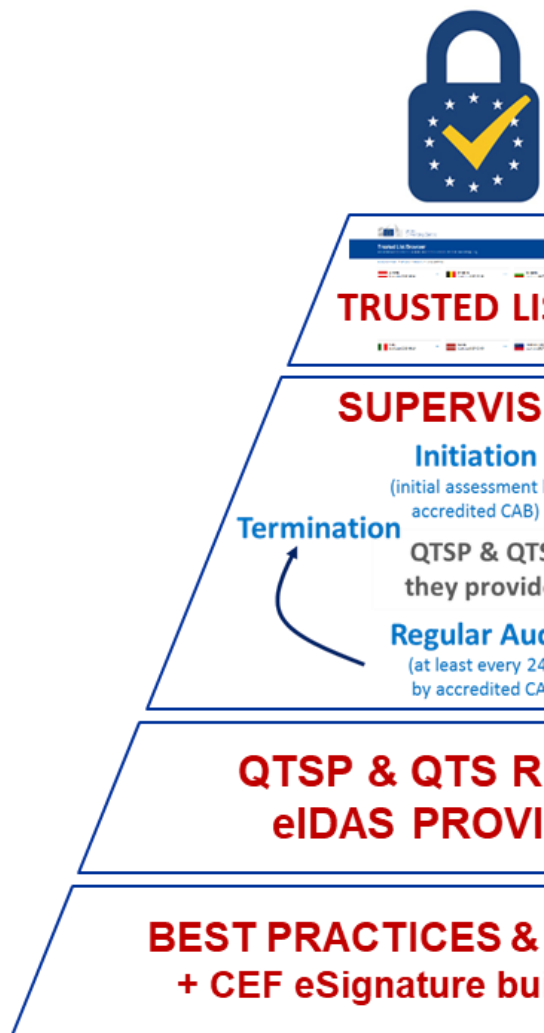

Equivalence?

Methodology

Main pillars for comparing PKI-based trust service schemes
(e.g. in a view of establishing recognition)

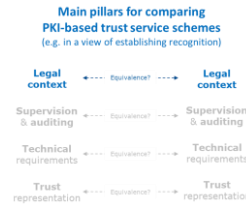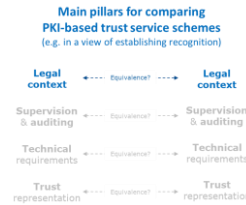|		
Legal context	←--- Equivalence? ---→	**Legal context**
Supervision & auditing	←--- Equivalence? ---→	**Supervision & auditing**
Technical requirements	←--- Equivalence? ---→	**Technical** requirements
Trust representation	←--- Equivalence? ---→	**Trust** representation

Left pyramid (blue/red):
- TRUSTED LI[STS]
- SUPERVIS[ION]
  - Initiation (initial assessment [by] accredited CAB)
  - Termination — QTSP & QTS[...] they provid[e]
  - Regular Aud[it] (at least every 24[...] by accredited CA[B])
- QTSP & QTS R[...] eIDAS PROVI[...]
- BEST PRACTICES & [...] + CEF eSignature bu[...]

Right pyramid (red):
- TRUST LOGO
- [T]RUSTED LISTS
- [S]UPERVISION & [A]UDITING MODEL
- [QTS]P & QTS LEGAL [P]ROVISIONS
- [PRA]CTICES & STANDARDS [s]upporting tools

Methodology

Legal context ← - - - Equivalence? - - - → **Legal context**

- ➢ 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. Creation / Preservation / Validation of electronic signatures / seals, of electronic time stamps, of electronic delivery services, of certificate for signatures, seals or website (device) authentication, of electronic documents, …
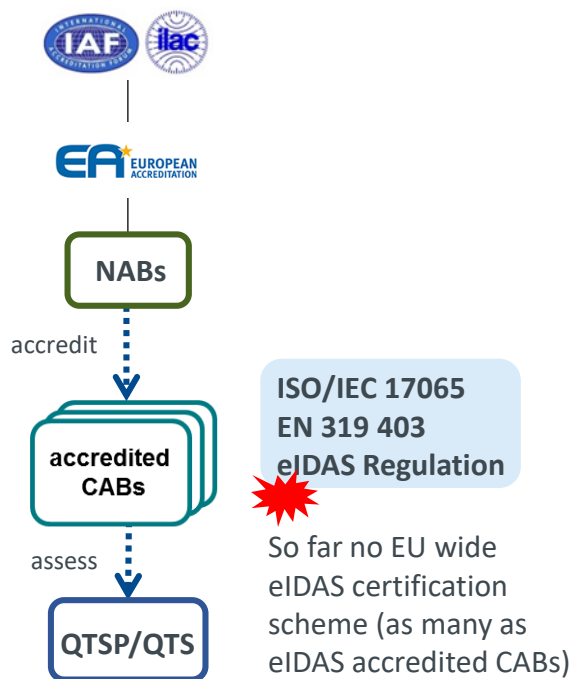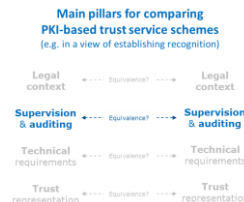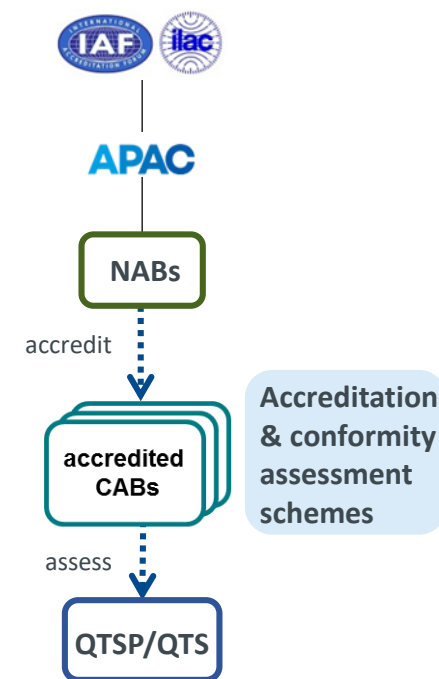
Methodology

…

- ➢ **TSP/TS Levels of reliability**
  - ➢ e.g. qualified vs non-qualified
- ➢ **Obligations of TSPs**
  - ➢ Liability & burden of proof, Accessibility for persons with disabilities, supervision/audits, Correct operations, Security risks management, Security/Personal data breach notifications, Data protection, Staff, Operations changes and termination, Insurances/Financial resources, Data recording, …
- ➢ **User obligations**
- ➢ **International aspects (mutual recognition)**

Methodology

Main pillars for comparing
PKI-based trust service schemes
(e.g. in a view of establishing recognition)

ETSI

Supervision & **auditing** ← - - Equivalence? - -→ **Supervision** & **auditing**   e.g.

- IAF / ilac
- EA EUROPEAN ACCREDITATION
- NABs
  - accredit
- accredited CABs
  - assess
- QTSP/QTS

**ISO/IEC 17065
EN 319 403
eIDAS Regulation**

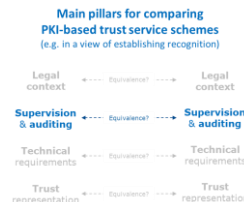So far no EU wide eIDAS certification scheme (as many as eIDAS accredited CABs)

- ➤ Authorities approving (accrediting) auditing bodies
- ➤ Auditing bodies approval (accreditation) scheme
- ➤ 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
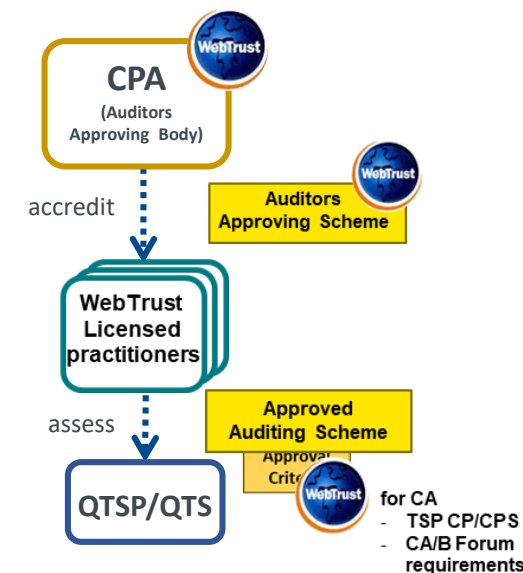- ➤ Supervision decision
- ➤ Links into trust representation

- IAF / ilac
- APAC
- NABs
  - accredit
- accredited CABs
  - assess
- QTSP/QTS

Accreditation & conformity assessment schemes

14

Methodology

Main pillars for comparing
PKI-based trust service schemes
(e.g. in a view of establishing recognition)

Supervision & **auditing** ← ---- Equivalence? --- → **Supervision** & **auditing**   **e.g.**

- ➤ Authorities approving (accrediting) auditing bodies
- ➤ Auditing bodies approval (accreditation) scheme
- ➤ 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
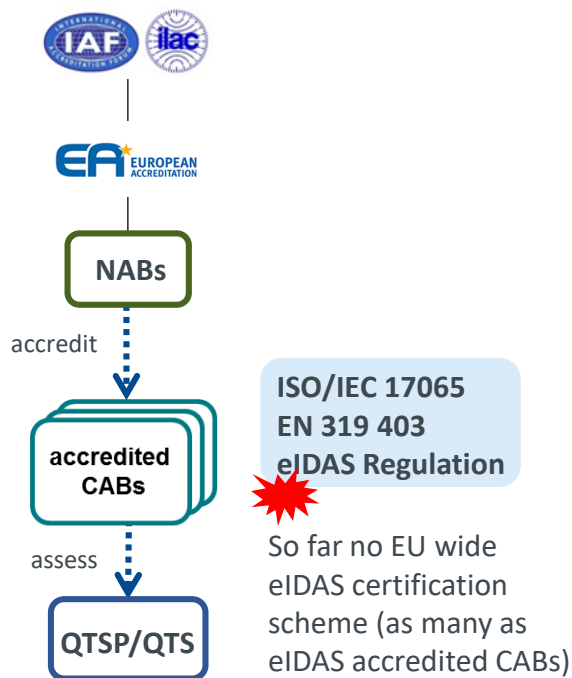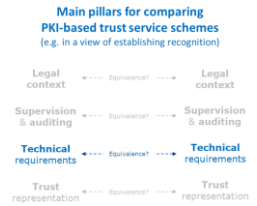- ➤ Supervision decision
- ➤ Links into trust representation

NABs

accredit

ISO/IEC 17065
EN 319 403
eIDAS Regulation

accredited CABs

assess

So far no EU wide eIDAS certification scheme (as many as eIDAS accredited CABs)

QTSP/QTS

CPA
(Auditors Approving Body)

accredit

Auditors Approving Scheme

WebTrust Licensed practitioners

assess

Approved Auditing Scheme

QTSP/QTS

for CA
- TSP CP/CPS
- CA/B Forum requirements

Methodology

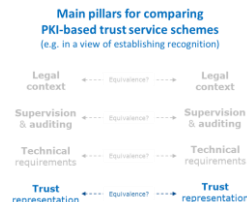Technical requirements ←--- Equivalence? --→ Technical requirements

e.g.

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

...

Methodology

Main pillars for comparing
PKI-based trust service schemes
(e.g. in a view of establishing recognition)

Trust representation ← ─ ┈ Equivalence? ┈ ─ → **Trust representation**

e.g.

TRUSTED LISTS

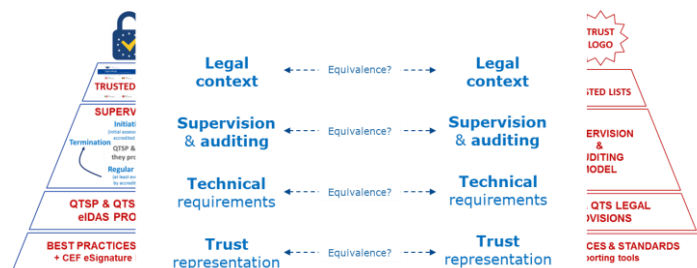➢ Different models for representing trust
  ➢ Trusted lists
  ➢ Trust anchor stores
  ➢ Bridging

➢ Easy to technically map between different trust representations but only meaningful when mapping other pillars

Trusted List

...

Cross-certification

Trust Stores

17

Final Points

➢ Study report due End 2019

    ➢ Investigate PKI-based trust service schemes and their trust model around the world

    ➢ Identify technical basis for mutual recognition

    ➢ Identify barriers & proposed solutions

➢ Please help by filling in our questionnaire:
https://docbox.etsi.org/ESI/Open/workshops/ETSIGlobalQuest.docx