# ETSI Study on Globalisation of Trust

Presented by:  **Olivier DELOS**

For:  **New York City - Workshop on Globalisation of Trust Services**

03.09.2019

# Agenda

➢ Background

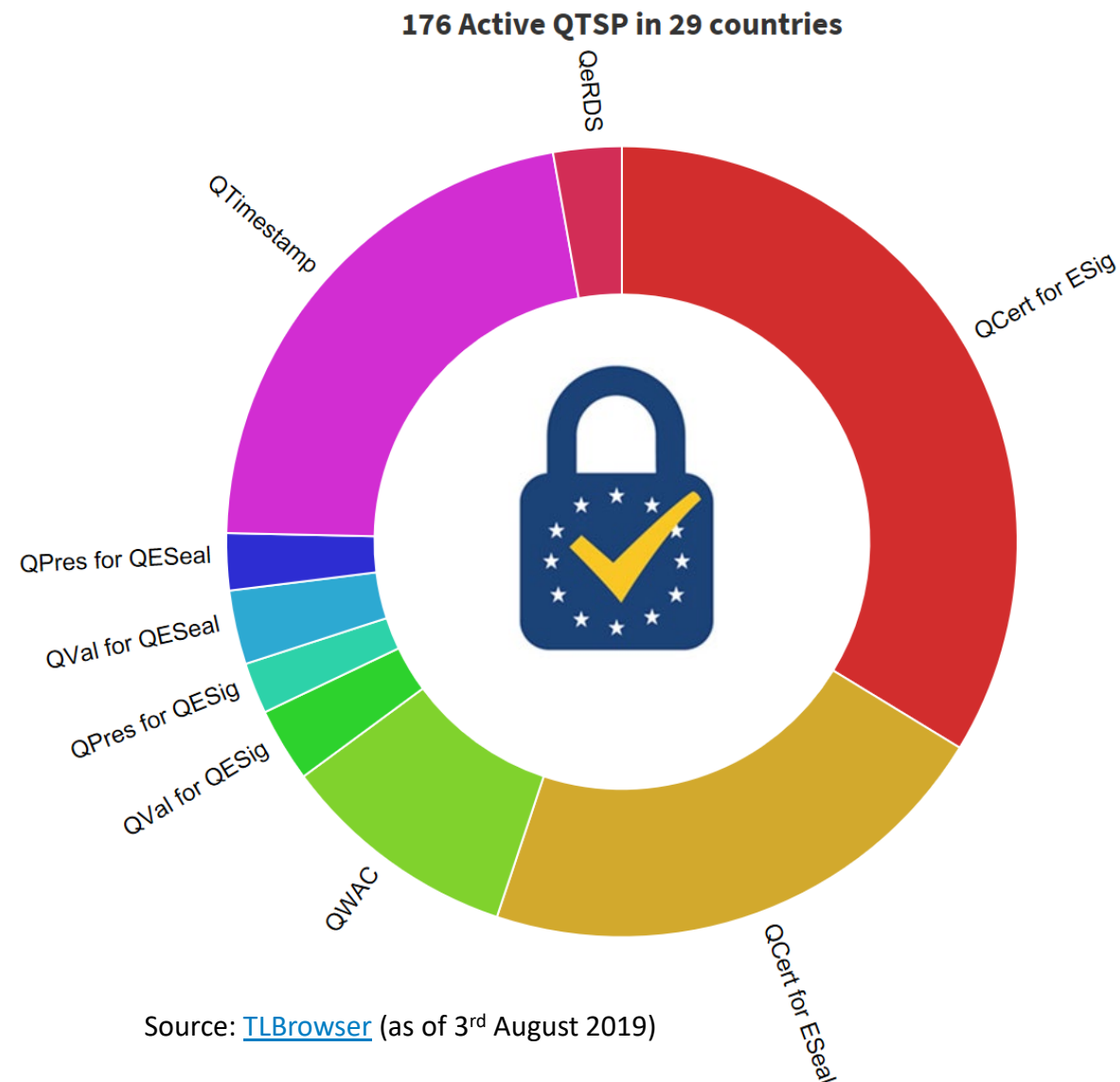➢ Study Aims

➢ 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)**
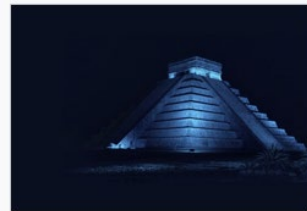
➢ Defines standards for trust services



**176 Active QTSP in 29 countries**

QeRDS
QTimestamp
QCert for ESig
QPres for QESeal
QVal for QESeal
QPres for QESig
QVal for QESig
QWAC
QCert for ESeal

Source: TLBrowser (as of 3rd August 2019)

# 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)
      ➢ North America (3 September - New York)

➢ ## 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…

🇺🇸 New York, US
📅 3 September 2019                    ▼ MORE

ETSI North America Workshop on Globalisation of Trust Services

ETSI is organizing a workshop on Globalisation of Trust Services for North American stakeholders, at…

# 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

Best practice ←--- Equivalence? ---→ Best practice

Trust representation ←--- Equivalence? ---→ Trust representation

# Methodology



**Main points for comparison between PKI-based trust service schemes**
(for each of the four pillars)

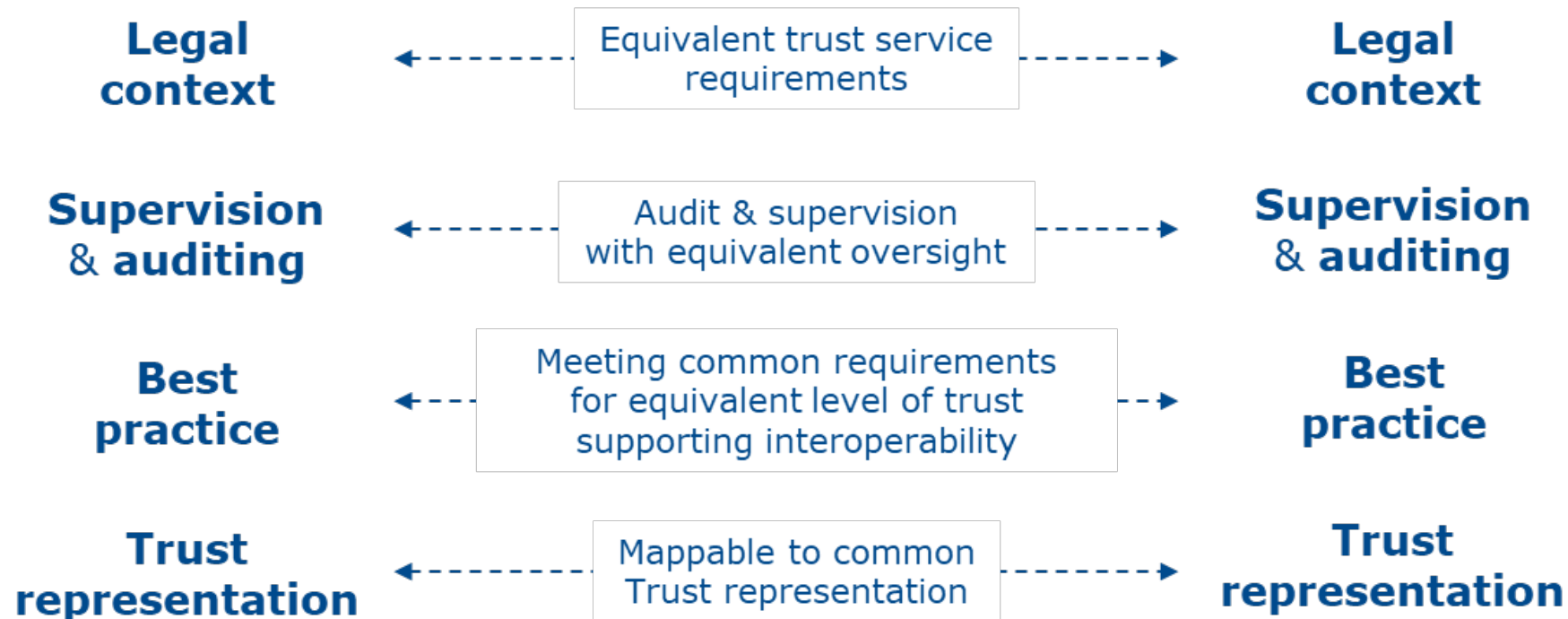| Legal context | ← Equivalent trust service requirements → | Legal context |
| Supervision & auditing | ← Audit & supervision with equivalent oversight → | Supervision & auditing |
| Best practice | ← Meeting common requirements for equivalent level of trust supporting interoperability → | Best practice |
| Trust representation | ← Mappable to common Trust representation → | Trust representation |

# Methodology

# 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 |
| Best practice | ← Equivalence? → | Best practice |
| Trust representation | ← Equivalence? → | Trust representation |

Left pyramid:
- TRUSTED LI
- SUPERVIS
  - Initiation (initial assessment accredited CAB)
  - Termination
  - QTSP & QTS they provid
  - Regular Aud (at least every 24 by accredited CA)
- QTSP & QTS R / eIDAS PROVI
- BEST PRACTICES & + CEF eSignature bu

Right pyramid:
- TRUST LOGO
- RUSTED LISTS
- UPERVISION & AUDITING MODEL
- P & QTS LEGAL PROVISIONS
- CTICES & STANDARDS upporting tools

# Methodology


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

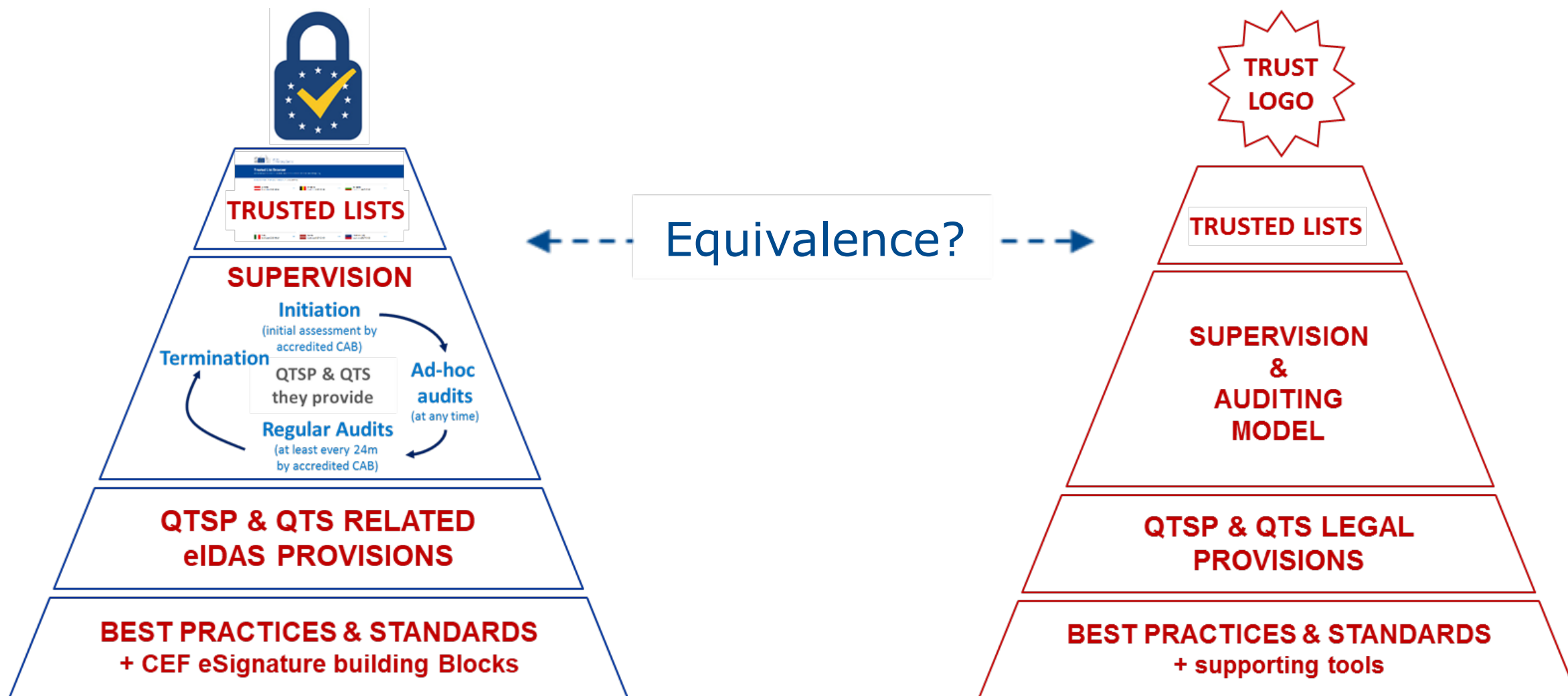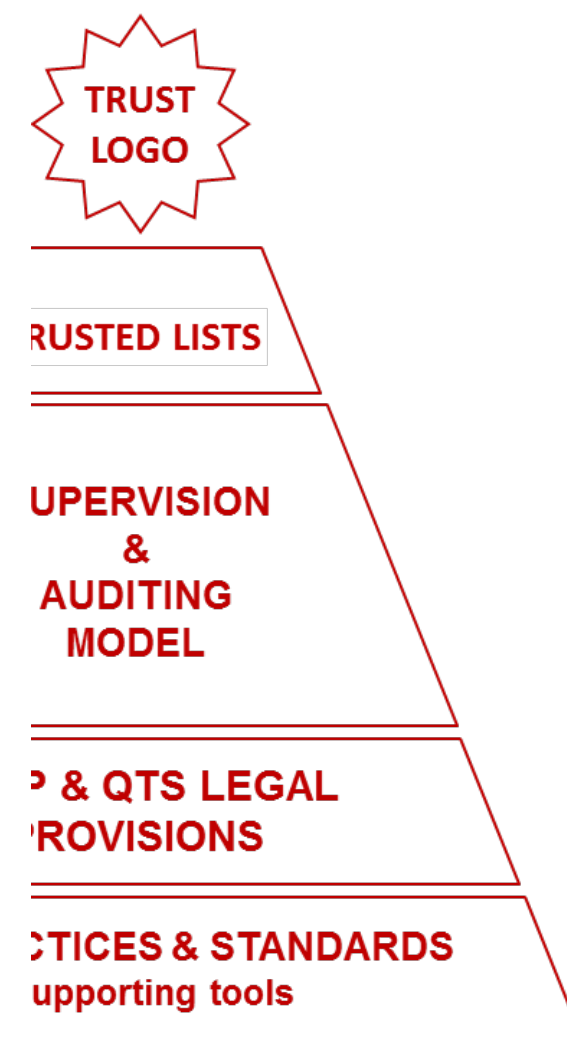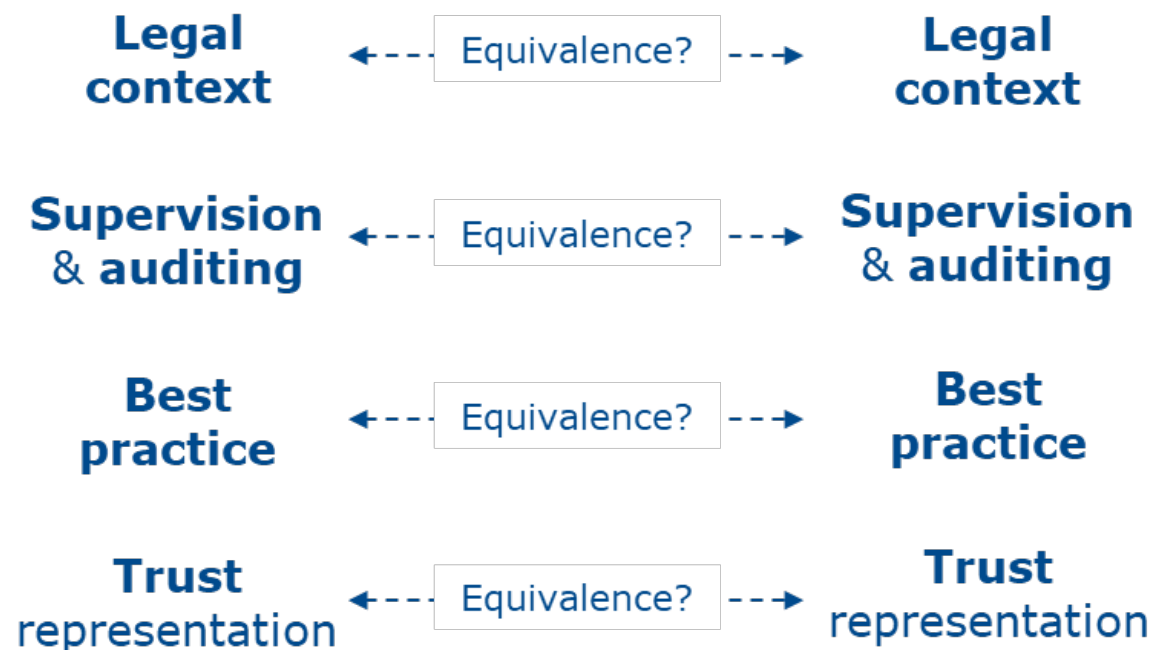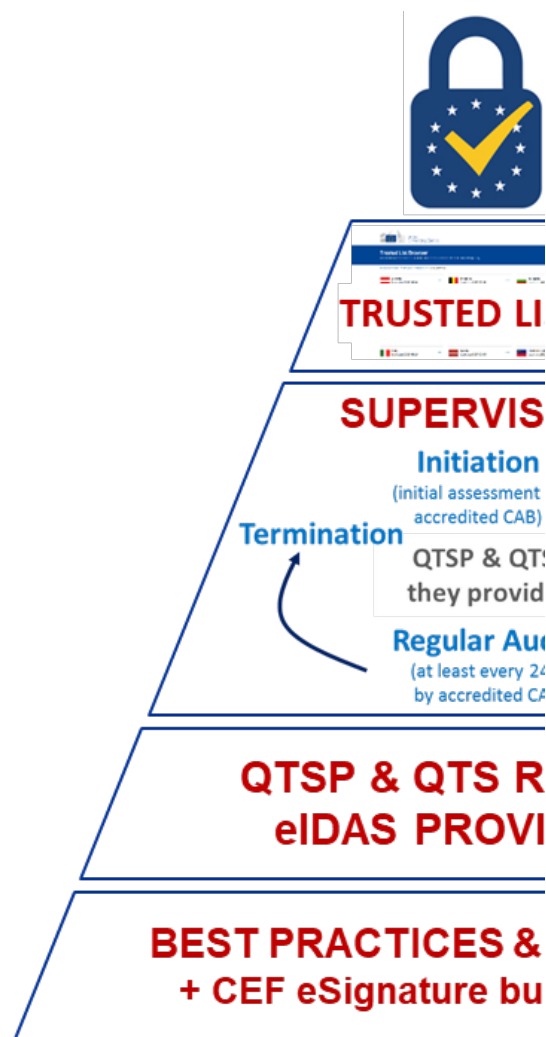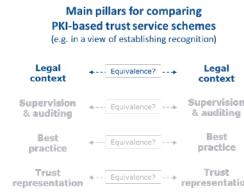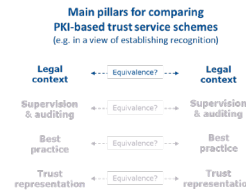**Legal context** ← - - - Equivalence? - - → **Legal context**

- ➢ Regulatory vs Agreement-based
- ➢ 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

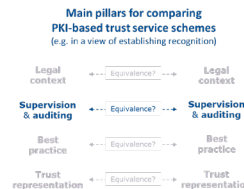Main pillars for comparing
PKI-based trust service schemes
(e.g. in a view of establishing recognition)

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

…

➢ 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
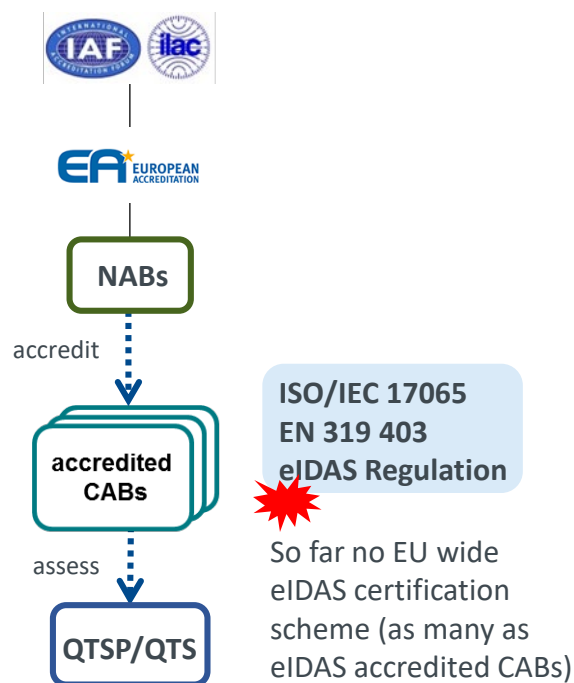
**Main pillars for comparing
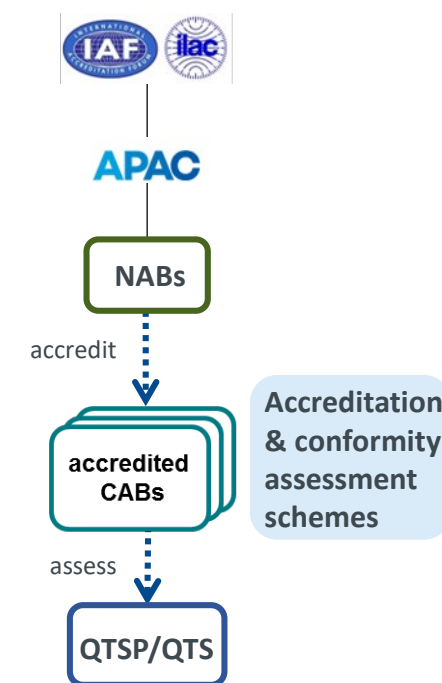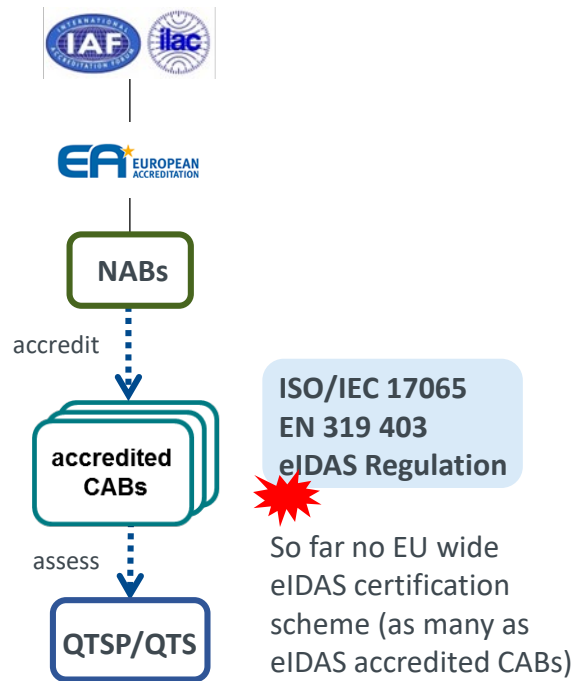PKI-based trust service schemes**
(e.g. in a view of establishing recognition)
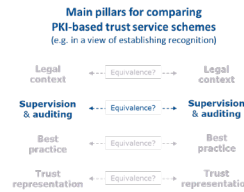
**Supervision** & **auditing** ←--- Equivalence? ---→ **Supervision** & **auditing**

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

accredited CABs

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

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

assess

QTSP/QTS

NABs

accredit

accredited CABs

**Accreditation & conformity assessment schemes**

assess

QTSP/QTS

11

# 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

Best practice ← Equivalence? → Best practice

Trust representation ← Equivalence? → Trust representation

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

NABs

accredit

accredited CABs

ISO/IEC 17065
EN 319 403
eIDAS Regulation

assess

QTSP/QTS

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
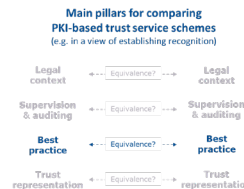
➤ Links into trust representation

**CPA**
(Auditors Approving Body)

accredit

**Auditors Approving Scheme**

**WebTrust Licensed practitioners**

assess

**Approved Auditing Scheme**
Approval Criteria

QTSP/QTS

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

# Methodology

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

**Best practice** ← - - Equivalence? - -→ **Best practice**     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



Trust representation ← - - - Equivalence? - - → Trust representation
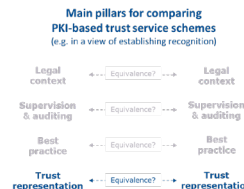
➢ **Different models for representing trust**
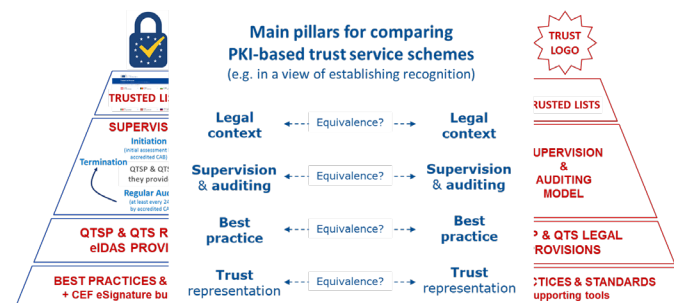  ➢ Trusted lists
  ➢ Trust anchor stores
  ➢ Bridging

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

**TRUSTED LISTS**

**e.g.**

Trusted List

Cross-certification

Trust Stores

# Hints on preliminary results

➢ **Legal context**

   ➢ Regulatory vs Agreement-based … two different worlds, with (difficult) interactions

   ➢ Facilitators (e.g. UNCITRAL, eIDAS as leading examples) & barriers (e.g. differences in TS provisions, in recognition provisions)

➢ **Supervision & auditing**

   ➢ In place, with pre-authorisation, in most countries & agreement-based realms

   ➢ Differences in auditing framework (e.g. national, IAF/ILAC MLA ISO/IEC 17065/21, ad hoc commercial)

➢ **Best practice**

   ➢ Many commonly used international standards (e.g. X.509, RFCC5280/3647, ETSI ESI standards)

   ➢ Still many possible different interpretations / divergent implementations / different levels of details

➢ **Trust representation**

   ➢ Technically not an issue (e.g. Root store, trusted lists, mixed & bridges) … so far no eIDAS Art.14 concrete activation

   ➢ One visible implementation … Adobe integration of EU MS trusted list based validation of QESig/QESeal

# 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