ETSI
The Standards People

Global acceptance of EU Trust Services

Presented by: **Olivier DELOS** For: **APKIC Symposium, Mumbai, India**

05.12.2019

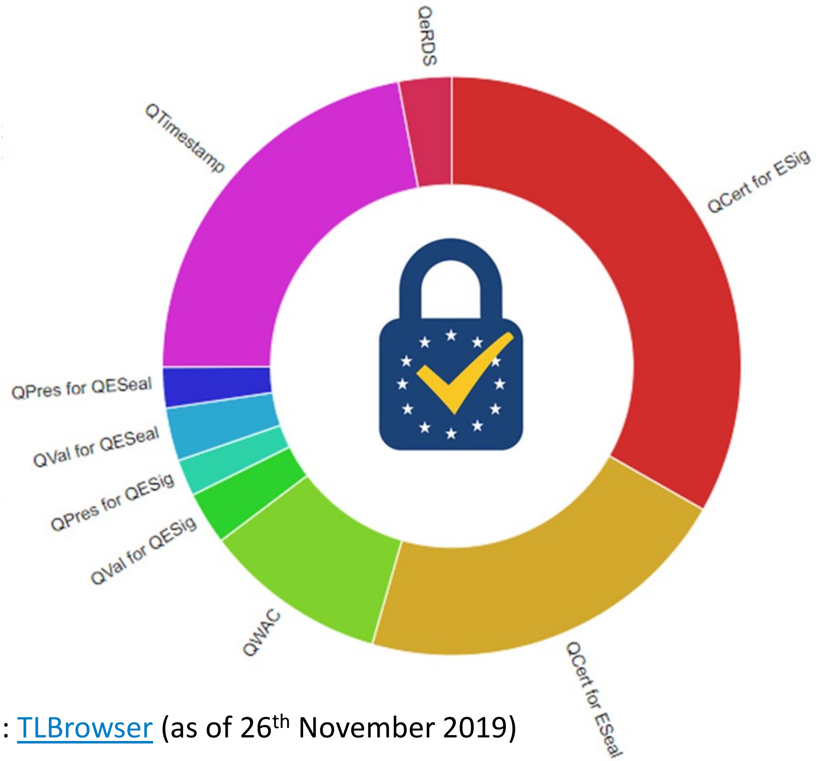
Agenda

- Background
- Study Aims
- Methodology
- Report recommendations
- Final points

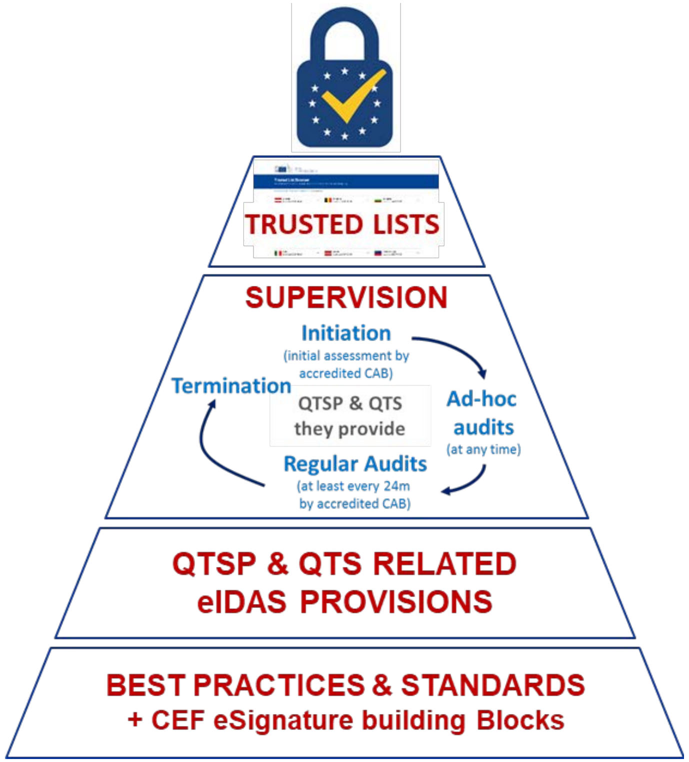
Background EU Trust Services

eIDAS EU Regulation 910/2014

- Establishes EU legal framework for (qualified) trust services from (qualified) trust service providers
- Ensure QTSP/QTS conformance through national supervisory regime and audits performed by accredited conformity assessment bodies (CABs)



Source: TLBrowser (as of 26th November 2019)

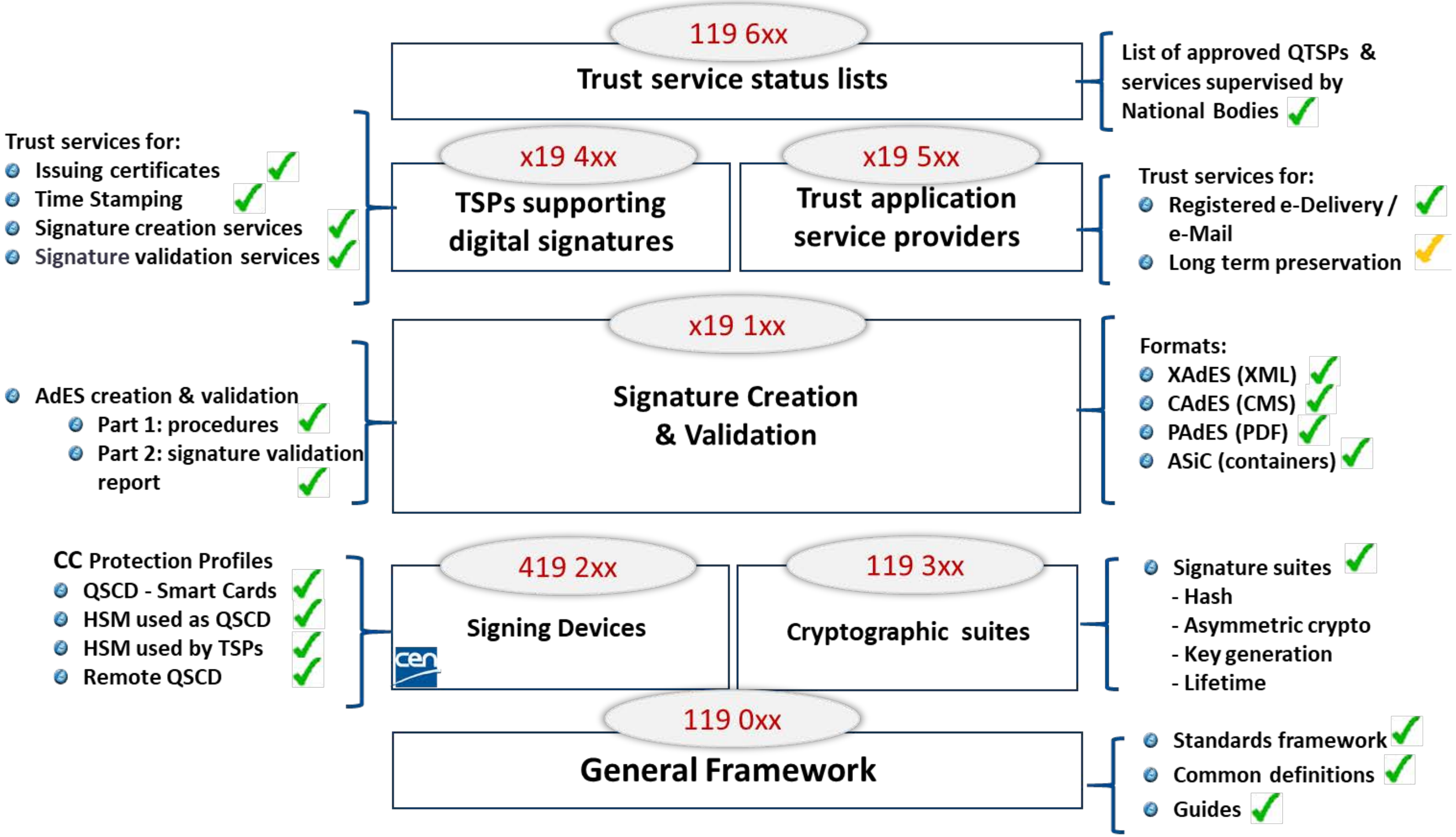


TRUSTED LISTS
SUPERVISION
Initiation
(initial assessment by accredited CAB)
Termination
QTSP & QTS they provide
Ad-hoc audits
(at any time)
Regular Audits
(at least every 24m by accredited CAB)
QTSP & QTS RELATED eIDAS PROVISIONS
BEST PRACTICES & STANDARDS
+ CEF eSignature building Blocks

Background EU Trust Services

ETSI TC ESI

- Defines standards for trust services



119 6xx

Trust service status lists

List of approved QTSPs & services supervised by National Bodies ✓

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

x19 4xx

TSPs supporting digital signatures

x19 5xx

Trust application service providers

Trust services for:
- Registered e-Delivery / e-Mail ✓
- 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

cen

119 3xx

Cryptographic suites

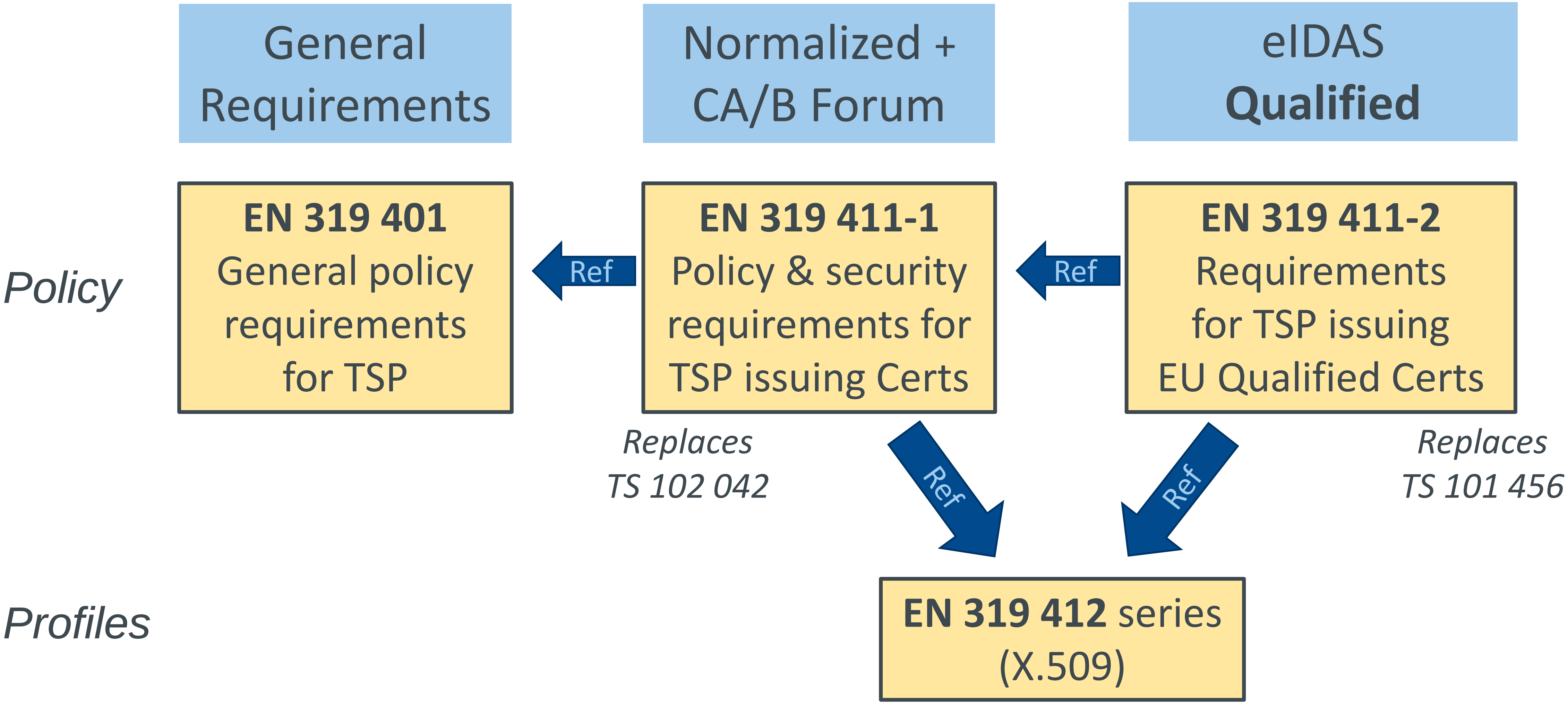
- Signature suites ✓
  - Hash
  - Asymmetric crypto
  - Key generation
  - Lifetime

119 0xx

General Framework

- Standards framework ✓
- Common definitions ✓
- Guides ✓

ETSI standards overview: Trust services issuing certificates



General Requirements

Normalized + CA/B Forum

eIDAS **Qualified**

Policy

EN 319 401
General policy requirements for TSP

Ref

EN 319 411-1
Policy & security requirements for TSP issuing Certs

Ref

EN 319 411-2
Requirements for TSP issuing EU Qualified Certs

Replaces TS 102 042

Ref

Ref

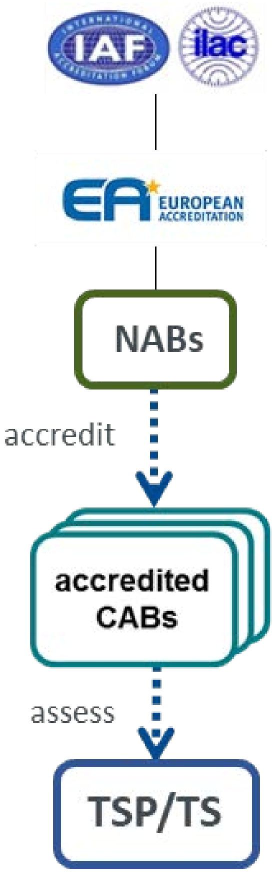
Replaces TS 101 456

Profiles

EN 319 412 series
(X.509)

ETSI standards overview: TSP audit requirements

- EN 319 403 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

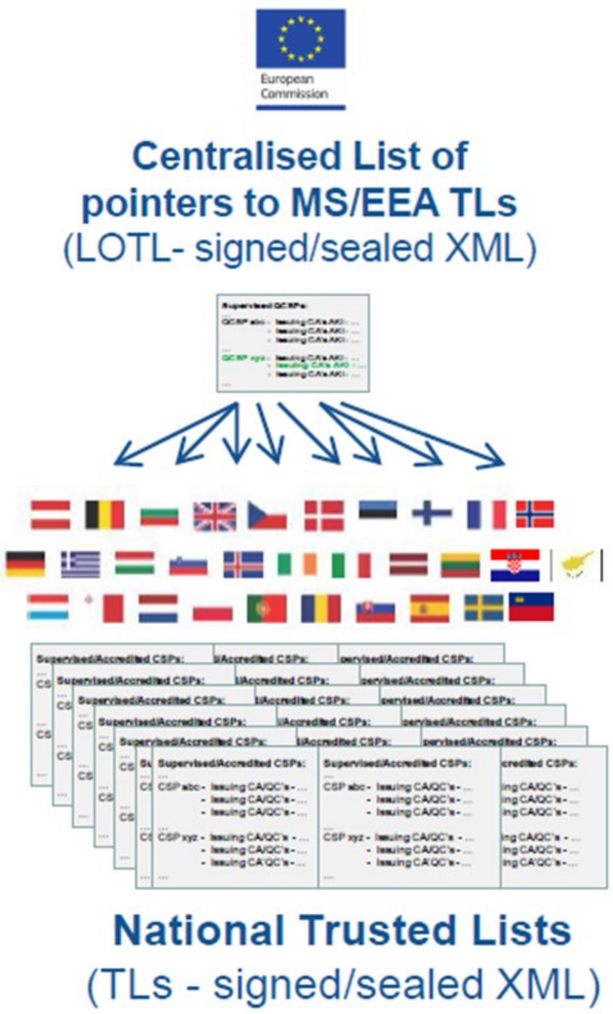


EA-MLA (EA 1/06) – IAF PR4

- 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

ETSI standards overview: Trusted Lists

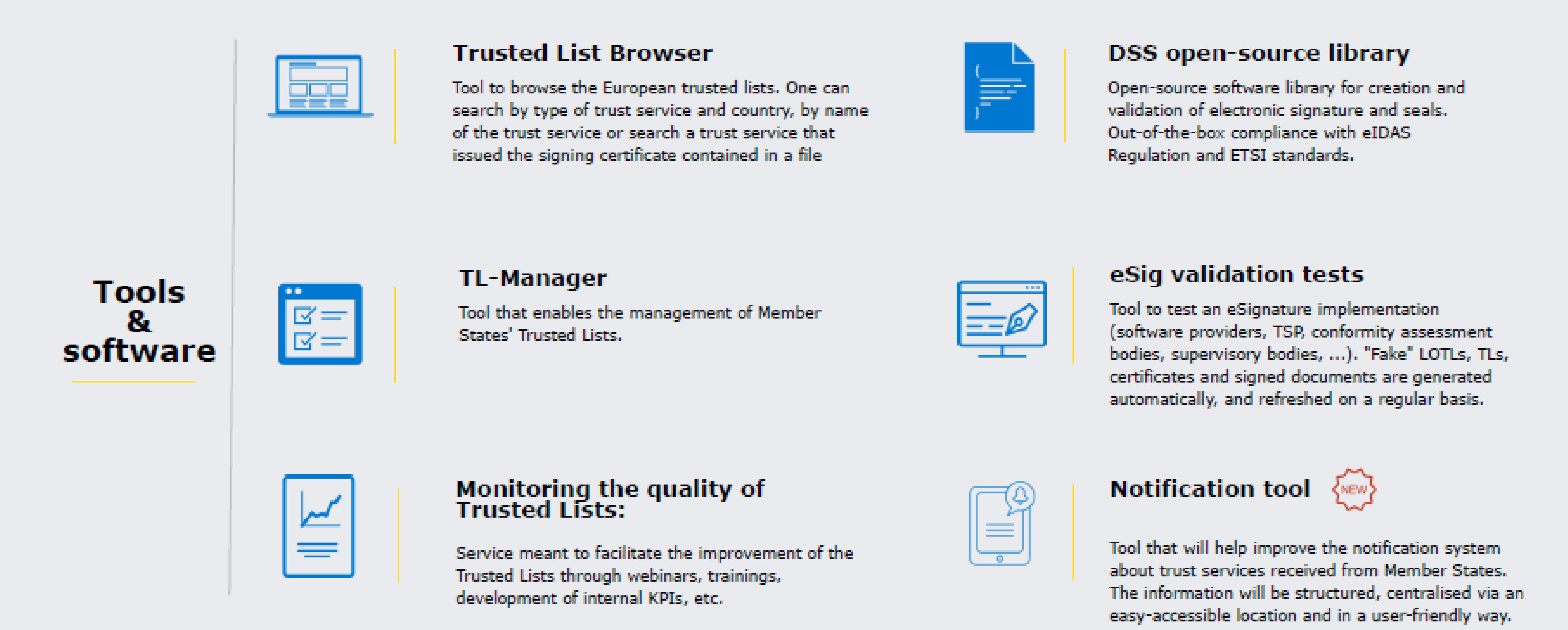
- eIDAS Regulation requires EU MS to maintain national trusted list having constitutive value on who is QTSP for what type of QTS
  - Legal certainty
  - With full history on qualified status
- CID (EU) 2015/1505
  - Procedures and formats for EU MS TL (signed XML)
  - Building upon **ETSI TS 119 612** v2.1.1
    - Specifies also TLs for 3rd countries or international organisations
- EC compiled list of pointers to EU MS TLs allowing for their location and authentication



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

National Trusted Lists (TLs - signed/sealed XML)

EC CEF eSignature Service Offering (also available to 3rd countries)



Tools & software

Trusted List Browser

Tool to browse the European trusted lists. One can search by type of trust service and country, by name of the trust service or search a trust service that issued the signing certificate contained in a file

TL-Manager

Tool that enables the management of Member States' Trusted Lists.

Monitoring the quality of Trusted Lists:

Service meant to facilitate the improvement of the Trusted Lists through webinars, trainings, development of internal KPIs, etc.

DSS open-source library

Open-source software library for creation and validation of electronic signature and seals. Out-of-the-box compliance with eIDAS Regulation and ETSI standards.

eSig validation tests

Tool to test an eSignature implementation (software providers, TSP, conformity assessment bodies, supervisory bodies, ...). "Fake" LOTLs, TLs, certificates and signed documents are generated automatically, and refreshed on a regular basis.

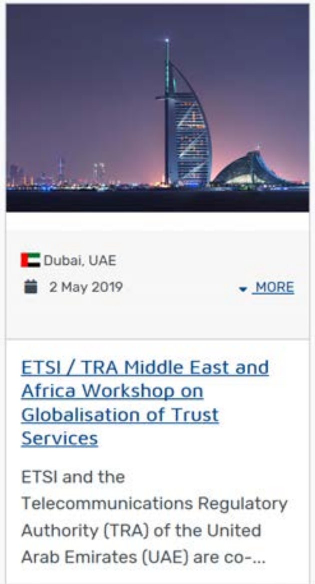
Notification tool NEW

Tool that will help improve the notification system about trust services received from Member States. The information will be structured, centralised via an easy-accessible location and in a user-friendly way.

Source: CEF eSignatures

STF 560 Study

- Investigate existing PKI-based trust service schemes and their trust model around the world
  - Questionnaire & Desktop research
  - Regional Workshops in Dubai, Tokyo, Mexico & New York
- Aims to facilitate cross recognition between EU eIDAS trust services, and other non-EU schemes.
- Identify technical basis for mutual recognition
  - Incl. model, barriers, solutions
- Methodology on 4 pillars:
  - legal context, supervision/audit, best practice, trust representation

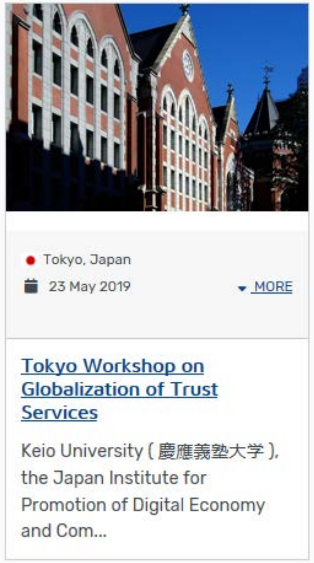


Dubai, UAE

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-...

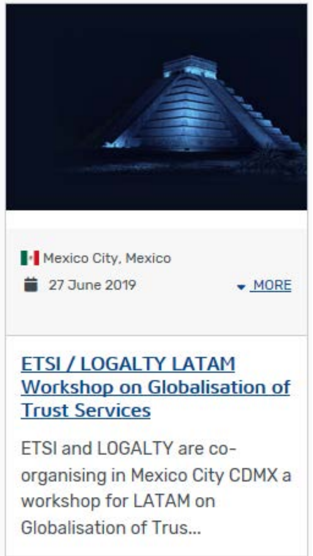


Tokyo, Japan

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...

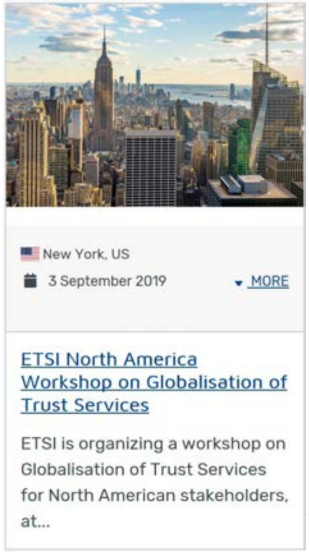


Mexico City, Mexico

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

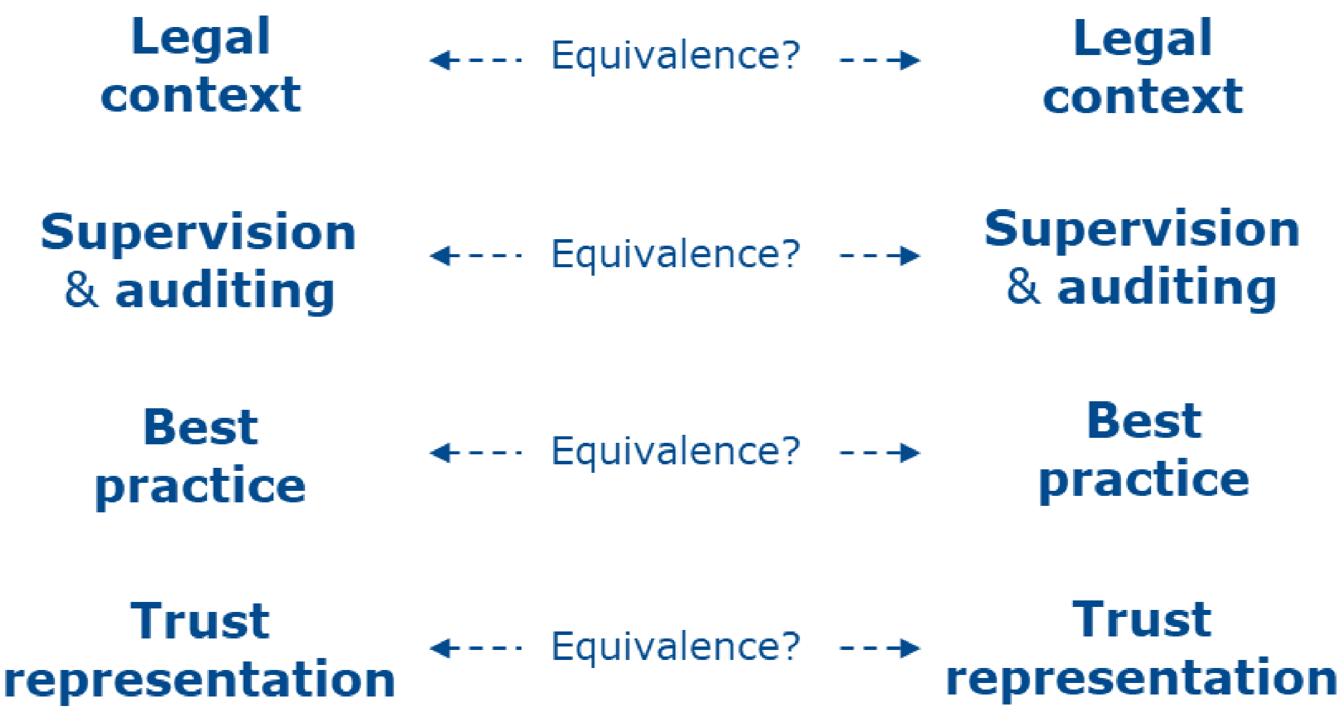
ETSI North America Workshop on Globalisation of Trust Services

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

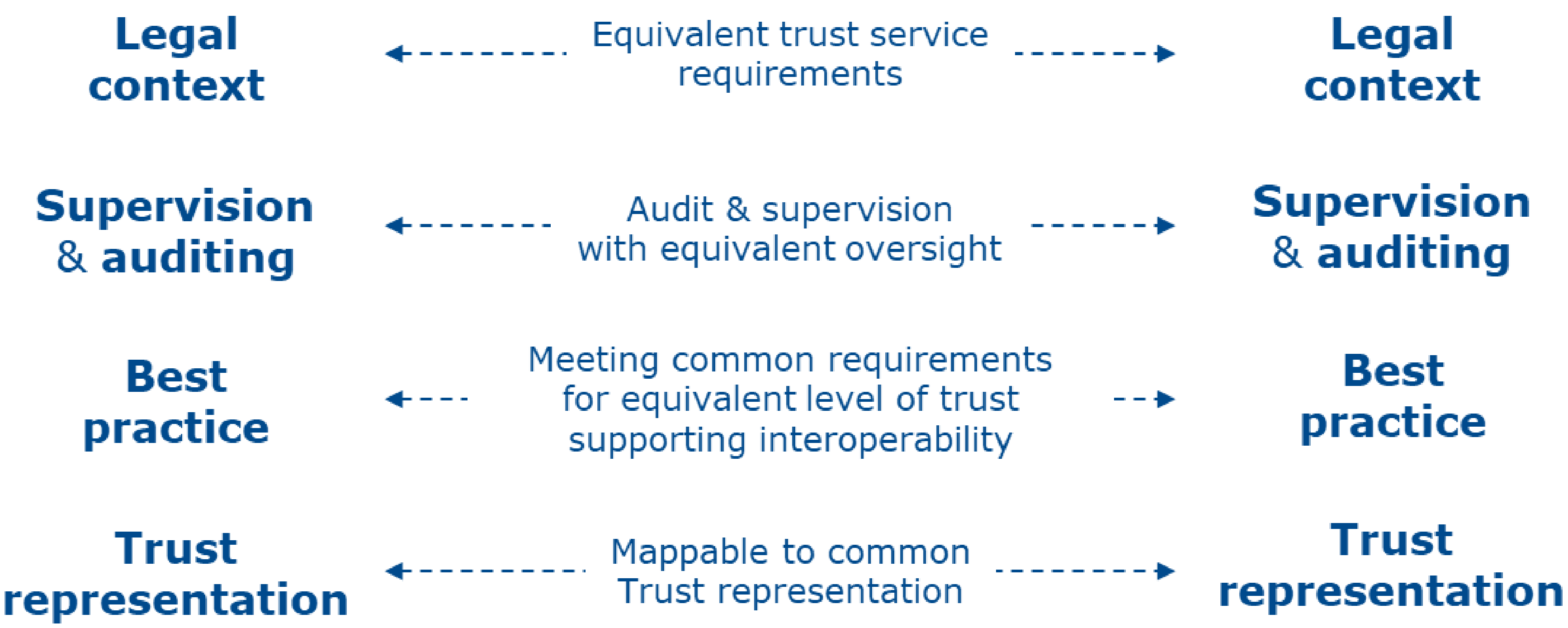
Best practice ←--- Equivalence? ---→ Best practice

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

Methodology

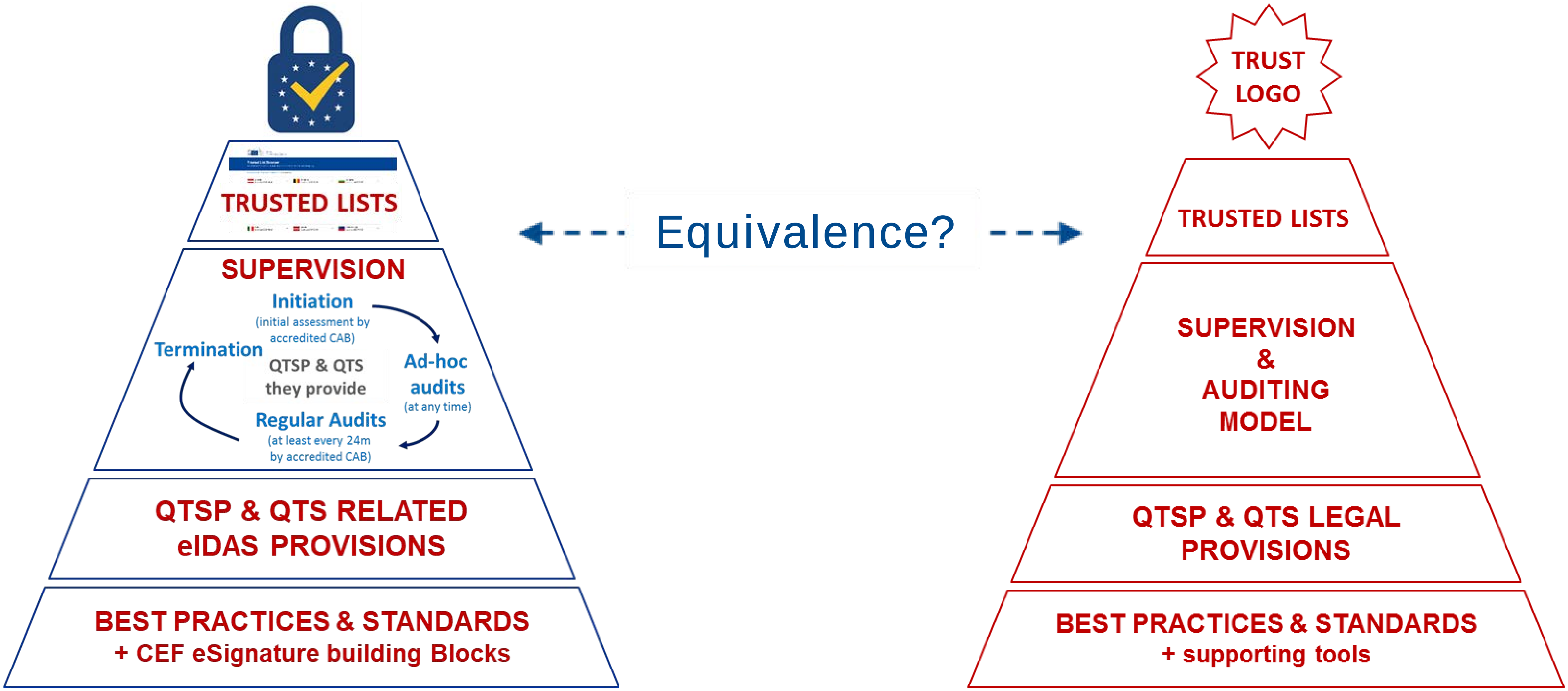
Main points for comparison between PKI-based trust service schemes

(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



TRUSTED LISTS

SUPERVISION

Initiation
(initial assessment by accredited CAB)

Ad-hoc audits
(at any time)

Regular Audits
(at least every 24m by accredited CAB)

Termination

QTSP & QTS they provide

QTSP & QTS RELATED eIDAS PROVISIONS

BEST PRACTICES & STANDARDS
+ CEF eSignature building Blocks

Equivalence?

TRUST LOGO

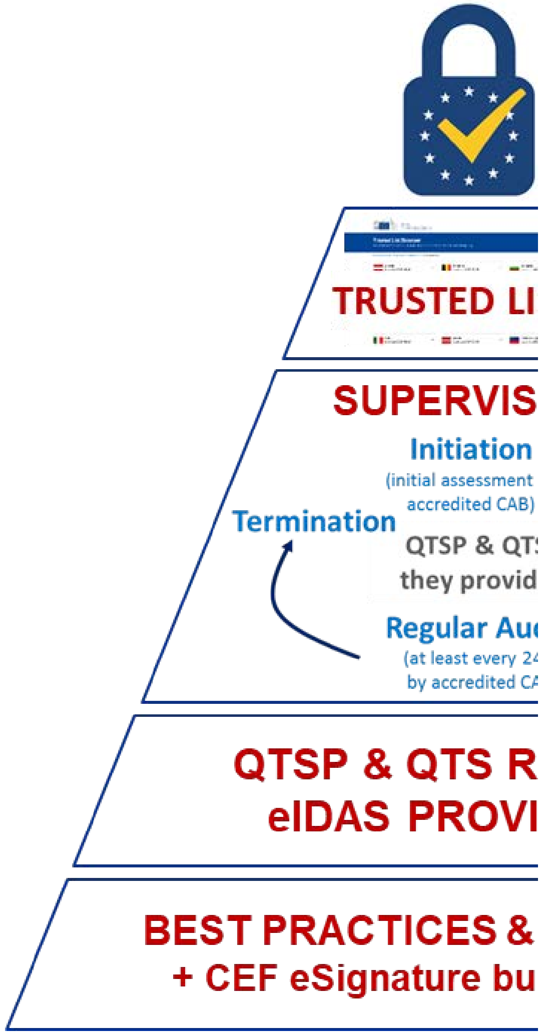
TRUSTED LISTS

SUPERVISION & AUDITING MODEL

QTSP & QTS LEGAL PROVISIONS

BEST PRACTICES & STANDARDS
+ supporting tools

Methodology



Main pillars for comparing PKI-based trust service schemes

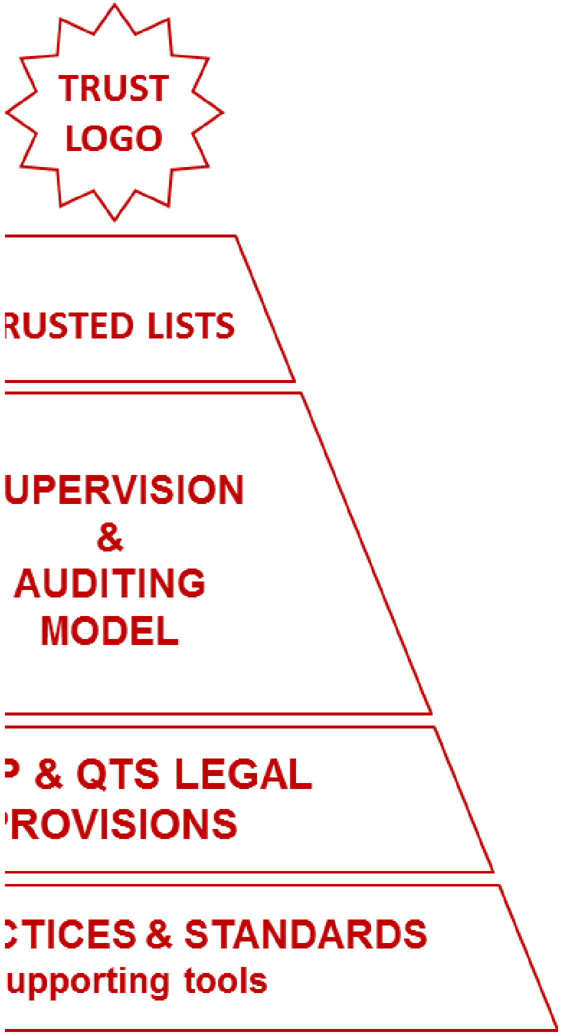
(e.g. in a view of establishing recognition)

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

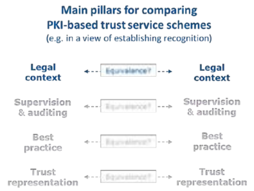
Supervision & auditing ←--- Equivalence? ---→ **Supervision & auditing**

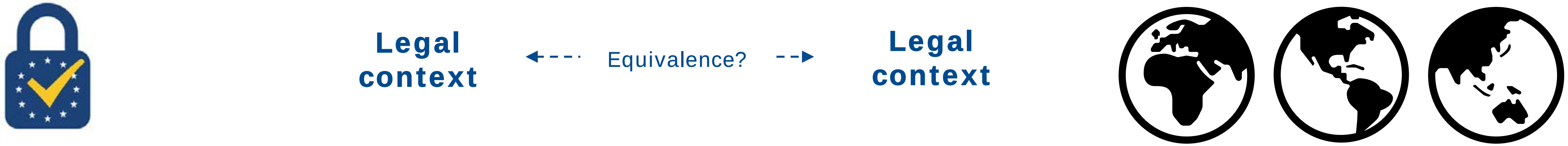
Best practice ←--- Equivalence? ---→ **Best practice**

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



Methodology

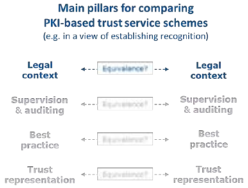




- Regulatory vs Agreement-based
- General principles
  - Non-discrimination against the use of electronic means
  - Technology neutrality (does not prevent being prescriptive with regards to a particular technology)
  - Functional equivalence
  - etc.
- Trust services
  - e.g. Creation / Preservation / 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



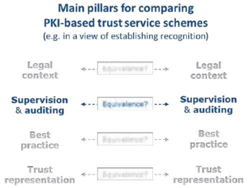
Main pillars for comparing PKI-based trust service schemes
(e.g. in a view of establishing recognition)

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

…

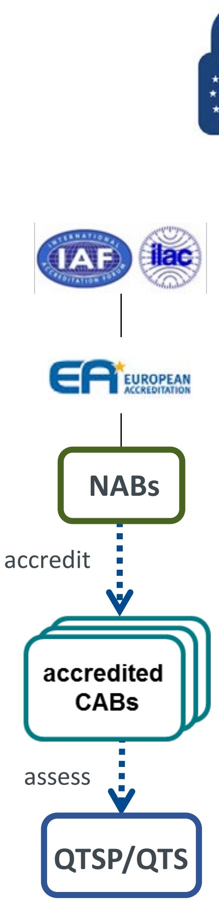
- TSP/TS Levels of reliability
  - e.g. qualified vs non-qualified
- Obligations of TSPs
  - Liability & burden of proof, Accessibility for persons with disabilities, supervision/audits, Correct operations, Security risks management, Security/Personal data breach notifications, Data protection, Staff,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

Methodology



Supervision & auditing ←--- Equivalence? ---→ **Supervision & auditing**

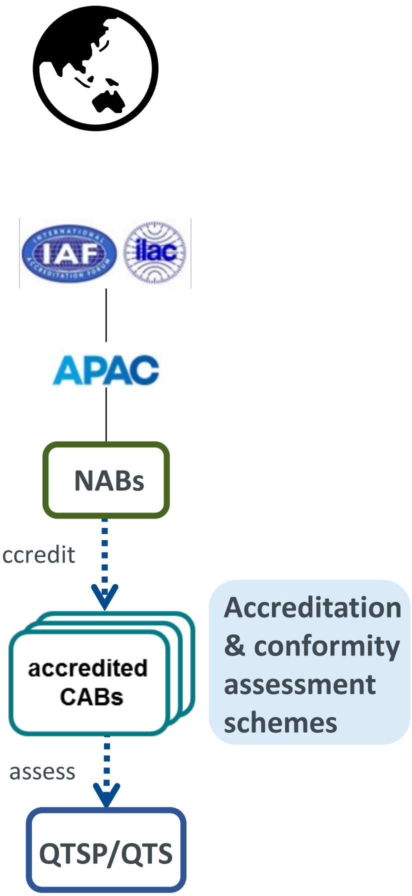
e.g.



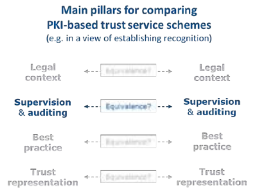
ISO/IEC 17011 certification
ISO/IEC 17065
EN 319 403
eIDAS Regulation

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

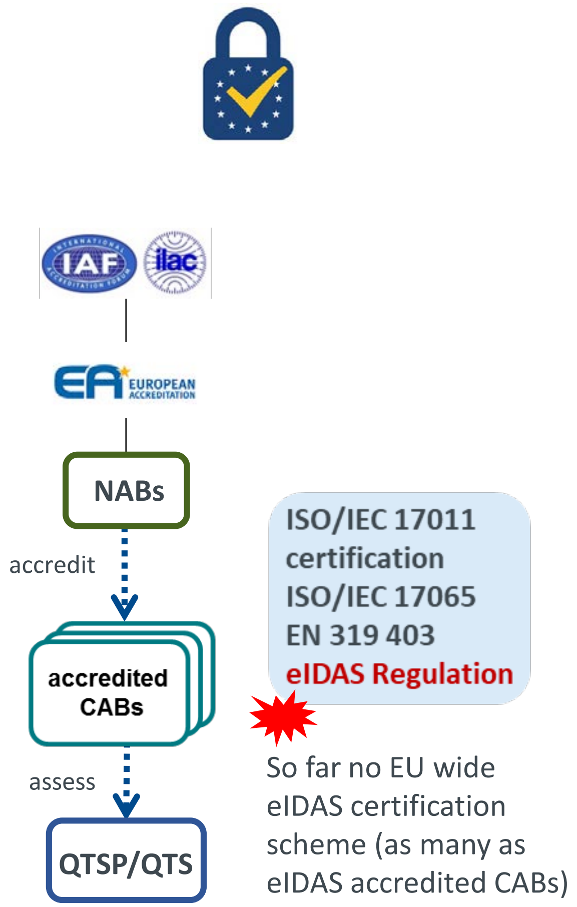
- ➢ Authorities approving (accrediting) auditing bodies
- ➢ Auditing bodies approval (accreditation) scheme
- ➢ Requirements on auditing bodies
  - ➢ Type of bodies
  - ➢ Conduct of assessment
  - ➢ Skills / competences
- ➢ Auditing (certification) scheme
- ➢ Assessment against what "normative document"
  - ➢ Regulation (legal requirements)
  - ➢ Technical standard
  - ➢ Mix
- ➢ Conformity assessment report
- ➢ Supervision decision
- ➢ Links into trust representation



Methodology



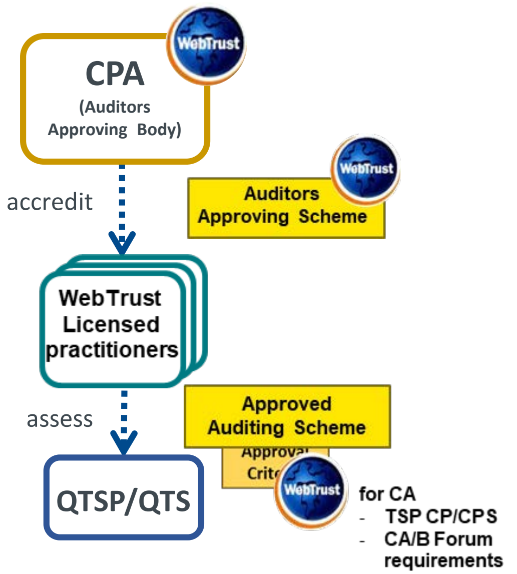
Supervision & auditing ← - - - Equivalence? - - → **Supervision & auditing** **e.g.**



ISO/IEC 17011 certification
ISO/IEC 17065
EN 319 403
eIDAS Regulation

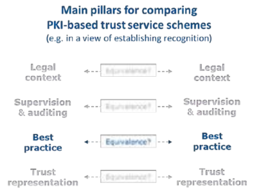
So far no EU wide eIDAS certification scheme (as many as eIDAS accredited CABs)

- 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


CPA
(Auditors Approving Body)
WebTrust
accredit
Auditors Approving Scheme
WebTrust Licensed practitioners
assess
Approved Auditing Scheme
Approval Crit
QTSP/QTS

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

Methodology



Best practice ← Equivalence? → Best practice

e.g.

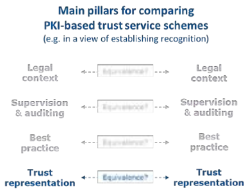
Common technical basis

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**

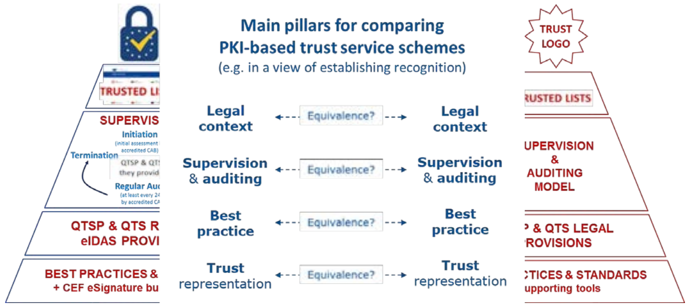
e.g.

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

Cross-certification

Trust Stores

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



Study report

- Publication due end 2019 (TR 103 684)
  - Investigate existing PKI-based trust service schemes and their trust model around the world
  - Identify technical basis for mutual recognition
  - Identify barriers & proposed solutions
- Analyses 37 existing schemes
- The study concludes with 20 recommendations

UNCITRAL
ISO/IEC 21188
ISO/IEC 27099
WebTrust® for CA
CA/Browser Forum
IMRT-WG (EU, JP, US)
Kantara

Adobe AATL
CertiPath
SAFE-BioPharma®
Google Chrome
Apple
Microsoft
Mozilla

Switzerland

AAECA Net
Israel
Sultanate of Oman
UAE
Botswana

Canada
México
US Federal PKI
Argentina
Bolivia
Brazil
Chile
Columbia
Paraguay
Peru
Uruguay

China
Hong Kong
India
Japan
APKIC
Russia

Report results – Comparison overview

- **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

Report recommendations – General

a) Establishing mutual recognition between EU and non-EU PKI based trust services, each of the 4 areas of comparison needs to be taken into account

b) ETSI maintain an ongoing liaison with a number of transnational groups, e.g.:

- Asia PKI Consortium,
- Arab African e-Certification Authorities Network,
- International Mutual Recognition Technical Working Group (EU, Japan and North America)

→ exchange information relevant to mutual recognition

Report recommendations – Legal context

c) Further harmonising at the international level, e.g. UNCITRAL work

d) EU should take opportunity of eIDAS 2020 revision to further facilitate international mutual recognition

e) EU mutual recognition approach needs to recognise the significant role of agreement-based schemes as well as of schemes based on a national regulations

f) Non-Qualified trust services supporting advanced electronic signatures may act as a basis both for the recognition of cross-border transactions … agreements

g) The advantages of EU Qualified trust services should be promoted. In particular that ..a single legal framework which avoids the variety of … trust schemes

h) eIDAS Art.14 is a barrier to mutual recognition of 3rd country trust services as QTS in EU

Report recommendations – Supervision & auditing

i) The ETSI standard for conformity assessment and audit EN 319 403 [i.23] should be promoted globally, particularly through the International Accreditation Forum (IAF)

j) In the absence of a global accreditation scheme for the audit of trust service providers, some flexibility may be necessary in the area of audit schemes, and schemes such as WebTrust might need to be recognised

k) The lack of consistency of the best practices used in the audit schemes for qualified trust services in Europe is jeopardizing their mutual recognition

l) The role of Policy Management Authorities (PMA) in agreement-based PKI schemes in overseeing the operation of trust services should be taken into account

m) Formal recognition of EN 319 403 through eIDAS article 20.4 or a certification scheme under Cyber security regulation → EN as preferred basis for cross recognition

Report recommendations – Best practices

n) The adoption of common standards, such as those defined by ETSI, as the basis for the provision of trust services will assist significantly in mutual recognition

o) Non-EU countries looking for mutual recognition should be encouraged to adopt the latest ETSI eIDAS-based standards

p) ETSI standards should be extended to provide an interoperable equivalent to the EU Qualified Certificate Policies (QCP-x) which may be adopted by non-EU countries and or agreement-based scheme, …

q) Upcoming standard to be ISO/IEC 27099 on PKI policy and practices framework should be influenced to ensure that it is aligned with ETSI standards for trust services

r) ETSI standards should take into account ISO/IEC 27701 on privacy to facilitate international alignment

Report recommendations – Trust representation

s) PKI schemes aiming to achieve mutual recognition with the EU should be encouraged to map their trust representation (e.g. bridge certificates) into an equivalent to EU trusted lists

t) The EN 319 412-5 QcCompliance statement should be updated to extend its scope to non-EU countries

Final Points

- ➢ Aiming for further update(s) in the future
  - ➢ Adding country profiles on PKI-based trust service schemes and their trust model
  - ➢ Identify / update technical basis for mutual recognition
  - ➢ Identify / monitor barriers & proposed solutions
- ➢ Interested countries & PKI scheme owners may contribute providing input following the report structure