ETSI Study on Globalisation of Trust

Presented by: Olivier DELOS
For: ETSI/TRA workshop (Dubai)

02.05.2019
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

Source: TLBrowser (as of 1 May 2019)
ETSI Standards for Trust Services

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

AdES creation & validation
- Part 1: procedures
- Part 2: signature validation report

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

List of approved QTSPs & services supervised by National Bodies

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

Formats:
- XAdES (XML)
- CADES (CMS)
- PAdES (PDF)
- ASiC (containers)

Signature creation & Validation

Signage Devices

Cryptographic suites

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

General Framework

Standards framework
- Common definitions
- Guides
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
Methodology

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

- Legal context
- Supervision & auditing
- Technical requirements
- Trust representation

Equivalence?
Methodology

- TRUSTED LISTS
- SUPERVISION
  - Initiation (initial assessment by accredited CAB)
  - QTSP & QTS they provide
  - Regular Audits (at least every 24m by accredited CAB)
  - Ad-hoc audits (at any time)
- 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

© ETSI 2019
Main pillars for comparing PKI-based trust service schemes
(e.g. in a view of establishing recognition)

- **Legal context**
  - Equivalence?

- **Supervision & auditing**
  - Equivalence?

- **Technical requirements**
  - Equivalence?

- **Trust representation**
  - Equivalence?
Methodology

- 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

Supervision & auditing

- 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

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

- 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

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

**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
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