UPDATE ON CEN & ETSI STANDARDISATION ON SIGNATURES

Workshop eIDAS Trust Services: 6 months on after the switch-over

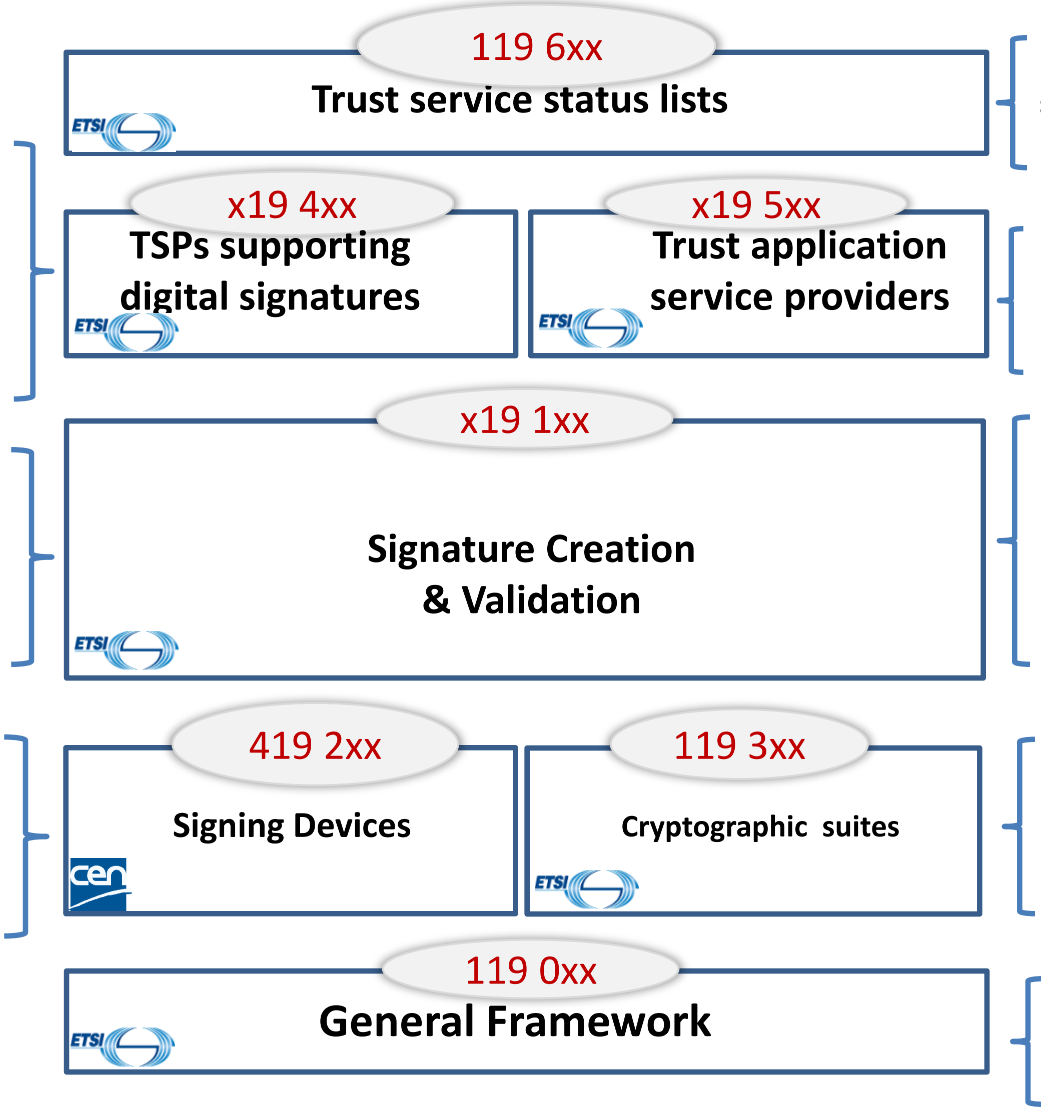
19 December 2016

Riccardo Genghini, TC ESI chairman

Topics

- eIDAS Standards Status
- ETSI Ongoing / Future Activities
  - TSP Standards Updates
  - Signature Validation Service
  - eDelivery
  - Preservation
  - Remote Signature Creation Component Services
- CEN Ongoing Activities
  - HSM & Time-stamping protection Profiles
  - Remote Signing

eIDAS Standards Framework: Published Standards



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
- Validation services

x19 4xx
TSPs supporting digital signatures

x19 5xx
Trust application service providers

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

- Procedures for AdES creation & validation ✓

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

Published work inclusion in CID

- 2 EC Implementing Decisions published on 8 Sept. 2015 mandating support by EU Member States (EUMS) of ESI specifications (baseline CAdES/XAdES/PAdES/ASiC signatures + Trusted Lists)
  - CID (EU) 2015/1505 on Trusted Lists: referring TS 119 612 v2.1.1
  - CID (EU) 2015/1506 on formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies: referring old baseline profiles, waiting for ENs to be published
- 1 EC Implementing Decision published on 25 April 2016 referring to CEN standards
  - CID (EU) 2016/650 for the security assessment of qualified signature and seal creation devices: referring to EN 419211

Published work - testing and interoperability

- Testing conformance and interoperability
  - ETSI organized 6 Plugtests in the past 2 years
    - Signature validation Plugtests Nov.-Dec. 2014, in coordination with EC
    - PAdES (May 2015) , CAdES (June-July 2015) and XAdES (October 2015) signature formats (testing previous TS and draft ENs)
    - Signature validation Plugtests in February 2016, in coordination with EC
    - ASiC (signature containers) Plugtests (Nov-Dec. 2016)
  - Availability of Signature Conformance checkers for CAdES, XAdES, PAdES and ASiC - freely accessible

ESI ongoing work

- TSP Standards updates to consider feedback received on published documents, revocation status beyond expiry…
- Signature validation service provided by TSP
  - Starting work
  - New standards
    - TS 119 441: TSP Policy requirements
    - TS 119 102-2: Signature Validation Report
    - TS 119 442: Protocols
- Signature Preservation: Scoping study and framework for long term preservation services
  - Aim complete early 2017
  - Preservation of the validity of digital signatures
  - Preservation of the integrity of digital objects using digital signature / time-stamping techniques

ESI ongoing work

- Registered eDelivery
  - Coherent set of Standards for Electronic Registered Delivery (ERD) and Registered Electronic Mail (REM), which ESI considers a special type of ERD.
  - Documents to be produced:
    - EN 319 522 (ERD) & 319 532 (REM) Technical specifications, including: architecture, semantic contents, formats, bindings to transport protocols
    - EN 319 521 & 319 531 Policy and security requirements
    - TS 119 524 & 119 534 Testing interoperability and conformance

ESI future work

- Remote Signature Creation Component Services
  - Plan Starting early 2017
  - New standards
    - TS 119 431-1: Policy requirements for TSP Service Components operating for a TSP operating a remote QSCD
      (Building on CEN standards for server signing)
    - TS 119 431-2: Policy requirements for TSP Service Components supporting AdES Signature Creation
    - TS 119 432: Protocols for remote digital signature creation
- Preservation

CEN - Ongoing Activities

- EN 419231 Time-stamping Protection Profile
  - Evaluation successfully completed, awaiting certification
  - About to be sent to CEN enquiry
- EN 419221-5 Protection Profile for TSP cryptographic device
  - evaluation successfully completed, awaiting certification
- CEN Server signing
  - EN 419 241-1 General System requirements
    about to be sent to CEN enquiry
  - EN 419 241-2 Protection Profile for QSCD for Server Signing will be sent out to evaluation and CEN enquiry in February 2017

Conclusions

All primary standards are published as ENs

- ETSI: available for free download
  http://www.etsi.org/standards-search

  Overview of ESI standards:
https://portal.etsi.org/TBSiteMap/ESI/ESIActivities.aspx
- CEN: available through National Standards Orgnisations

Ongoing support for eIDAS standards

Any questions