





Welcome to the World of Standards



CA DAY

Status Update ETSI eSignature Standardization

Nick Pope, Thales – Vice Chair TC ESI

-  eIDAS Standards Status
-  ETSI Ongoing / Future Activities

eIDAS Standards Framework: Published Standards

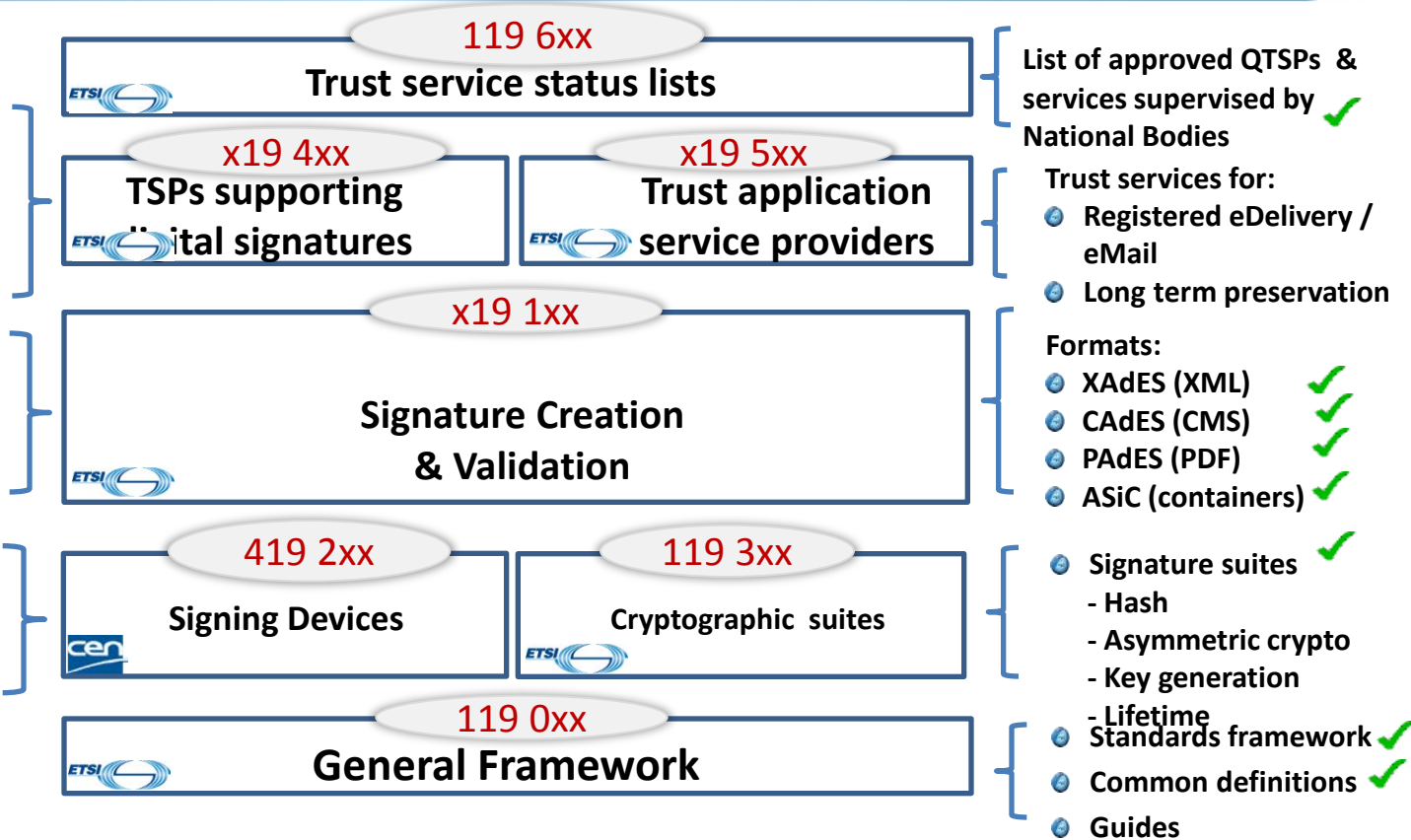


- Trust services for:
- Issuing certificates ✓
 - Time Stamping ✓
 - Signature creation services
 - Validation services

- Procedures for AdES creation & validation ✓

CC Protection Profiles

- QSCD - Smart Cards ✓
- HSM used as QSCD
- HSM used by TSPs ✓
- Remote QSCD



- Maintenance of existing 319 4xx standards
- AdES Signature validation services
- [Remote] Signature Creation Services
- Registered E-Delivery
- Long term (signature) preservation
- Ongoing AdES Signature


- Updates to 319 411-1, 319 411-2 and 319 412-x
- Ongoing CA/Browser Forum alignment
- Options for Representing eID minimum attributes in X.509 Certificate
- Short term certificates
 - Certified key valid for a limited session
 - Aim to treat in the same way as other certificates
- CRL / OCSP beyond certificate expiry


- 🌐 TSP Policy and security requirements
- 🌐 Protocols profiles for TSP providing validation services
- 🌐 Signature Validation report


- Policy and security requirements for TSP component service operating remote QSCD
- Policy and security requirements for TSP component service supporting AdES digital signature creation
- Protocols for remote digital signature creation


Coherent set of Standards for:
Registered Electronic Mail (REM) and
Electronic Registered Delivery (ERD).


- 🌐 Policy and security requirements
- 🌐 architecture, semantic contents, formats, bindings to transport protocols
- 🌐 Testing interoperability and conformance

-  SR 019 510 : Scoping study and framework for long term preservation services
 - Aim complete end 2016
 - General purpose preservation services using digital signature / time-stamping techniques
 - Includes preservation of digital signatures

-  Aim to start 2017 on specific standards

-  PAdES Document Time-stamp signature
 - RFC 3161 timestamp on document

-  ETSI hold regular AdES Interoperability test events
<http://xades-portal.etsi.org/pub/index.shtml>

-  AdES Conformance checker
<http://signatures-conformance-checker.etsi.org/pub/index.shtml>

Thank you for your attention



ETSI Documents: Free download

<http://www.etsi.org/standards-search>

E-Signature news:

http://list.etsi.org/scripts/wa.exe?SUBED1=e-signatures_news&A=1

Further information:

<https://portal.etsi.org/TBSiteMap/ESI/TrustServiceProviders.aspx>