Welcome to the World of Standards

ETSI

World Class Standards

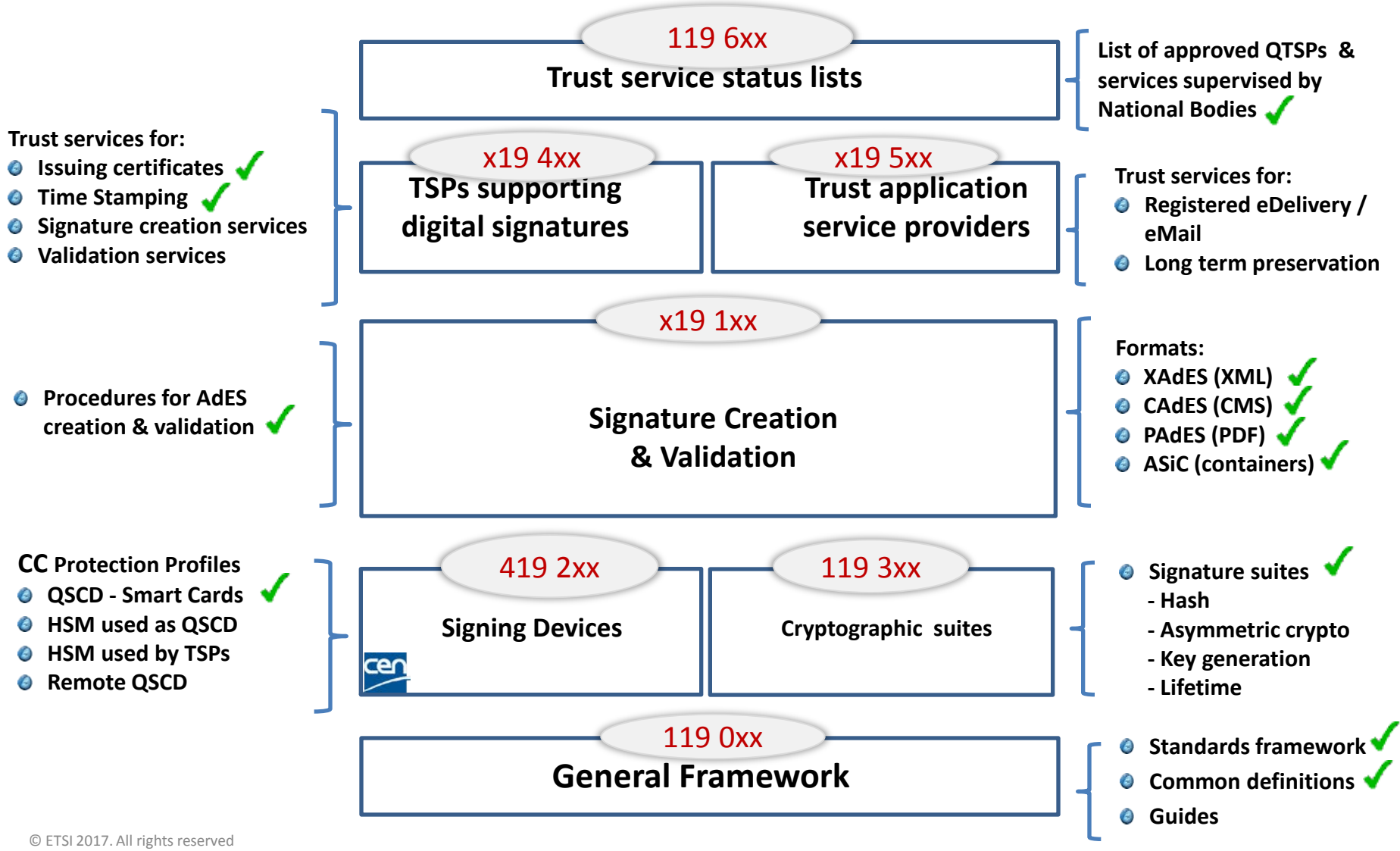
UPDATE ON STANDARDISATION UNDER eIDAS

CA Day 28 Nov 2017

Nick Pope – Vice Chair ETSI Electronic Signatures and Infrastructures

© ETSI 2017. All rights reserved

eIDAS Standards Framework: Published Standards



© ETSI 2017. All rights reserved

Ongoing Standardisation

- Updates to TSP Policy Requirements: EN 319 411-1/2
- Support for PSD2 use of Qualified certificates
- Signature Validation
- Remote signing
  - CEN Standards
  - ETSI Standards
- Electronic Registered Delivery and Registered Electronic Mail Services
- Long term (signature) preservation
- Using Trusted Lists
- Internationalisation
- Need for Clarifying Audit Requirements

Updates to TSP Policy Requirements: EN 319 411-1/2

- Each individual requirement clearly identified
- Alignment with CA Browser Forum
  (EVCG V.1.6.1 for ECVP and BRG v1.4.2)
- Several detailed clarifications
- OCSP & CRL: OCSP recommended (not mandated),
  support for long term validation,
  details on OCSP requirements
- Clearly identify requirement relating to a specific component

Under EN approval: Ballot closed – Detailed issues to be addressed

Documents (with revisions marked):
https://docbox.etsi.org/esi/Open/Compared_deliverables

© ETSI 2017 All rights reserved

Qualified Certificates under PSD2 new Background

- Directive 2015/2366/EU aimed at regulating “payment services”

- Draft Regulatory Technical Standards:
  - High level technical requirements for:
    - strong customer authentication
    - common and secure open standards of communication
  - Final publication by commission due November 2017
  - Requires use of qualified Certificates for secure communications & transactions between payment service providers:
    - Web site authentication certificates
    - e-Seal certificates
  - Requires PSD2 Specific certificate attributes
    - Identifies member state competent authority
    - Payment services authorised

© ETSI 2017. All rights reserved

Qualified Certificates under PSD2 new Work item

ETSI working with ECB ERPB PIS WG to define:

- Qualified Certificate profiles
  - PSD2 Qualified Website Authentication Certificates
  - PSD2 Qualified Seal Certificates

- TSP Policy Requirements for PSD2 Qualified Certificate
  - Requirements for validation of PSD2 specific attributes
  - Revocation of PSD2 certificate due to change in PSD2 attribute status

  Involves interaction with National (Financial) Competent Authority

© ETSI 2017. All rights reserved

Signature Validation

- Standards being developed:
  - TS 119 102-2: Validation Report
  - TS 119 441: Policy requirements for TSPs providing Signature validation services
  - TS 119 442: Protocol for signature validation services
- Protocol features:
  - Supports both XML and JSON exchanges
  - Aligned with OASIS DSS
- Timescale
  - Stable draft for review: Dec 2017
  - Publication: Sept 2018
- Open Workshop
  - 10th January 2018: http://www.etsi.org/news-events/events/1222-2018-01-esignature-and-eseal-validation-workshop

© ETSI 2017. All rights reserved

Remote Signing
CEN Standards for Trustworthy Systems

- Draft CEN Standards:
  - prEN 419 241-1: General System requirements
  - prEN 419 241-2: Protection Profile for QSCD for Server Signing
  - prEN 419 221-5: Cryptographic module
- Authentication can be delegated to an Identity Provider outside QSCD
- Timescale:
  - EN 419 241-1: 1st round agreed with minor revisions, final approval by end 2017
  - EN 419 241-2: 1st round agreed subject to evaluation under Common criteria, aim final approval Q1 2018
  - EN 419 221-5: Final approval by end 2017

© ETSI 2017. All rights reserved

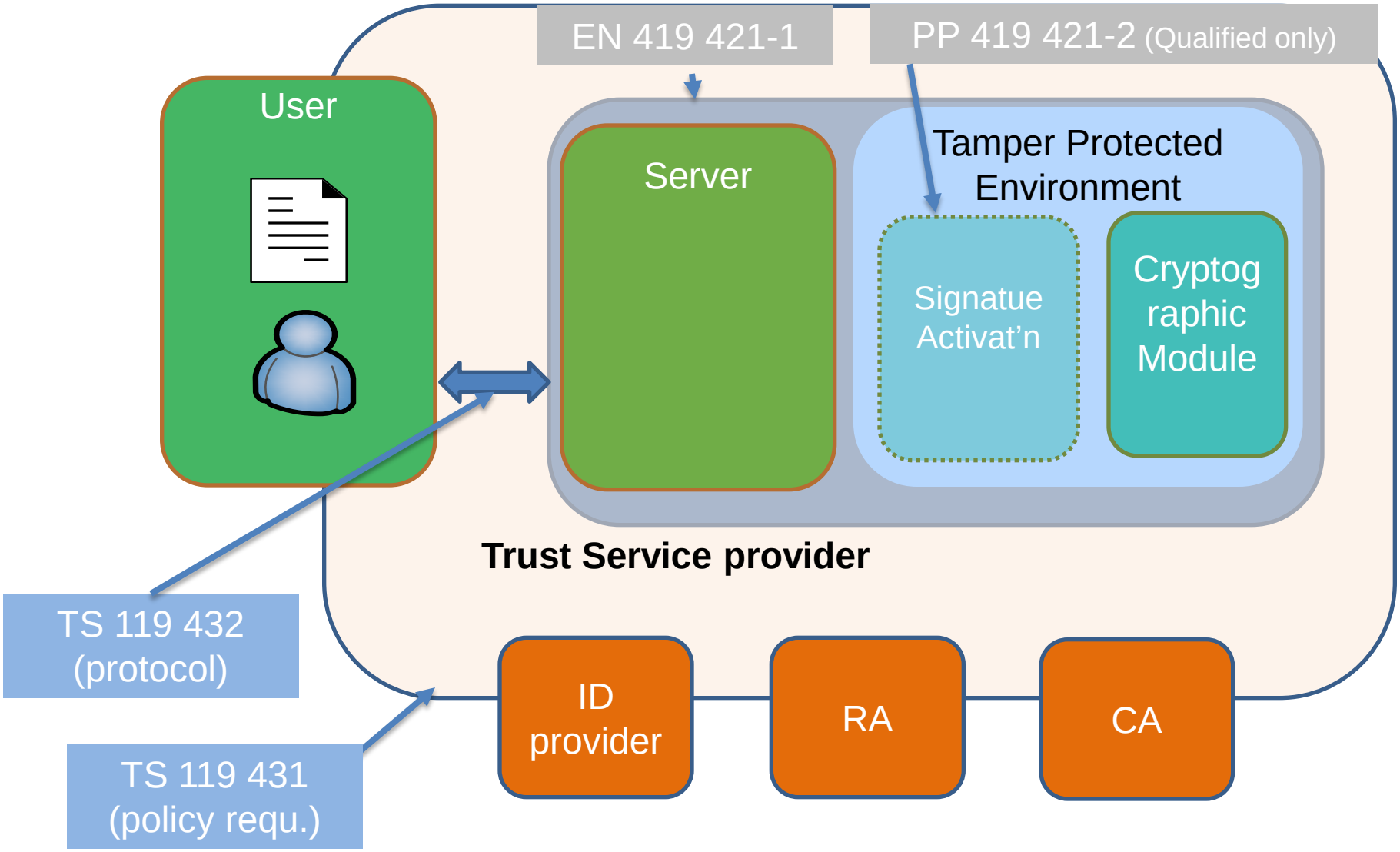
ETSI Signature Creation Protocols & TSP Component Policy Requirements

- Standards being developed:
  - TS 119 431-1: Policy and security requirements for TSP service components operating a remote QSCD / SCD
  - TS 119 431-2: Policy and security requirements for TSP service components supporting AdES digital signature creation
  - TS 119 432: Protocols for remote digital signature creation

- Timescale
  - Started work on detailing scope
  - Funded STF activity started: Oct 2017
  - Stable draft for review: June 2018
  - Publication: Nov 2018

© ETSI 2017. All rights reserved

Scope of remote signing standards



© ETSI 2017. All rights reserved

Electronic Registered Delivery and Registered Electronic Mail

- Existing standards:
  - TS 102 640 (parts 1 to 6) Registered Electronic Mail
- Standards being developed
  - EN 319 522: Electronic Registered Delivery Services
  - EN 319 532: Registered Electronic Mail (REM) Services
  - EN 319 521: Policy and security requirements for Electronic Registered Delivery Service Providers
  - EN 319 531: Policy and security requirements for Registered Electronic Mail Service Providers
  - TS 119 524: Testing Conformance and Interoperability of Electronic Registered Delivery Services
  - TS 119 534: Testing Conformance and Interoperability of Registered Electronic Mail Services
- Timescale
  - **Stable draft of ENs for review: End Oct 2017**
  - EN approval starts: End April 2018
  - ENs published : Feb 2019

© ETSI 2017. All rights reserved

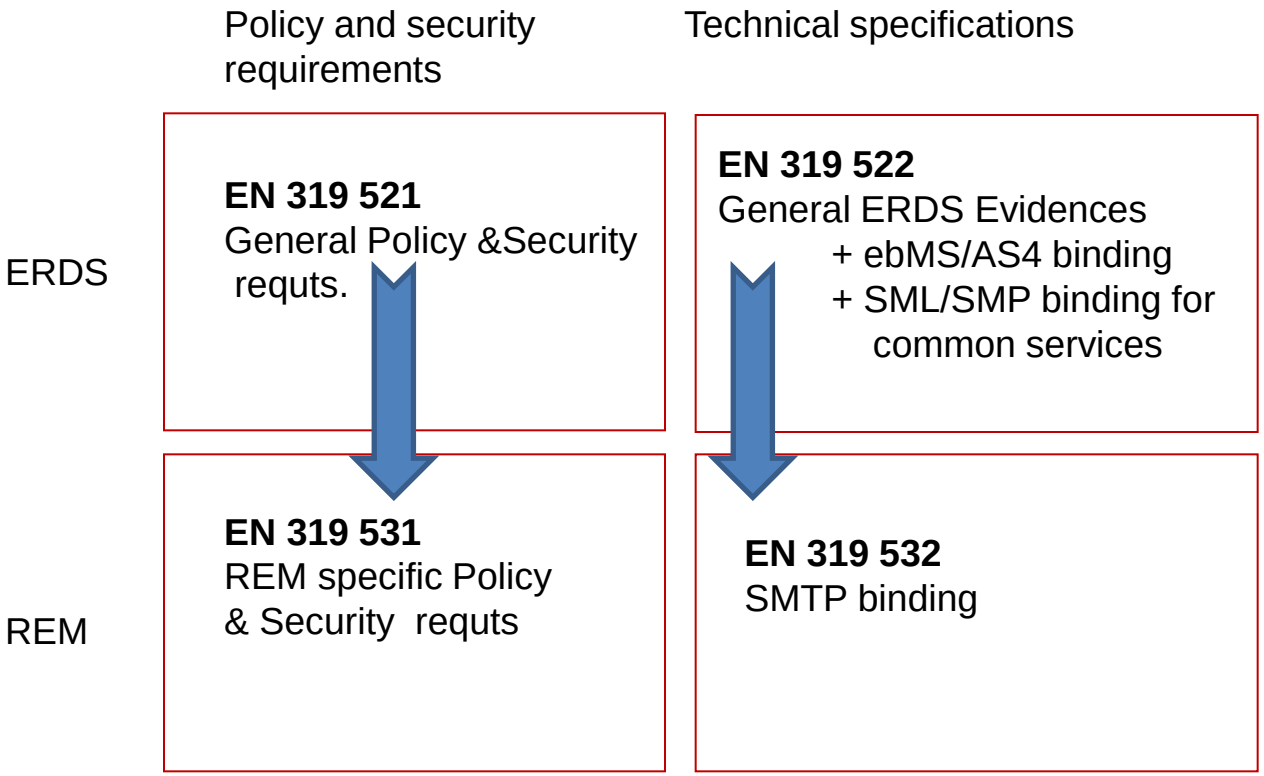
Electronic Registered Delivery and Registered Electronic Mail - Liaison

- ESI has liaised with CEN TC 331/WG2 for properly dealing with CEN TS 16326 specifications on Postal Registered Electronic Mail (PrEM).
- ESI will also liaise with UPU, as its S52 specification is the basis for CEN TS 16326, for properly dealing with the three sets of specifications.
- ESI has also conducted meetings with CEF as a major key player in the ERDS arena.

© ETSI 2017. All rights reserved

Electronic Registered Delivery and Registered Electronic Mail: deliverables and their relationships

Denotes a path from general requirements, common to any ERDS, to requirements that are specific ONLY to REM services and REM services providers.



TS 119 524 Testing Conformance and Interoperability of Electronic Registered Delivery Services
TS 119 534 Testing Conformance and Interoperability of Registered Electronic Mail Services
TR 119 500 Business Driven Guidance for Trust Application Service Providers

Long term (signature) preservation

- Work started:
  - TS 119 511 Policy & security requirements for trust service providers providing long-term preservation of digital signatures or unsigned data using signature techniques
  - TS 119 512 Protocols for trust service providers providing long-term preservation of digital signatures or unsigned data using signature techniques
- Time scale:
  - Stable draft for review April 2018
  - Publication: November 2018

© ETSI 2017. All rights reserved

Using Trusted List [new]

- Use of information within a Trusted List by relying parties
  - Covers use not only for e-Signatures / e-Seal validation but other trust services such QWAC and Registered e-Delivery, validation reports
  - Include algorithm which can be used for machine processing for the purpose of validation of TSP issued information

- Timescale:
  - Stable draft for public review: March 2018

© ETSI 2017. All rights reserved

Internationalisation – USA

- ETSI / US Workshop on “International Trust in digital signatures” 8 March 2017
  - Recognised equivalence between ETSI EN 319 411-1 & 2 and US Federal Bridge Policies
  - Equivalence between US Federal Bridge and EU Trust
    - Tool available to map data between different representations
  - Possible basis of cross recognition of signatures would be via trade agreement
  - Further justification needed to get buy in from US Government

  - SAFE Biopharma produced list of signing CAs that are cross certified directly with SafeBipharma + Federal bridge CA in Trust List format

© ETSI 2017. All rights reserved

Internationalisation – Japan

ETSI / JIPDEC Workshop on “Interoperable Global Trust for Digital Signatures” held 4 July 2017

- ETSI standards for trust services and signatures already widely adopted in Japan
- Looking at comparison of trust infrastructure in Japan and Europe
- JNSA Remote Signature Task Force developed initial architecture
- Considering harmonization with CEN Standards EN 419 241-x
- Interested in ETSI standards for remote signing.

Meeting report & slides available

© ETSI 2017. All rights reserved

Need for clarification of Audit Requirements

- Qualified TSP Audit Supervisory Body Concerns
  - Bi-annual audit
  - No Consistency of audit report
  - Clear statement against eIDAS articles
  - Majority ETSI Based, but not exclusively

- CA/Browser Audit - Browser Software Supplier Concerns
  - Ongoing annual full audit including checks on past year operation
  - Webtrust or ETSI

© ETSI 2017. All rights reserved

Conclusions

- Information on available standards and current activities:

  https://portal.etsi.org/TBSiteMap/ESI/ESIActivities.aspx

- ETSI standards: available for free download

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

  CEN standards: available through National Standards Organisations

- Updates on standardisation:

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

© ETSI 2017. All rights reserved