ETSI standardization for eIDAS

Presented by: **Ernst Giessmann** For: **PKI Forum St. Petersburg**

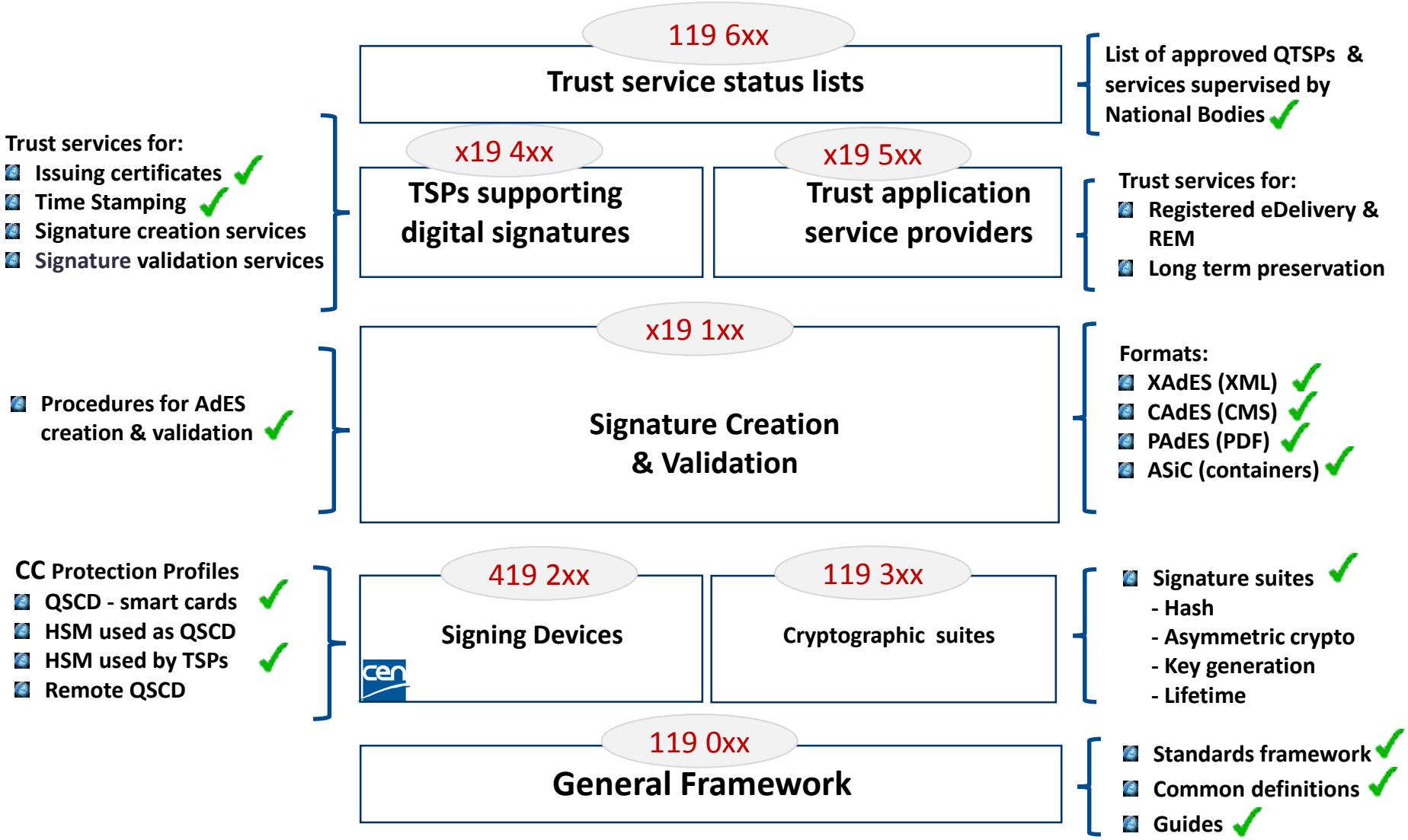
2018-09-25

Agenda

- Signature formats
- CA policy requirements: EN 319 411-1/2
- Signature validation
- Remote signing (CEN & ETSI standards)
- Electronic Registered Delivery and Registered Electronic Mail (REM) services
- Long-term (signature) preservation
- Using Trusted Lists
- Need for clarifying audit requirements

→ **When completed, standards will cover all trust services defined by eIDAS**

eIDAS Standards Framework: Published Standards



Policy Requirements

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

Each individual requirement clearly identified & mapped to a specific component

New TR 119 411-4 : unified checklist for all CPs (Certificate Policy)

Alignment with CA Browser Forum for website certificates

- CA Browser Forum's BRG v1.4.2 / CA Browser Forum's EVCG V.1.6.1 used for EVCP

Several detailed clarifications

OCSP & CRL:

- Mandatory to have at least 1 of OCSP or CRL, OCSP recommended
- Support for long term validation (beyond certificate expiry)

EN 319 411-1 v1.2.2, EN 319 411-2 v 2.2.2, TR 119 411-4 published in May 2018

(see ETSI download page at end of presentation)

PSD2

Qualified Certificates under PSD2 – Background

Directive 2015/2366/EU aimed at regulating payment services

Commission Delegated Regulation (EU) 2018/389:

- High level technical requirements for:
  - Strong customer authentication
  - Common and secure open standards of communication
- Requires use of qualified certificates for secure communication & transactions between payment service providers:
  - Qualified website certificates for payment service providers
  - Qualified e-Seal certificates for payment service providers
- Requires PSD2 specific certificate attributes
  - Identify the authorisations of the payment service provider
  - Identify the Member State Competent Authority assigning the authorisations

Secure interface must be implemented by March 2019

Qualified Certificates under PSD2

ETSI joint work with ECB ERPB PIS WG / Open Banking Europe

Qualified Certificate profiles

- PSD2 Qualified Website Authentication Certificates
- PSD2 Qualified Seal Certificates

CA 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

Published as TS 119 495 in May 2018

Developing Annex with EBA on information to Competent Authorities on how to supply authorisation information to CAs

Signature Validation

Signature Validation

Standards being developed:

- TS 119 102-2: Validation Report
- TS 119 441: Policy Requirements for TSPs Providing Signature Validation Services (including annex for qualified service)
- TS 119 442: Protocol for Signature Validation Services
- TS 119 172-4: Signature Validation Policy for European Qualified Electronic Signatures/Seals Using Trusted Lists

Signature Validation

Protocol features:

- Supports both XML and JSON exchanges
- Aligned with OASIS DSS

Timescale

- 10th January 2018: http://www.etsi.org/news-events/events/1222-2018-01-esignature-and-eseal-validation-workshop
- Approval of final of awaiting OASIS DSS validation protocol documents
- Publication: End 2018

Draft documents available to JNSA as ETSI member

Remote Signing

Remote Signing
CEN Standards for Trustworthy Systems

CEN standards for remote signing systems:

- EN 419 241-1: General System Requirements
- prEN 419 241-2: Protection Profile for QSCD for Server Signing
- EN 419 221-5: Cryptographic Module

Authentication can be delegated to an Identity Provider outside QSCD

Timescale:

- EN 419 241-1: Approved and Published
- prEN 419 241-2: Certification complete - Document available via CC portal soon
- EN 419 221-5: Approved and published

ETSI Signature Creation Protocols & TSP Component Policy Requirements

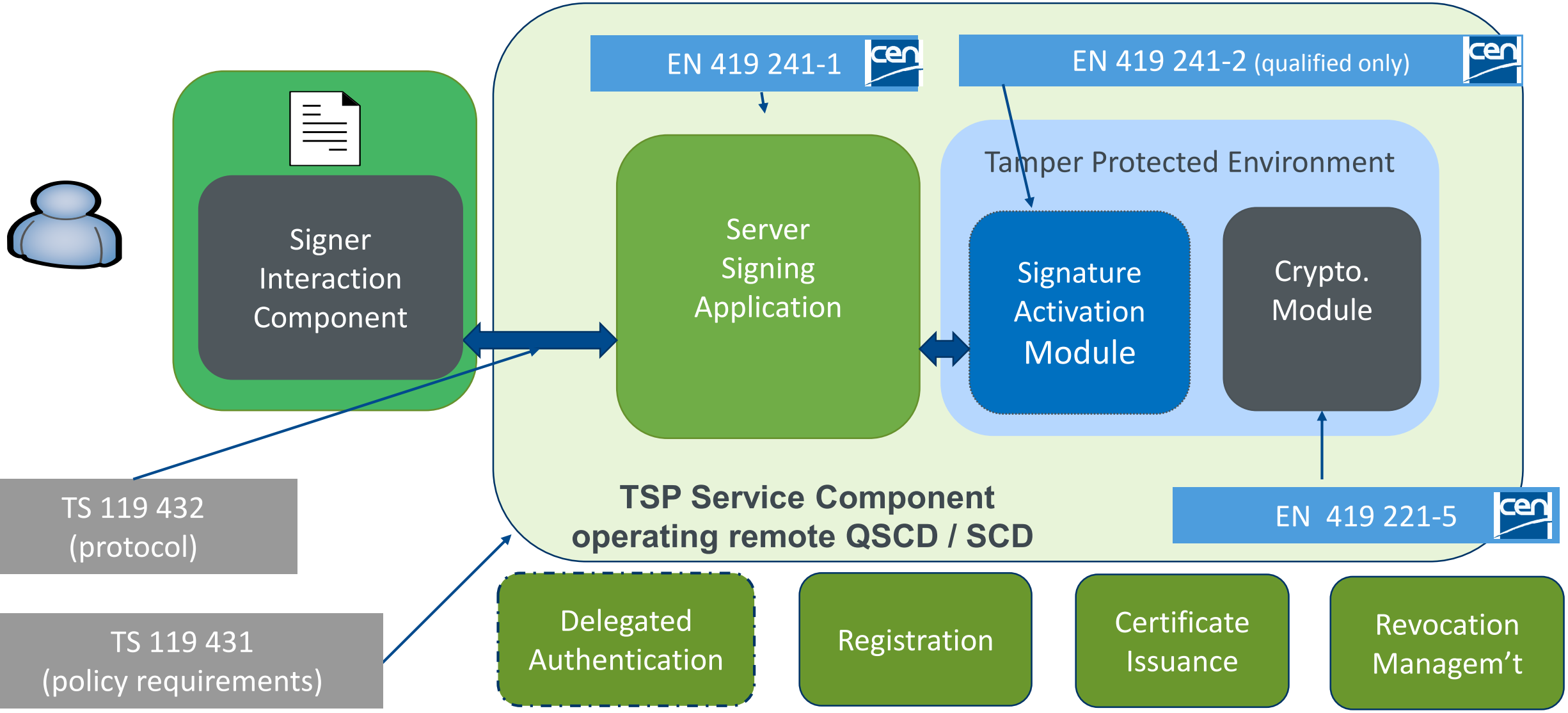
Standards being developed:

- 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

- Funded STF activity started: Oct 2017
- Stable draft for review: June 2018
  See https://docbox.etsi.org/ESI/Open/Latest_Drafts/
- Publication: Nov 2018

Scope of Remote Signing Standards



Electronic Registered Delivery & REM

Electronic Registered Delivery and Registered Electronic Mail

Standards for approval (on ENAP – European Standard Approval Procedure):

- EN 319 522: Electronic Registered Delivery Services
- EN 319 521: Policy and Security Requirements for Electronic Registered Delivery Service Providers

- EN 319 532: Registered Electronic Mail (REM) Services
  - Will supersede ETSI TS 102 640
- EN 319 531: Policy and Security Requirements for Registered Electronic Mail Service Providers

Electronic Registered Delivery and Registered Electronic Mail

Standards under development

- 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

Timescale

- End of ENAP's Public Enquiry: End August 2018
- ENAP's Weighted National Vote: From end November 2018 to January 2019
- ENs published: End February 2019

Electronic Registered Delivery and Registered Electronic Mail - Liaison

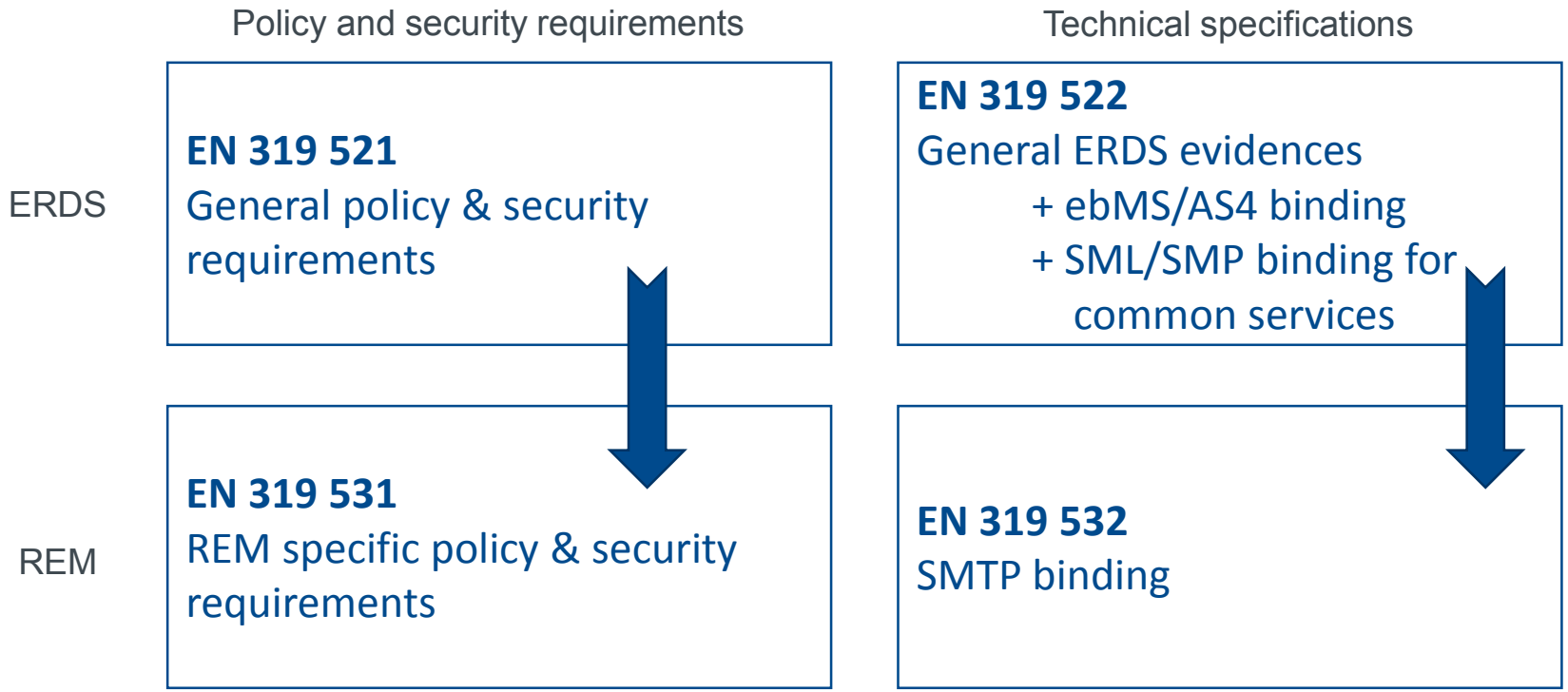
ESI has liaised with CEN TC 331/WG2 for properly dealing with CEN TS 16326 specifications on Postal Registered Electronic Mail (PrEM).

ESI has liaised with UPU (Universal Postal Union), as its S52 specification is the basis for CEN TS 16326, for properly dealing with the three sets of specifications.

ESI has liaised with CEF Digital, responsible for the eDelivery building block resulting from the EU large-scale pilots. ETSI standards have a broader scope but the CEF eDelivery building block may be used to implement services that conform to the ETSI standards.

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

Preservation

Long-Term (Signature) Preservation

Work started:

- TS 119 511 Policy and 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 summer 2018
- Publication end of 2018

Trusted Lists

Using Trusted Lists

Use of information within a Trusted List by relying parties

- How to process a trusted list in order to obtain information about a QTSP and the QTS/QTSs it provides
- For validating a qualified signature/seal (see also upcoming TS 119 172-4)
- To link trusted list information to evidences produced by some types of trust services: validation service, preservation service, electronic registered delivery services
- Complements TS 119 612

Timescale:

- Target publication: December 2018

TSP Audits

Supplements to EN 319 403 TSP Audit Requirements

Draft TS 119 403-2: Additional Requirements for Conformity Assessment Bodies Auditing TSPs that Issue Publicly-Trusted Certificates (e.g. as in CA/Browser Forum)

- Annual audit (versus bi-annually for eIDAS)
- Audit covers period of time since last audit
- Audit attestation requirements fitting web browser requirements

Published:

http://www.etsi.org/deliver/etsi_ts/119400_119499/11940302/01.01.01_60/ts_11940302v010101p.pdf

Supplements to EN 319 403 TSP Audit Requirements

Draft TS 119 403-3: Additional Requirements for CABs Assessing QTSPs against the eIDAS Regulation Requirements

- Auditor capabilities to carry out audits under eIDAS
- Required details included in conformity assessment report
- https://docbox.etsi.org/ESI/Open/Latest_Drafts/ESI-0019403-3v004-public.pdf

Stable draft distributed for public review:

https://docbox.etsi.org/ESI/Open/Latest_Drafts/ESI-0019403-3v004-public.pdf

Signature Algorithms

ETSI TS 119 312: Cryptographic suites V1.2.2 (2018-09)

Since 2003 ETSI TC publishes suitable algorithms and parameters for digital signatures ("Algo Paper")

Main focus:

- Security for a given time: short and mid term
- Interoperability: list widely deployed algorithms and their OIDs
- https://portal.etsi.org (search for "119312")

Latest version bases on the SOG-IS list of agreed cryptographic mechanism

- https://sogis.org/uk/supporting_doc_en.html (version 1.1)

ETSI TS 119 312: Algorithms and Parameters

RSA

- PKCS#1v1.5: only until end of 2022
- PSA-PSS: key length less than 3000 bit only until 2024
- Key generation with seed entropy of at least 125 bit

Elliptic Curve Cryptography

- Dedicated curves with 256, 384, 512 and 521 bit key length
- EC-DSA, EC-GDSA, EC-KCDSA, EC-SDSA

Hash functions

- SHA-256, SHA-384, SHA-512 (SHA-224 only until 2022)
- SHA3-256, SHA3-384, SHA3-512

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:
Subscribe on the mailing list

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