The Standards People

ETSI ESI and Signature Validation Services

Presented by: **Andrea Röck – Universign and ETSI STF 524 expert**

For: **CA day**

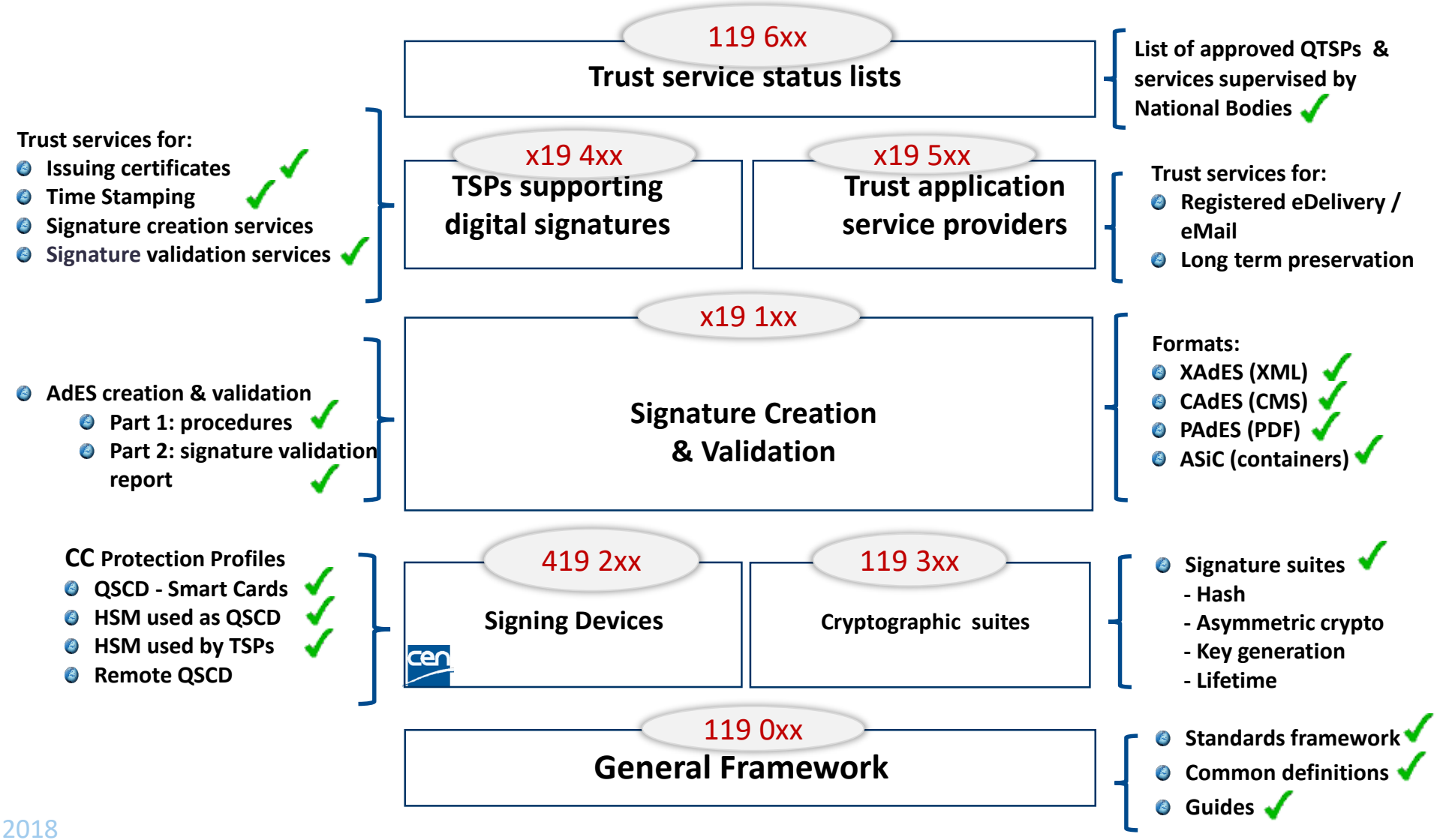
24.10.2018

Agenda

- Update on standardisation under eIDAS
- Signature validation service

Update on standardisation under eIDAS

eIDAS Standards Framework: Published Standards



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)

ETSI policies acknowledged by, and incorporating major requirements of, CA/B forum

- 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

Qualified Certificates under PSD2

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

To fulfil need from Commission Delegated Regulation (EU) 2018/389:

- 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

Update taking into account input from European Banking Authority under final review expected publication November

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 awaiting publication
- EN 419 241-2: Technically Approved under Common Criteria awaiting final CEN approval and publication
- EN 419 221-5: Approved and published

Remote signing ETSI Signature Creation Protocols & TSP Component Policy Requirements

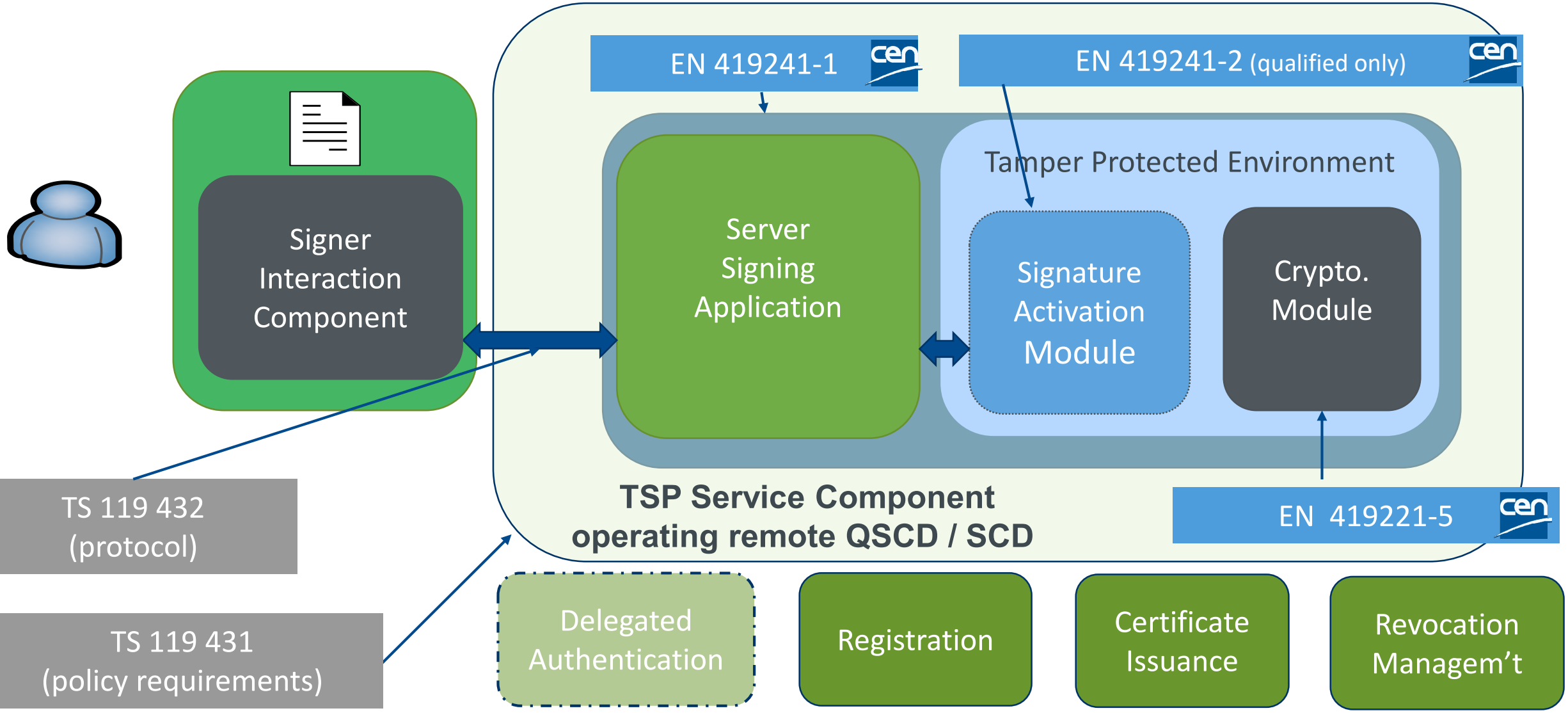
Standards being developed:

- 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

- TS 119 431-1 and TS 119 431-2 publication Nov 2018
- TS 119 432 depends on OASIS DSS-X and CSC 1.0, publication Jan 2019

Scope of Remote Signing Standards



Electronic Registered Delivery and Registered Electronic Mail

Published standards:

- ETSI EN 319 522: Electronic Registered Delivery Services
- ETSI EN 319 532: Registered Electronic Mail (REM) Services (Supersedes ETSI TS 102 640)

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

- ETSI EN 319 521: Policy and Security Requirements for Electronic Registered Delivery Service Providers
- ETSI EN 319 531: Policy and Security Requirements for Registered Electronic Mail Service Providers

Standards under development

- ETSI TS 119 524 / ETSI TS 119 524 Testing Conformance and Interoperability for eDelivery/REM
- ETSI TR 119 500 Business Driven Guidance for Trust Application Service Providers

Timescale: ENs & TS & TR published: End February 2019

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 general data using digital signature techniques
- TS 119 512 Protocols for trust service providers providing long-term data preservation services

Timescale:

- Stable draft for review end of 2018
- Publication: Beginning of 2019

Using Trusted Lists

Standards under development

- TS 119 615
  - on the 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 QTS(s) it provides
  - Building blocks
    - 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: Beginning 2019

Supplements to EN 319 403 TSP Audit Requirements

TS 119 403-2: Part 2: Additional requirements for Conformity Assessment Bodies auditing Trust Service Providers 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: https://www.etsi.org/standards-search#search=TS119403-2

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 reportTimescale:

- Timescale: Publication January 2019

Machine-processable signature policy formats

Machine-processable signature policy formats

- TS 119 172-2: XML format for signature policies
- TS 119 172-3: ASN.1 format for signature policies
- Timescale:
  - Drafts for public review: June 2019
  - Published: End November 2019

Global acceptance of European Trust Services

- Study report on Global Acceptance of EU Trust Services
  - Analysis of international, regional and sector specific communities adopting Public Key Infrastructure technology
- International co-hosted workshops:
  - Target regions; Japan, North America, South America, Africa

Signature Validation Service

ETSI STF 524

Standards for eIDAS trust services including electronic signatures – trust services for validation

- Started in 2016
- Three documents
  - 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
- Workshop 10/01/2018

ETSI TS 119 102-2: Validation Report

- **Published:** https://www.etsi.org/standards-search#search=TS119102-2
- Preparation of update correcting small XML scheme errors
- No longer relies on OASIS (based on feedback from workshop and on TB ESI assessment)
- To be used by validation service but also outside of a service

ETSI TS 119 441: Policy Requirements for TSPs Providing Signature Validation Services

- Published: https://www.etsi.org/standards-search#search=TS119441
- Based on ETSI EN 319 401
- General part EU independent
- Normative annex for requirements for qualified validation service for qualified electronic signatures/seals
- Informative mapping to eIDAS requirements
- Checklist for self-assessment or independent conformity assessment
- Clarifies relation between
  - signature validation policy: set of (technical) validation constraints
  - signature applicability rules: requirements for determination of whether a signature is fit for a particular business or legal purpose

ETSI TS 119 442: Protocol for Signature Validation Services

Protocol features:

- Supports both XML and JSON exchanges
- Aligned with OASIS DSS V2.0
- Supports validation, augmentation and augmentation with validation

Timescale

- Publication: January 2019 (delayed to align with OASIS DSS v2 publication)

Related documents

Validation plugtest

- Planned for Q2 2019

ETSI TS 119 102-1 AdES digital signatures creation and validation

- Updated version published August 2018 to be aligned to work of STF
- EN approval procedure only after plugtest

ETSI TS 119 172-4 Signature Validation Policy for European Qualified Electronic Signatures/Seals Using Trusted Lists

- Timescale: Publication March 2019

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

STF 524 on validation:
https://portal.etsi.org/STF/stfs/STFHomePages/STF524