Where do we stand on standards for Remote Signature Creation ?

Presented by: **Nick Pope**

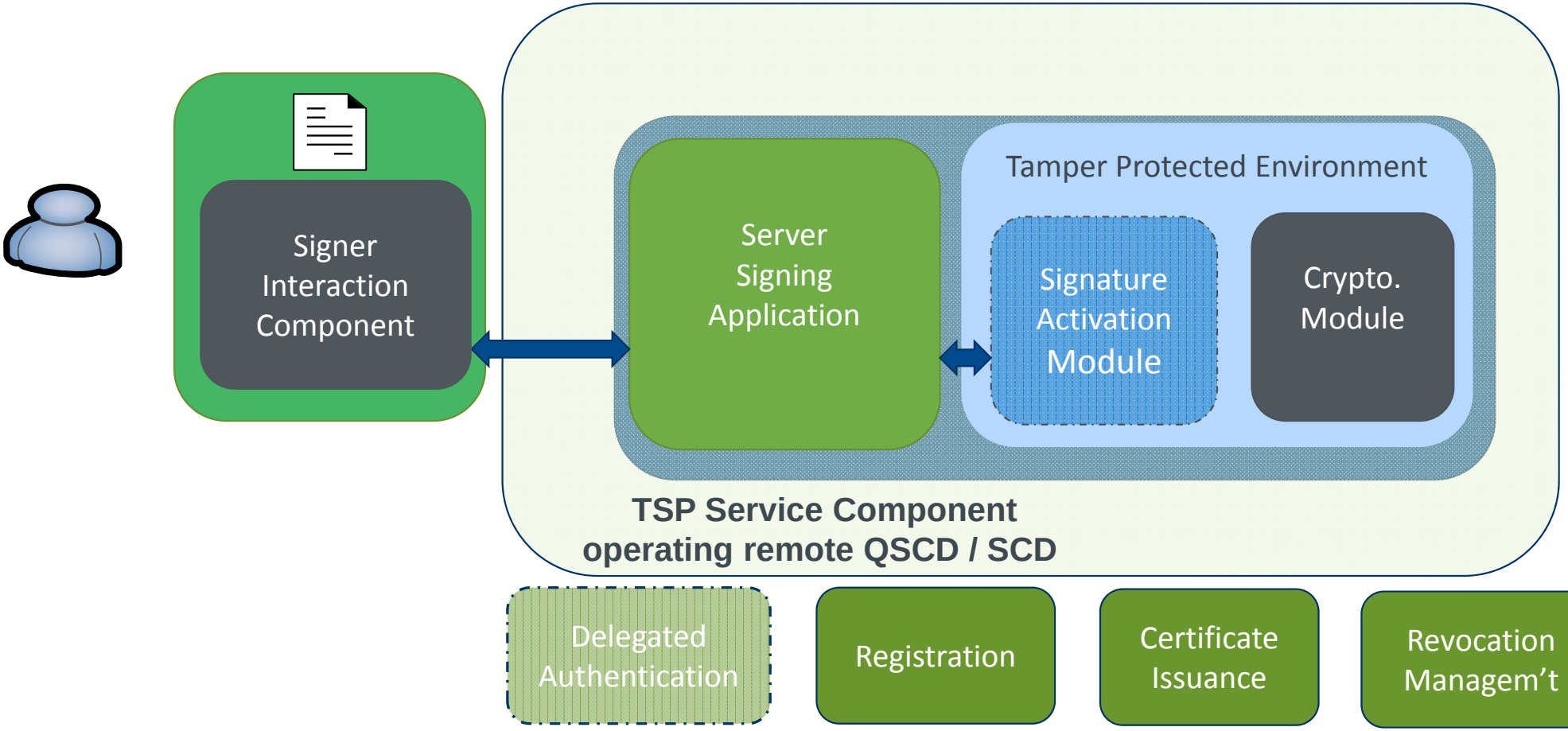
For: **ETSI Security Week: Remote Signature Creation Services**

13.6.2018

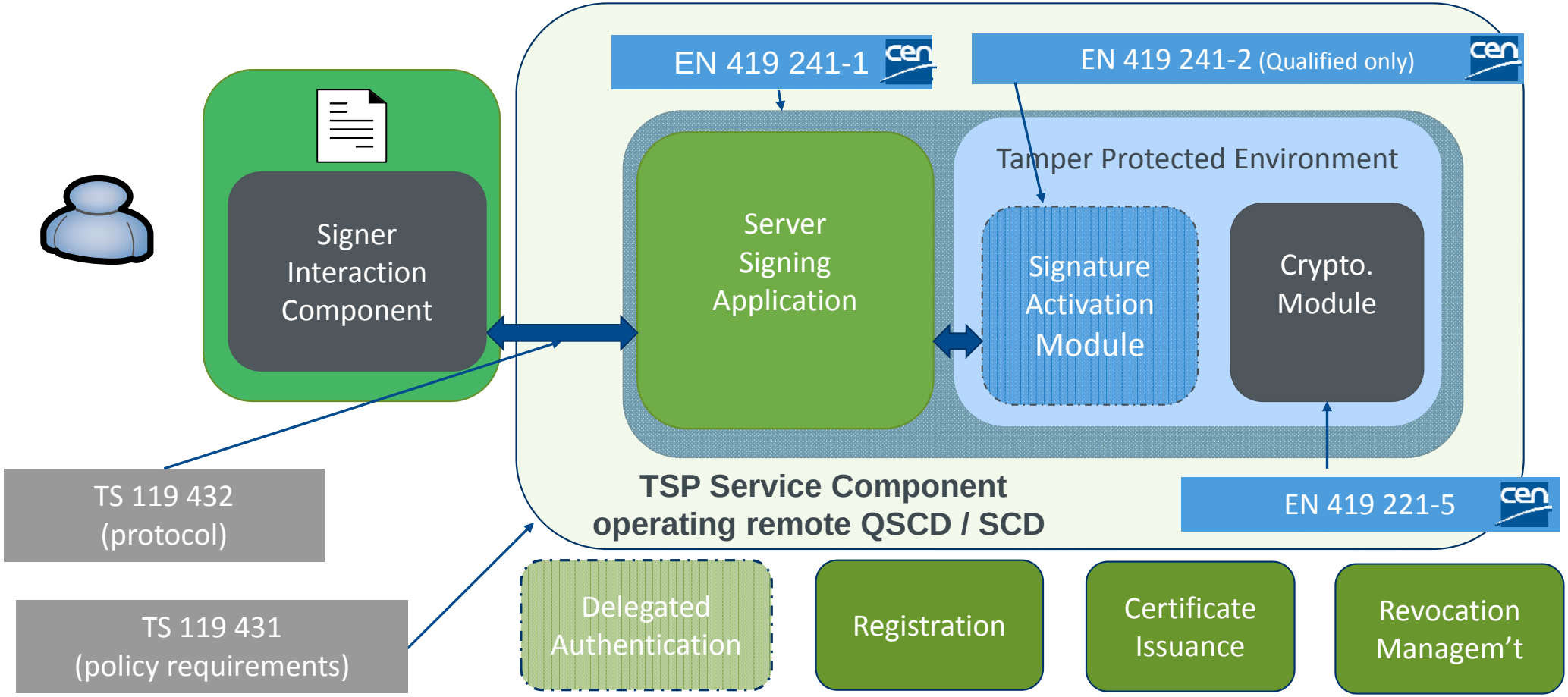
Agenda

- Model for remote signing standards
- Status of CEN Standards
- Status of ETSI standards
- TSP vs Component Services

Model for remote signing



Scope of remote signing standards



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: final stages of certification due summer 2018
- EN 419 221-5: Approved and published

ETSI Signature Creation Protocols & 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
- Publication: Nov 2018

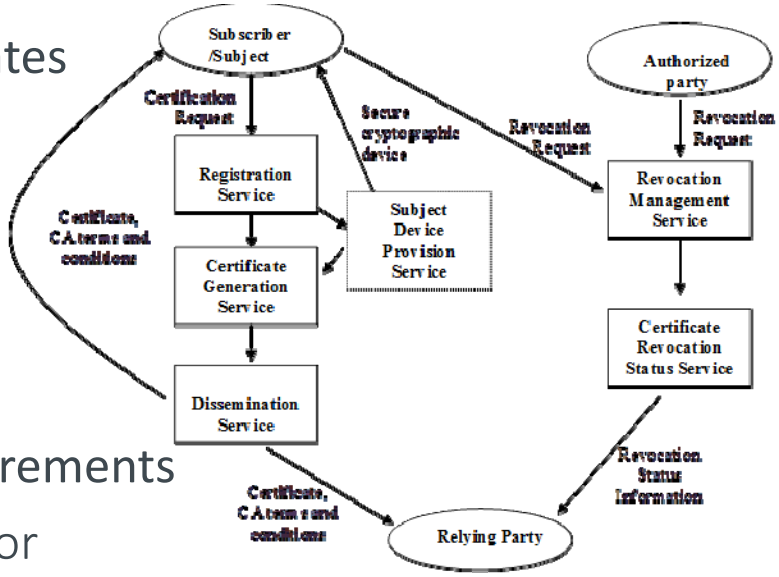
TSP vs Component Services

TSP – Entity that has overall responsibility for provision of a trust service to its users

TSP may involve a number of component services

e.g. EN 319 411-1 Components of TSP Issuing Certificates

- Registration
- Certificate generation
- Revocation management
- …



Each service component has its own well defined requirements

- Requirements specific to the service component, or
- Requirements applicable across TSP

Remote Signature Creation and eIDAS regulation

- eIDAS does not recognise Remote Signature Creation as an independent Trust Service
- Proposal to develop standard for independent Trust Service for Signature Creation rejected
- Remote Signature Creation provided as an adjunct to other trust services
  - Certificate issuance
  - Time-stamping
  - Signature validation

Component Service for Remote Signature Creation

- Independent set of policy requirements
  - Requirements common to all trust services (EN 319 401)
  - Requirements specific to remote signing
  - Requirements relating to signer (delegated) authentication (c.f. eIDAS electronic identity)
  - Requirements relating to interaction with other component services
    - Certificate registration and proof of control over signing key
    - Certificate revocation and deletion of signing key

TSP providing Remote Signature Creation must ensure all policy requirements are met

TSP Audit and “outsourcing” component service audit

- **TSP Audit must demonstrate that all requirements are met but ..**
- TSP Audit may “outsource” audit on component service under EN 319 403 through ISO 17065 clause 7.4.5:
  “The certification body shall only rely on evaluation results related to certification completed prior to the application for certification, where it takes responsibility for the results and satisfies itself that the body that performed the evaluation fulfils the requirements contained in 6.2.2 (outsourcing) and those specified by the certification scheme.”