Remote signing

Presented by: Andrea Röck (Universign)       For: ETSI Standards Training Webinar

01.06.2021
Agenda for Preservation

- Standards on the different remote signing components
- CEN EN 419 241: Trustworthy Systems Supporting Server Signing
- Signature activation system with SCAL1
- Signature activation system with SCAL2
- ETSI TS 119 431-1
- ETSI TS 119 431-2
- ETSI TS 119 432
- Cloud Signature Consortium (CSC) specification
Standards on the different remote signing components

Signer Interaction Component

Server Signing Application

Signature Activation Module

Crypto. Module

Tamper Protected Environment

TSP Service Component operating remote QSCD / SCD

EN 419 241-1

EN 419 241-2 (Qualified only)

EN 419 221-5

Delegated Authentication

Registration

Certificate Issuance

Revocation Management

TS 119 432 (protocol)

TS 119 431 (policy requirements)
Part 1: General System Security Requirements

Part 2: Protection Profile for QSCD for Server Signing

Defines two different Sole Control Assurance Level [CEN EN 319 419-1]

SCAL1:
- The signing keys are used, with a low level of confidence, under the sole control of the signer.
- The authorized signer’s use of its key for signing is enforced by the server signing applications which authenticates the signer.

SCAL2:
- The signing keys are used, with a high level of confidence, under the sole control of the signer.
- The authorized signer’s use of its key for signing is enforced by the Signature Activation Module (SAM) by means of Signature Activation Data (SAD) provided, by the signer, using the Signature Activation Protocol (SAP), in order to enable the use of the corresponding signing key.
- Aiming to support qualified electronic signatures
Signature activation system with SCAL1

CEN EN 419 241-1: Figure 2
CEN EN 419 241-1: Figure 3

- Signature activation data shall link
  - DTBS/R
  - Authenticated signer
  - Key to be used
Policy and security requirements for Trust Service Providers (TSP) implementing a service component operating a remote signature creation device (SCDev)

Server Signing Application Service Component (SSASC)

Based on requirements in CEN EN 419 241-1

Defines three SSASC policies

- **LSCP**: Lightweight SSASC Policy (less demanding than NSCP, linked to SCAL1)
- **NSCP**: Normalized SSASC Policy (general recognized best practice, linked to SCA2)
- **EUSCP**: EU SSASC Policy (linked to eIDAS regulation with specific requirements to QSCD management)

Handles the cryptographic signature
provides policy and security requirements for trust service providers (TSP) implementing a service component supporting AdES digital signature creation

signature creation application service component (SCASC)
Protocol for remote signing

Allows creation of cryptographic signature to be used by an SSASC

Allows creation of AdES signature to be used by an SCASC

Does not cover the creation of the SAD (not just SCAL2 but signature activation data in a more general sense) but uses the SAD as input

Defines main functionality and semantic of the protocol

Allows for symmetric and asymmetric calls

Defines two different implementations

- JSON: based on Cloud Signature Consortium specification
- XML: based on OASIS DSS-X
Cloud Signature Consortium (CSC) specification

- https://cloudsignatureconsortium.org/
- V1.0 was published in 2018
- V2.0 is in work (planned to be published in 2021)
- A protocol for remote signing based on JSON and REST API
- V1.0 version only covers creation of cryptographic signatures on hash
- In addition to ETSI TS 119 432, it also covers mechanisms to create the SAM
- Very flexible protocol, that allows the signing application to discover which specific functionalities a server signing application supports
- V2.0 will contain features of ETSI TS 119 432 (AdES signatures, asynchrony calls) and more possibilities for the credential authorization