Audit Requirements for TSPs Operating a Remote QSCD / SCD

Presented by: **Franck Leroy**

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

13.6.2018

TS 119 431-1

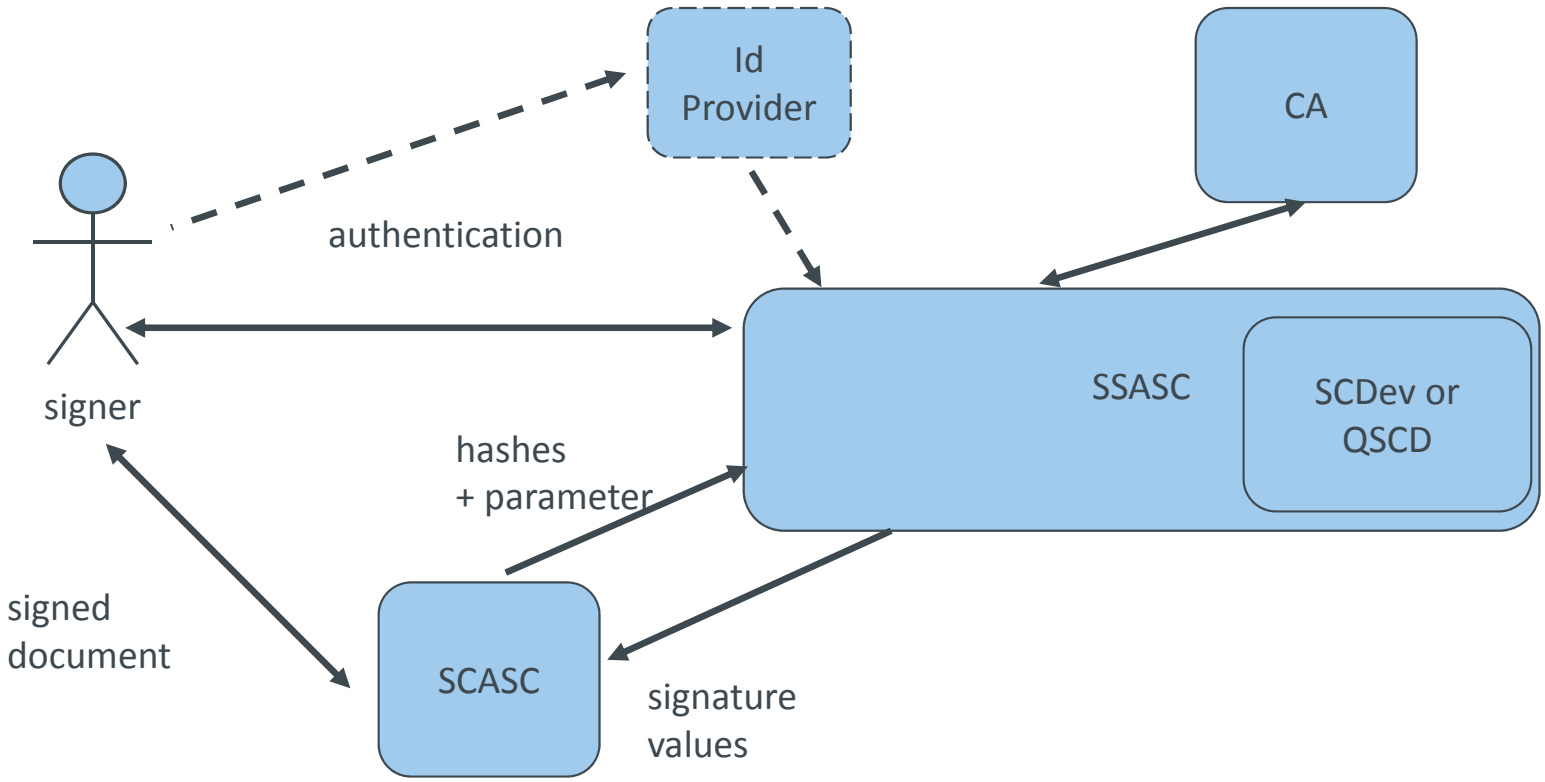
Policy and security requirements for trust service providers; TSP service components operating a remote QSCD / SCDev

- Based on ETSI EN 319 401 (General Policy Requirements for Trust Service Providers)
- References to some requirements of ETSI EN 319 411-1 (Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements)
- References to many requirements of CEN EN 419 241-1 (Trustworthy Systems Supporting Server Signing Part 1: General System Security Requirements)

Server signing application service component (SSASC)

- In combination with a signature creation device (SCDev)
- Specifics requirements for uses of an qualified signature creation device (QSCD)
- Creates/manages signing keys
- Binds authentication means and certificates to the signing keys.
- Authenticates remote signers
- Creates the digital signature (i.e. PKCS#1)

Architecture (example)



Different trust service policies

Policies defined in the document

- A Lightweight SSASC Policy (LSCP) offering a quality of service less onerous than the normalized one
- A Normalized SSASC Policy (NSCP) which meets general recognized best practice for TSPs operating a remote QSCD / SCDev
- An EU Qualified SSASC Policy (EUQSCP) which offers the same quality as that offered by the NSCP but with specific requirements related to the European eIDAS Regulation

Relations with CEN EN 419 241 series

- Lightweight Policy is related to Sole Control Level 1 of CEN 419 241 part 1
- Normalized Policy is related to Sole Control Level 2 of CEN 419 241 part 1
- EU Qualified Policy requires QSCD
  - could be met by using CEN 419 241 part 2

eIDAS Challenges

- Not a standalone policy
- It's an additional component to an existing TSP
- The TSP is not mandatory the CA
- But strong relation with the CA is needed

- The main challenge is to ensure that the remote signer is the same person that the one that has been enrolled by the CA