The Standards People

Audit Requirements for TSPs Supporting AdES Digital Signature Creation

Presented by: **Andrea Röck**

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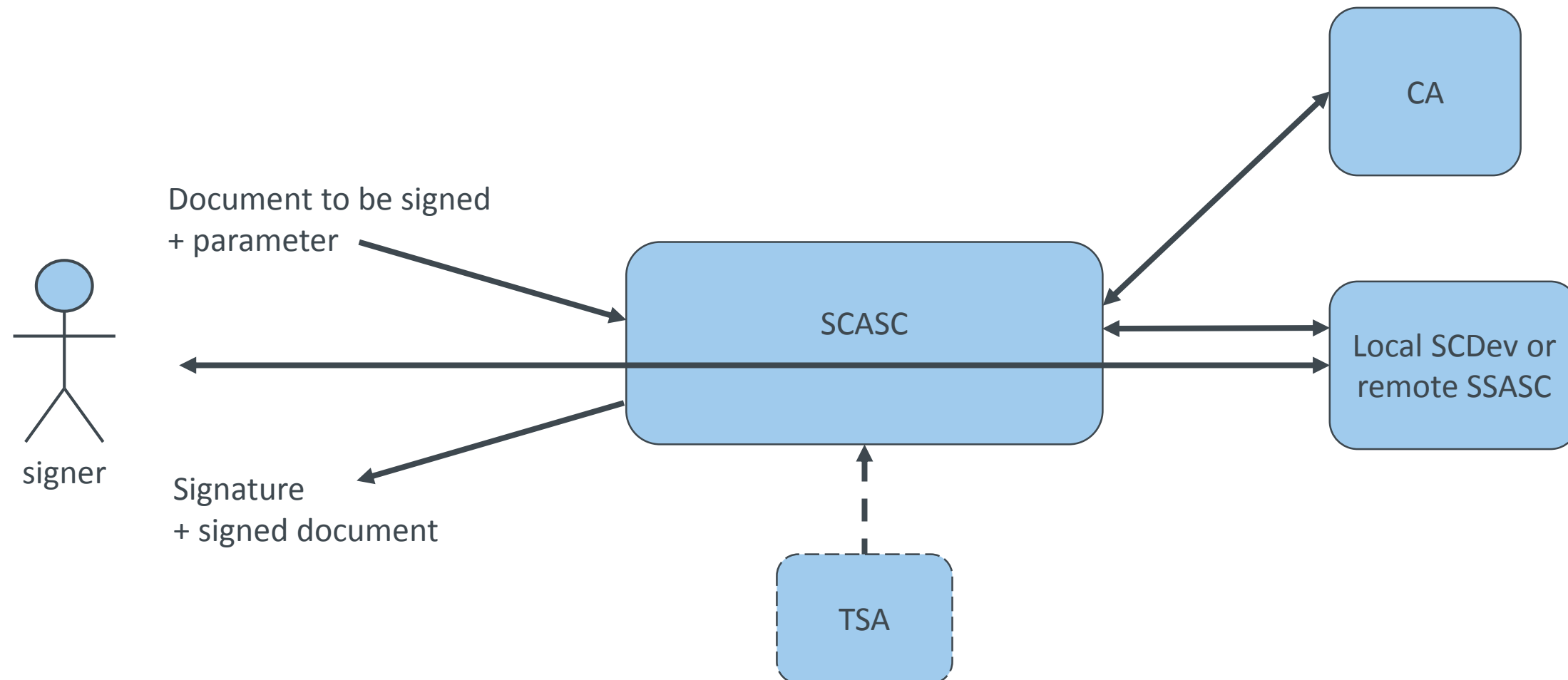Remote Signature Creation Services**

13.6.2018

TS 119 431-2

Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation

- ◊ Based on EN 319 401 (General Policy Requirements for Trust Service Providers)

- ◊ References to some requirements of TS 119 101 (Policy and security requirements for applications for signature creation and signature validation)

Signature creation application service component (SCASC)

- Not necessarily in combination with a server signing application service component (SSASC)

- Creates the (C/X/P)AdES signature

- Can provide presentation of document to be signed

Architecture

signer

Document to be signed + parameter

Signature + signed document

SCASC

CA

Local SCDev or remote SSASC

TSA

Documentation

Documents

- Terms & conditions

- SCASC practice statements

Shall state the supported

- Signature creation policies

- Signature parameters

- Signature formats

- Signature classes

- Remote SSASC or local signature creation device (SCDev)

Different trust service policies

Policies defined in the document

- Main policy

- EU advanced electronic signature / seal

  - The certificate shall represent the signer
  - The certificate shall be included in the signature

- EU qualified electronic signature / seal

  - For the moment not clear if this has any specific requirements

The EU specific ones aim at fulfilling the requirements of the regulation

Informative annex for mapping to regulation

Presentation of the document to be signed

∇ Optional feature of the SCASC

∇ Conditional requirements

∇ Goal is to make sure that the signer is aware of what he/she is signing