Potential
For European Digital Identity

Co-funded by
the European Union

Qualified eSignature

# Activation of a remote QES using OID4VP and transaction_data

Mark Ullmann,
LSP Potential Use Case 5 DE

08/08/2024

# Remote Qualified Electronic Signature

Creation of a Qualified Electronic Signature needs two Wallet functionalities:

## Signer Identification (on LoA high)

- for creating a **certificate** for the signer

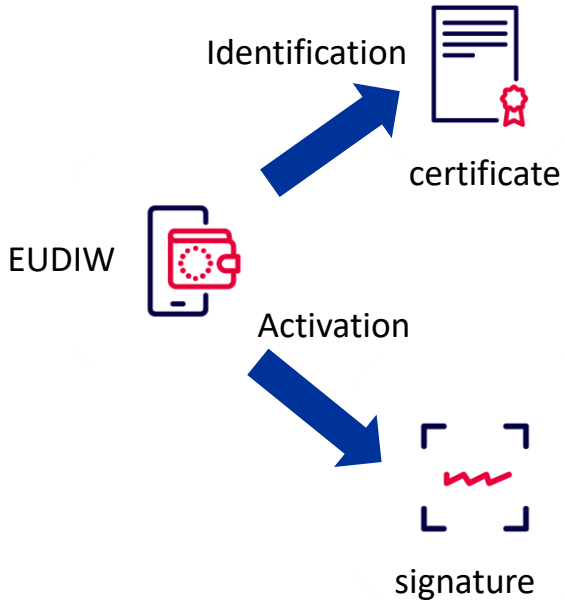
⇒ using PID presentation of the Wallet

## Signature Activation (with SCAL2)

- for creating an electronic **signature** for a document

⇒ using PID/Credential presentation with transaction_data of the Wallet

Note: Some models for QES with the EUDIW require more functionality, but this is less relevant to OID4VP.






Potential
For European Digital Identity
Co-funded by the European Union

# Activation of a qualified electronic signature needs “sole control assurance level 2” (SCAL2)

## Activation: Sole Control Assurance Level 2 (SCAL2)

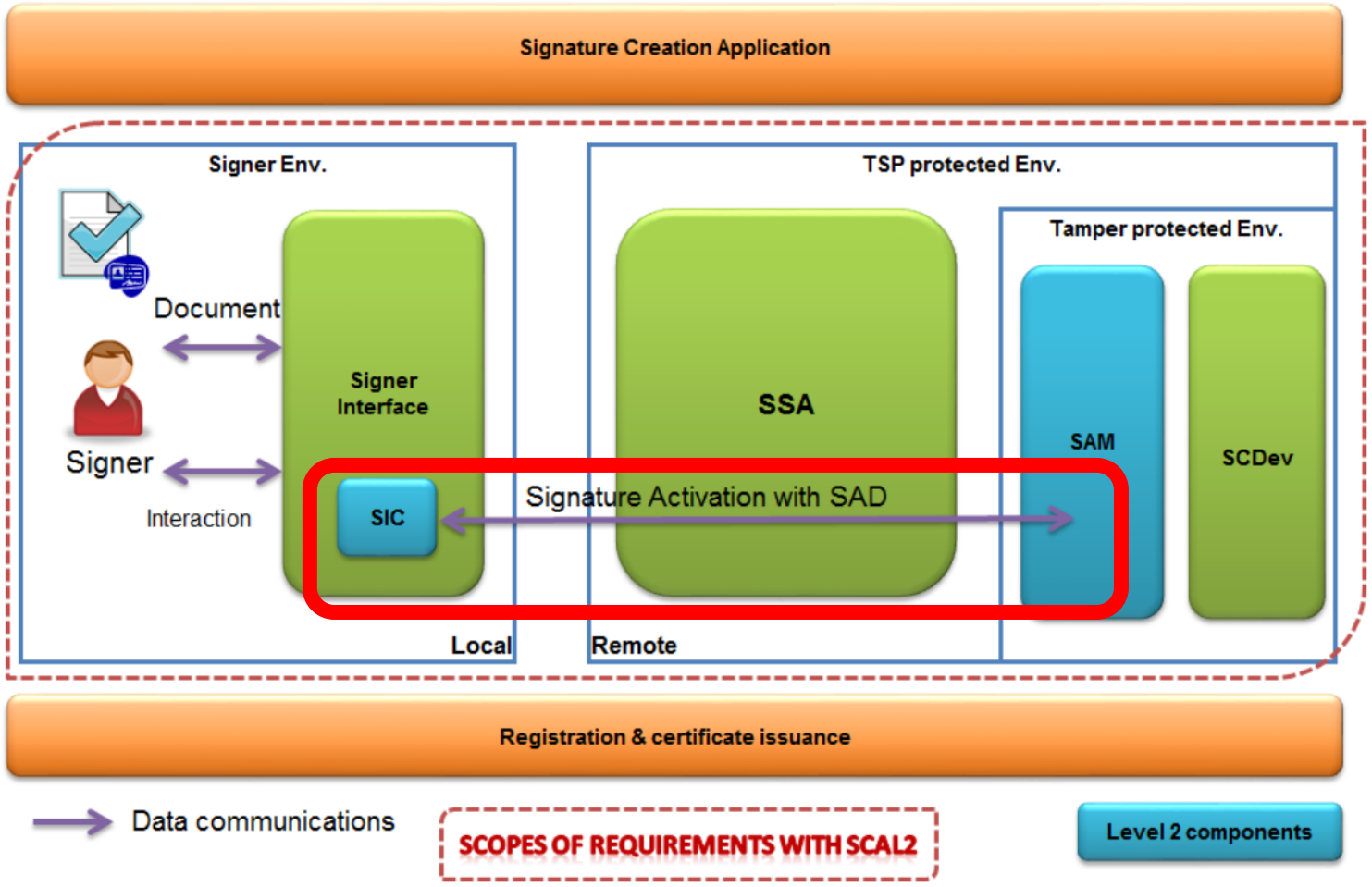



**Figure 3 — Signature activation system with SCAL2*)**

SSA: Server Signing Application
SAD: Signature Activation Data
SAP: Signature Activation Protocol
SAM: Signature Activation Module
SCDev: Signature Creation Device
TSP: Trust Service Provider
SIC: Signer‘s Interaction Component
QTSP: Qualified TSP

*) Source: CEN EN 419 241-1:2018 Trustworthy Systems Supporting Server Signing – Part 1: General System Security Requirements

Potential ...pean Digital Identity
Co-funded by the European Union

# Signature Activation Data

- Signature Activation Data needs to link three items: (CEN EN 419 241-1, SRA_SAP.2)
  - a given DTBS/R or a set of DTBS/R, (“the document”)
  - items to identify the authenticated signer, and (“the identity of the signer”)
  - default or selected signing key. (“the certificate”)

- transaction_data can satisfy these:
  - a credential or PID is transferred
  - transaction_data can contain a reference to DTBS/R or similar
  - transaction_data can contain a reference to the certificate
  - these need to be bound together

  } 
  - following requirements of QTSP
  - depending on certification of SAM

⇒ If source Wallet is certified, a QTSP can integrate this into their certification requirement from CEN EN 419 241-1 for their remote signature service.



Potential For European Digital Identity
Co-funded by the European Union

# Example transaction_data for qes_authorization


```
{
  "type": "qes_authorization",
  "signatureQualifier": "eu_eidas_qes",
  "credentialID": "oEovC2EHFiEFrDpUx8mR0o7yeGHk2h74b3XywkNgBGo=",
  "documentDigests": [
    {
      "label": "Example Contract",
      "hash": "sTOgwOm+474gFj0q0x1iSNspKqbcse4IeiqlDg/HWuI=",
      "hashAlgorithmOID": "2.16.840.1.101.3.4.2.1",
      "documentLocations_uri": "https://protected.rp.example/contract-
01.pdf?token=HS9naJKWwp901hBcK348IUHiuH8374",
      "documentLocation_method": {
        "method": {
          "type": "public"
        }
      },
      "dtbsr": "VYDl4oTeJ5TmIPCXKdTX1MSWRLI9CKYcyMRz6xlaGg",
      "dtbsrHashAlgorithmOID": "2.16.840.1.101.3.4.2.1"
    }
  ],
  "processID": "eOZ6UwXyeFLK98Do51x33fmuv4OqAz5Zc4lshKNtEgQ="
}
```

Thank you.

Dr. Mark Ullmann, Bundesdruckerei/D-Trust
Mark.Ullmann@bdr.de



Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or of the European Health and Digital Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.