OBSERWATORIUM.BIZ

Qualified Electronic Signature for the wallet

Michał Tabor

10th Trust Services and eID Forum

Anniversary

25th September 2024

16th CA-Day

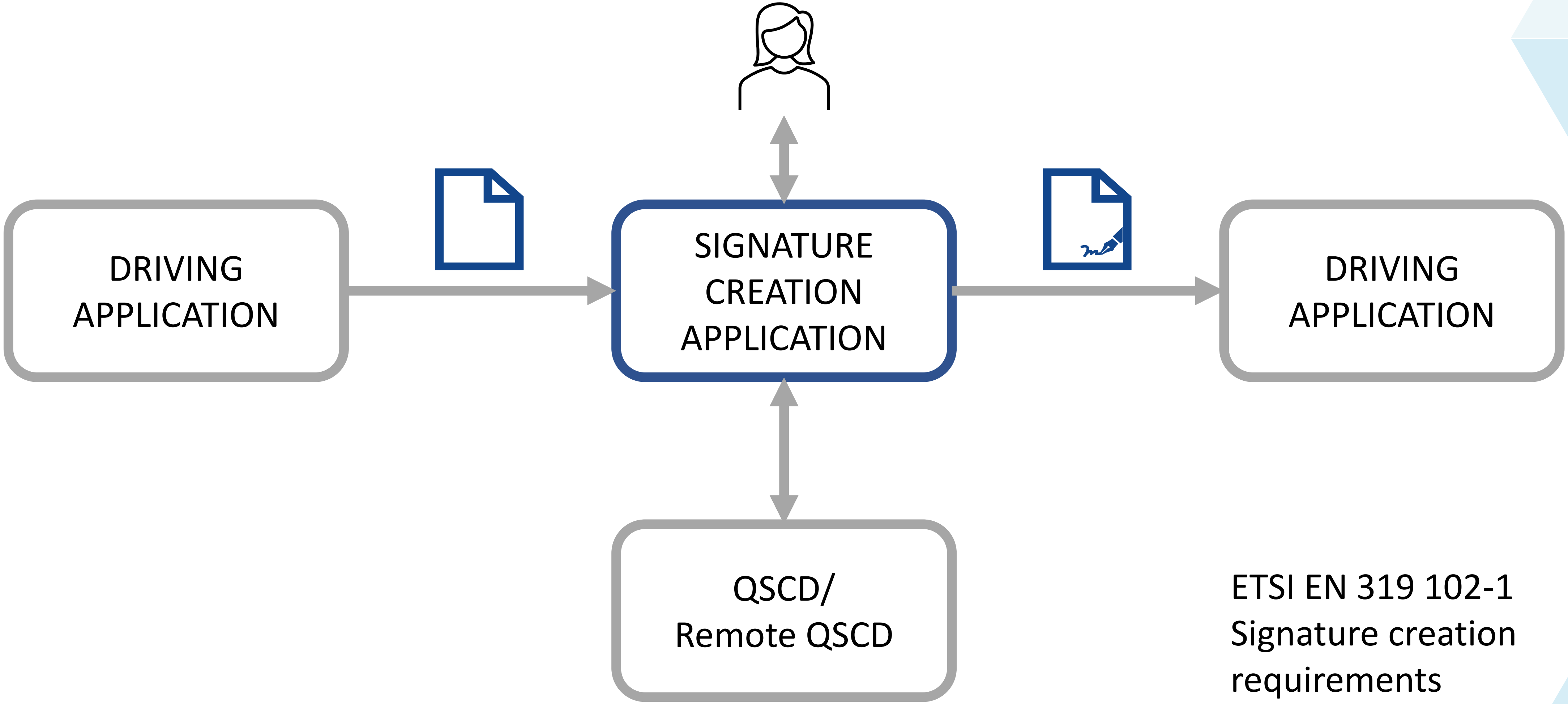
26th September 2024

HERAKLION, GREECE | ONLINE

Co-organised by

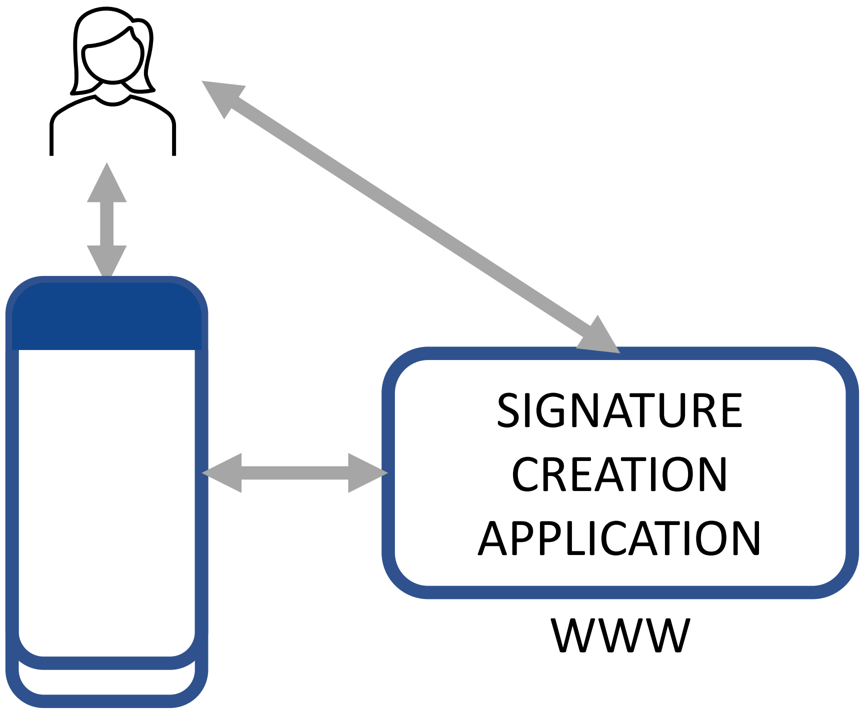
enisa
20 years!
European Commission
TÜVIT
TÜVNORDGROUP
d-trust.

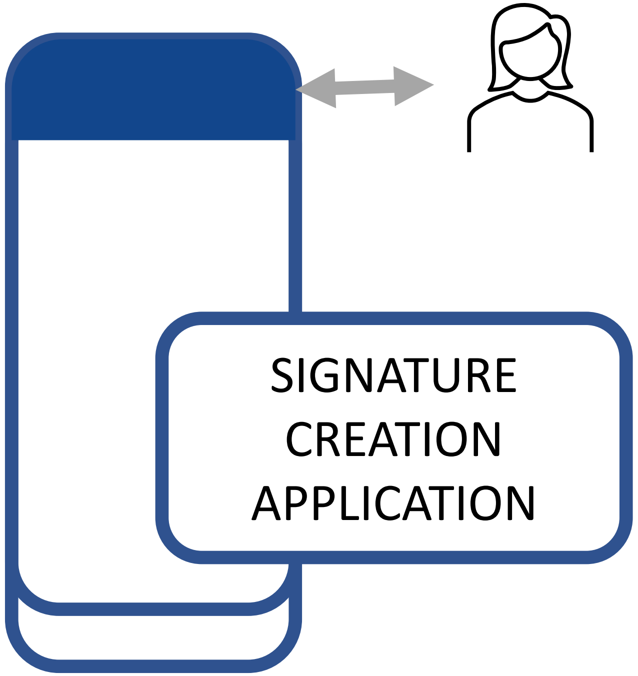
Signature Creation Application



ETSI EN 319 102-1
Signature creation
requirements

Signature Creation Application models

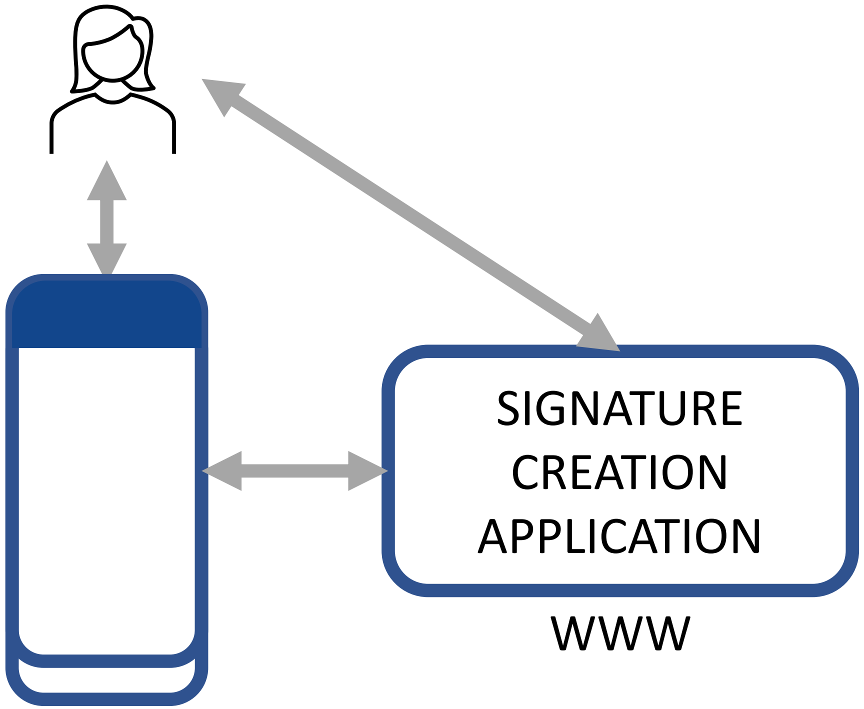




SCA as a service independent from the wallet solution

SCA as software included or connected to the wallet solution directly

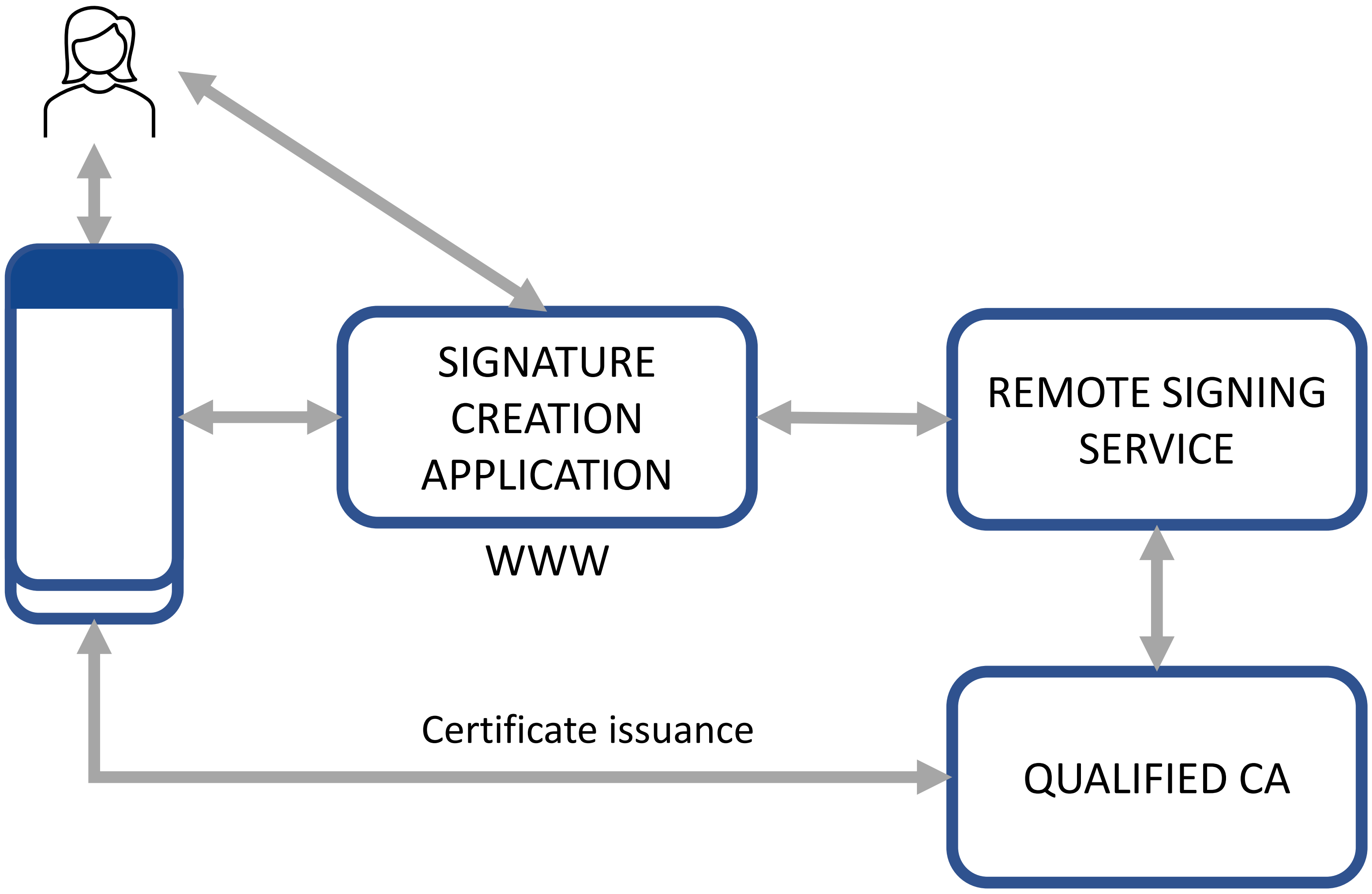
Independent SCA



SIGNATURE CREATION APPLICATION

WWW

Remote QES with the wallet



SIGNATURE CREATION APPLICATION

WWW

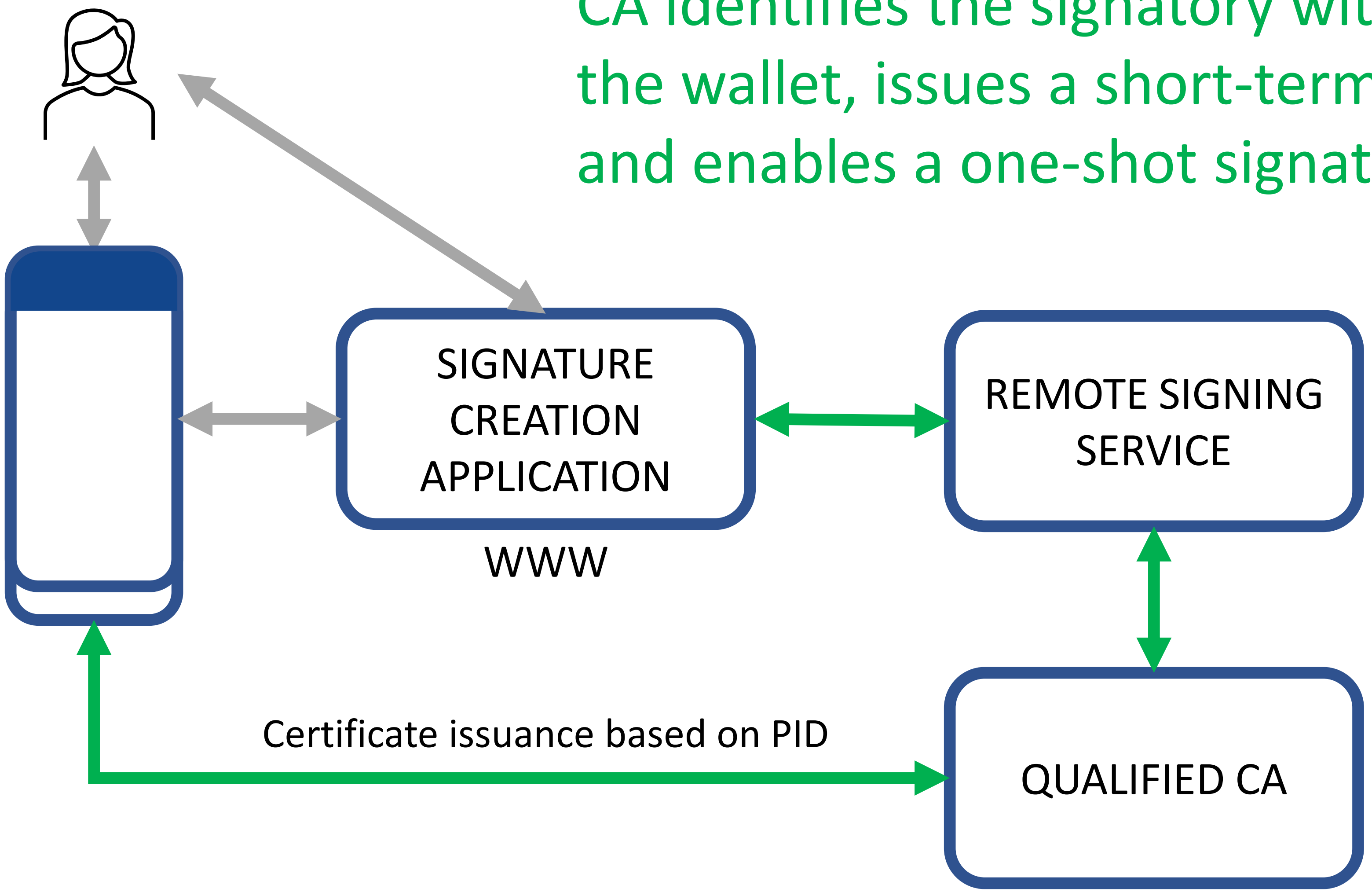
REMOTE SIGNING SERVICE

QUALIFIED CA

Certificate issuance

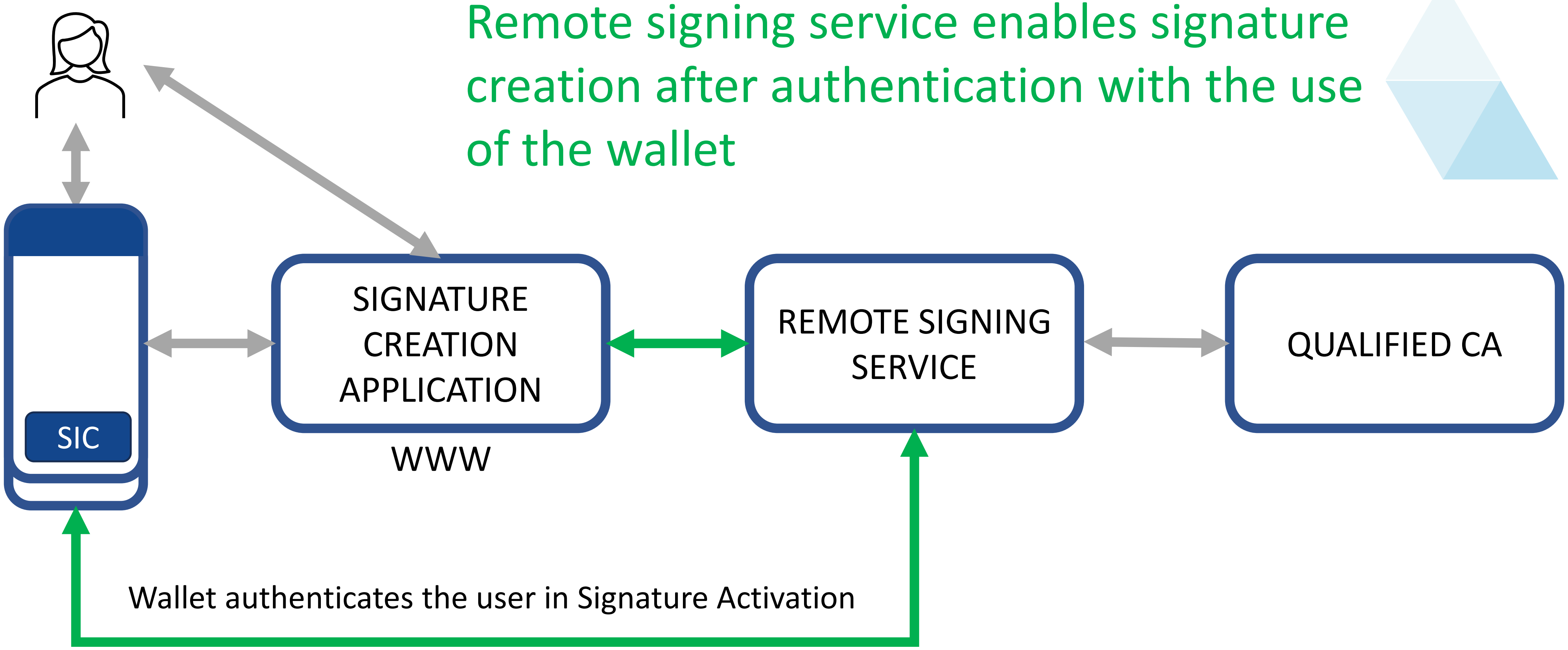
Remote QES on the fly

CA identifies the signatory with PID on the wallet, issues a short-term certificate, and enables a one-shot signature


SIGNATURE CREATION APPLICATION
WWW
REMOTE SIGNING SERVICE
QUALIFIED CA
Certificate issuance based on PID

Remote QES with long term certificate

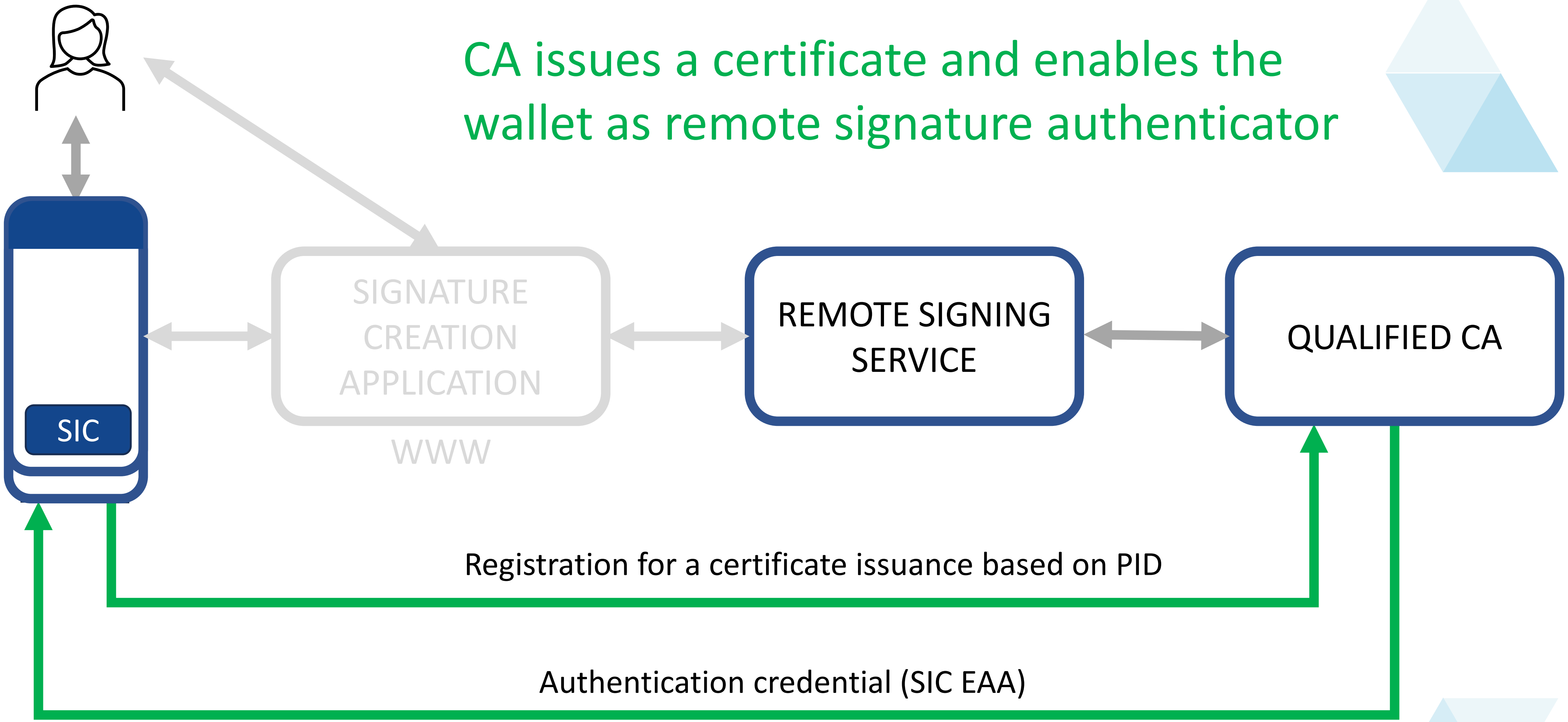
Remote signing service enables signature creation after authentication with the use of the wallet



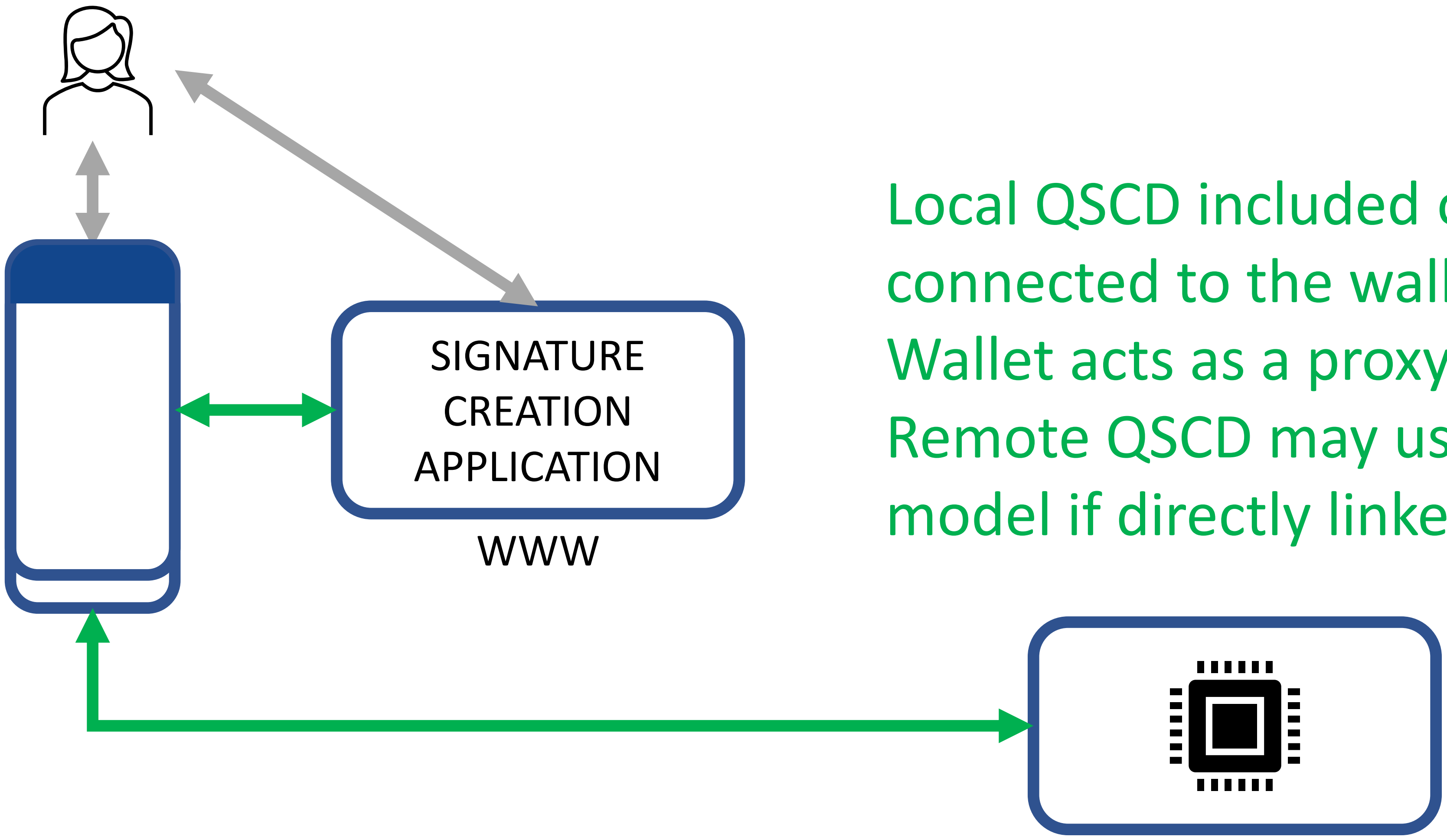
Wallet authenticates the user in Signature Activation

Long term Remote QES certificate issuance

CA issues a certificate and enables the wallet as remote signature authenticator


SIC
SIGNATURE CREATION APPLICATION
WWW
REMOTE SIGNING SERVICE
QUALIFIED CA
Registration for a certificate issuance based on PID
Authentication credential (SIC EAA)

Local (and remote) signature



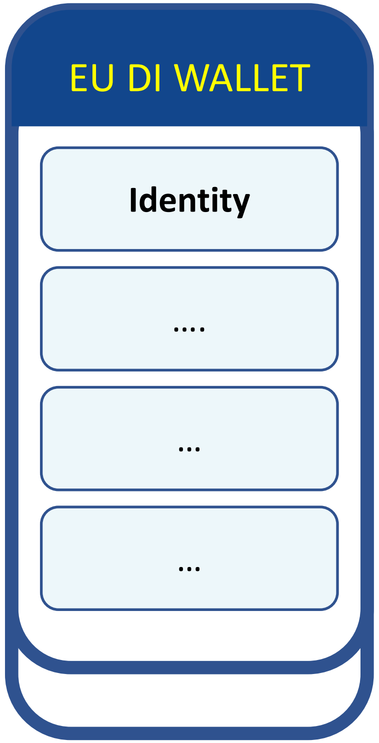
Local QSCD included or connected to the wallet directly.

Wallet acts as a proxy for QSCD

Remote QSCD may use the same model if directly linked to wallet

Creation of Qualified Electronic Signature

One time



EU DI WALLET

Identity

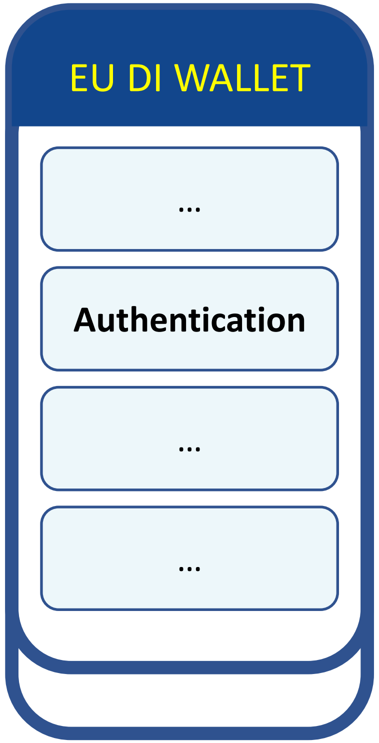
....

...

...

- Short term certificate
- One time signature
- Wallet provides identification

Multi use



EU DI WALLET

...

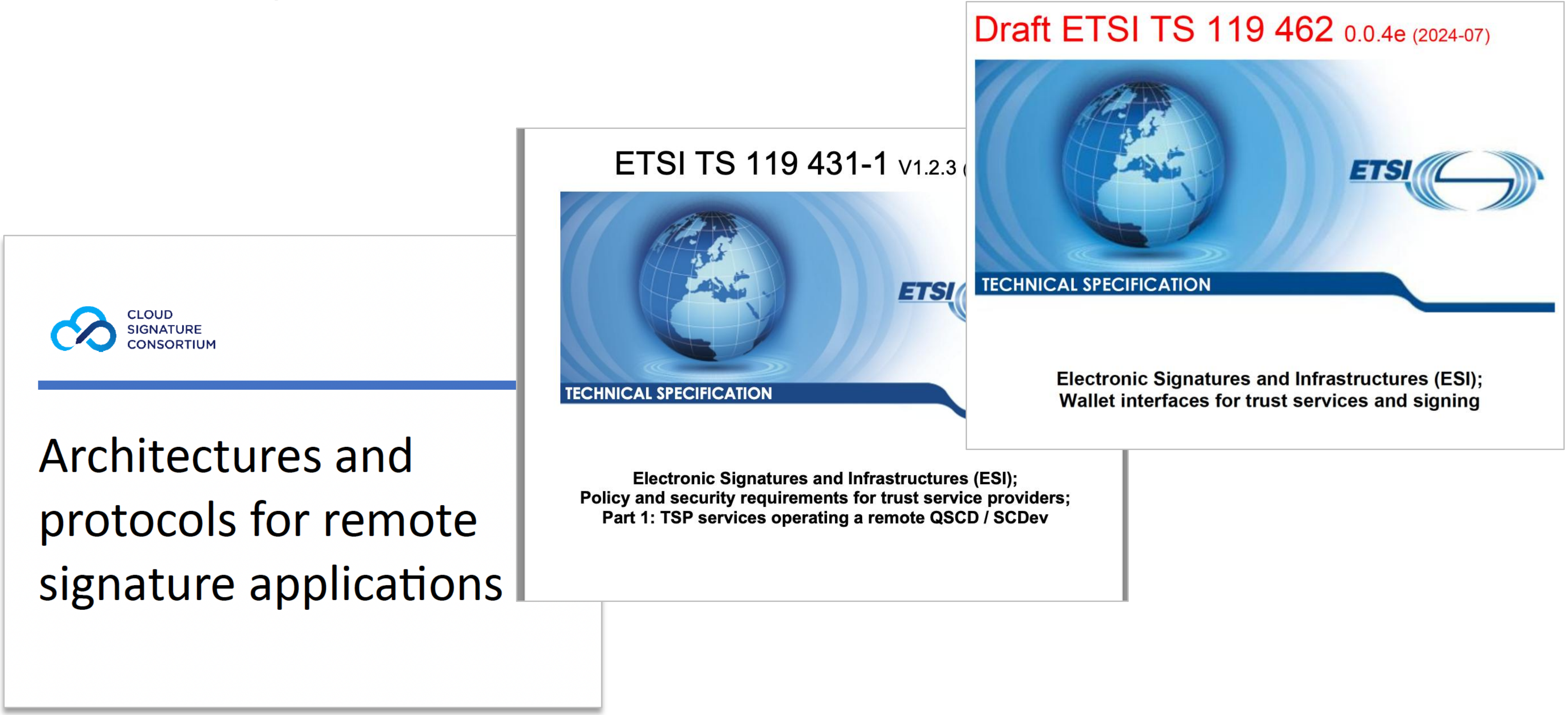
Authentication

...

...

- Long term certificate
- Signature Activation for Remote QSCD
- Wallet provides authentication

Remote signature standards



CLOUD SIGNATURE CONSORTIUM

Architectures and protocols for remote signature applications

ETSI TS 119 431-1 V1.2.3 (

TECHNICAL SPECIFICATION

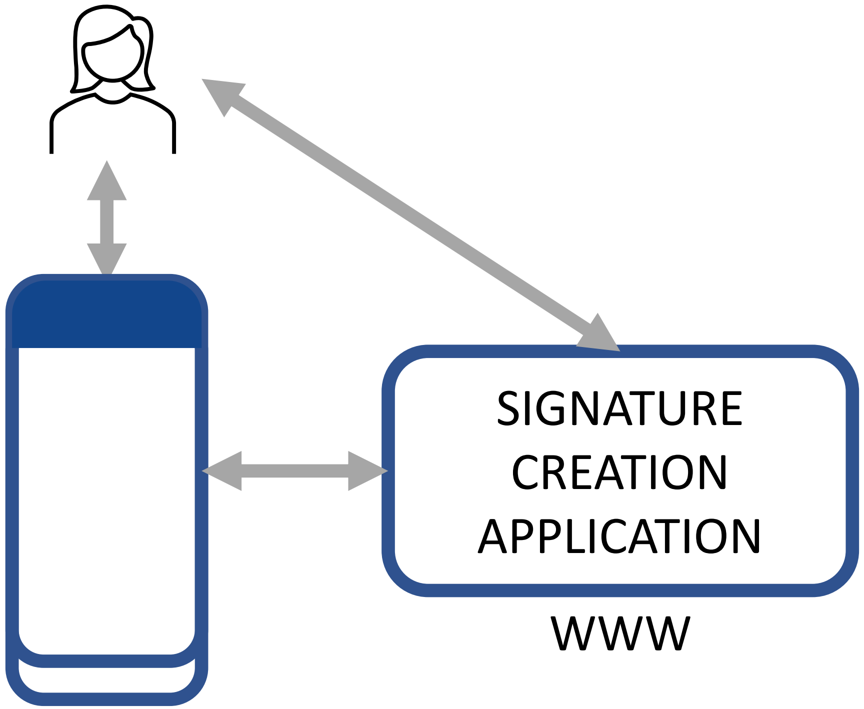
Electronic Signatures and Infrastructures (ESI);
Policy and security requirements for trust service providers;
Part 1: TSP services operating a remote QSCD / SCDev

Draft ETSI TS 119 462 0.0.4e (2024-07)

TECHNICAL SPECIFICATION

Electronic Signatures and Infrastructures (ESI);
Wallet interfaces for trust services and signing

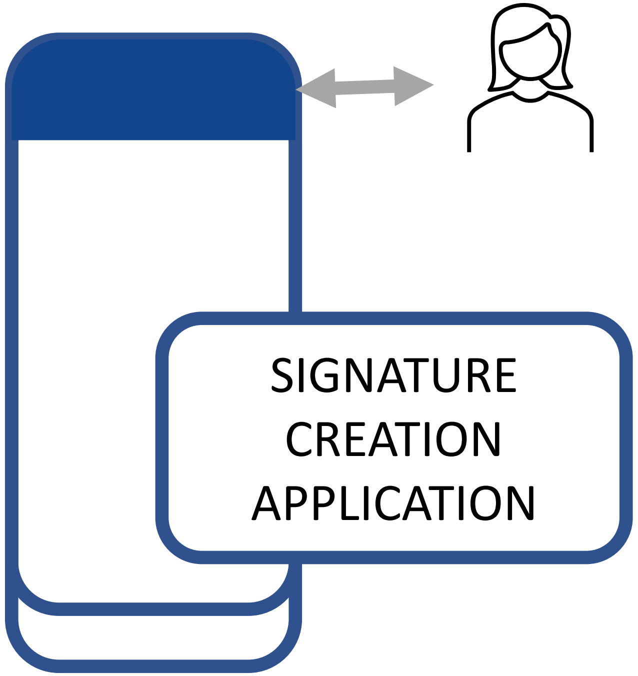
Signature Creation Application models



SIGNATURE CREATION APPLICATION

WWW

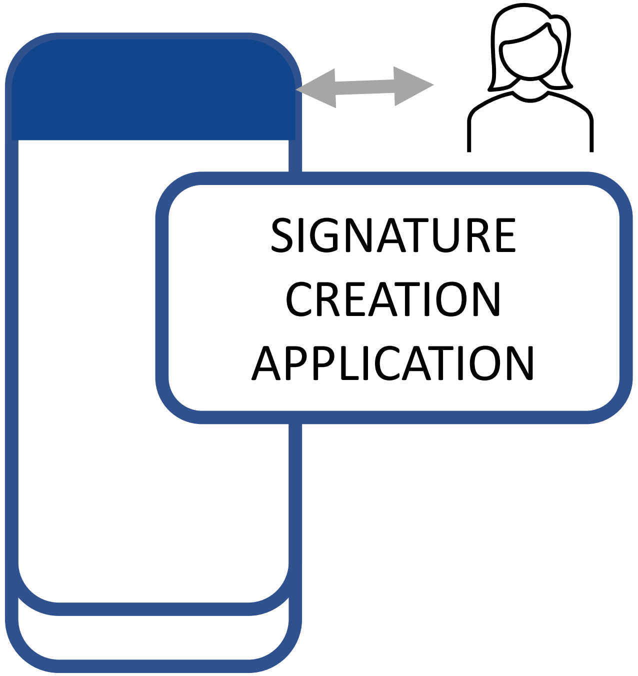
SCA as a service independent from the wallet solution



SIGNATURE CREATION APPLICATION

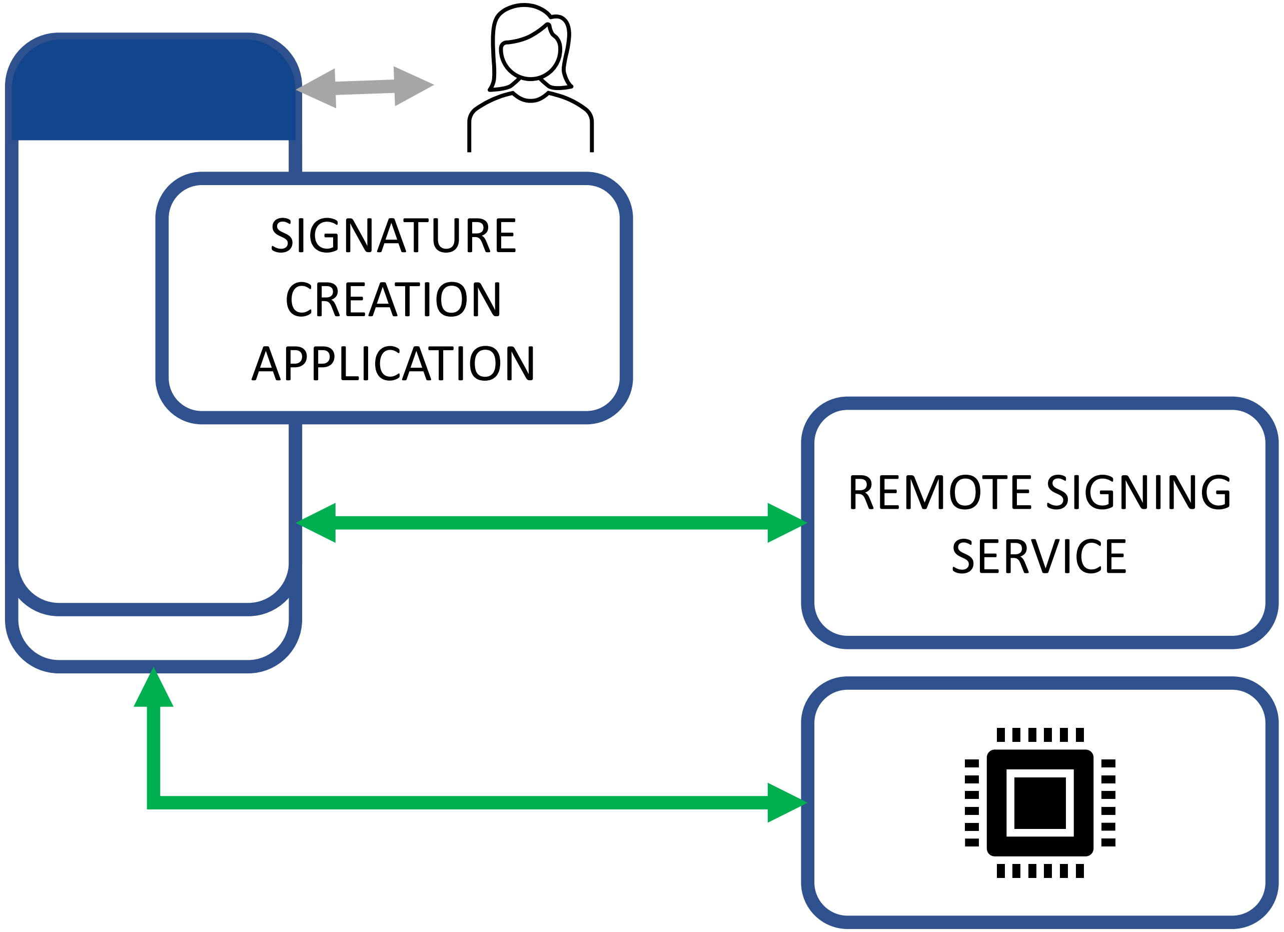
SCA as software included or connected to the wallet solution directly

Signature Creation Application models



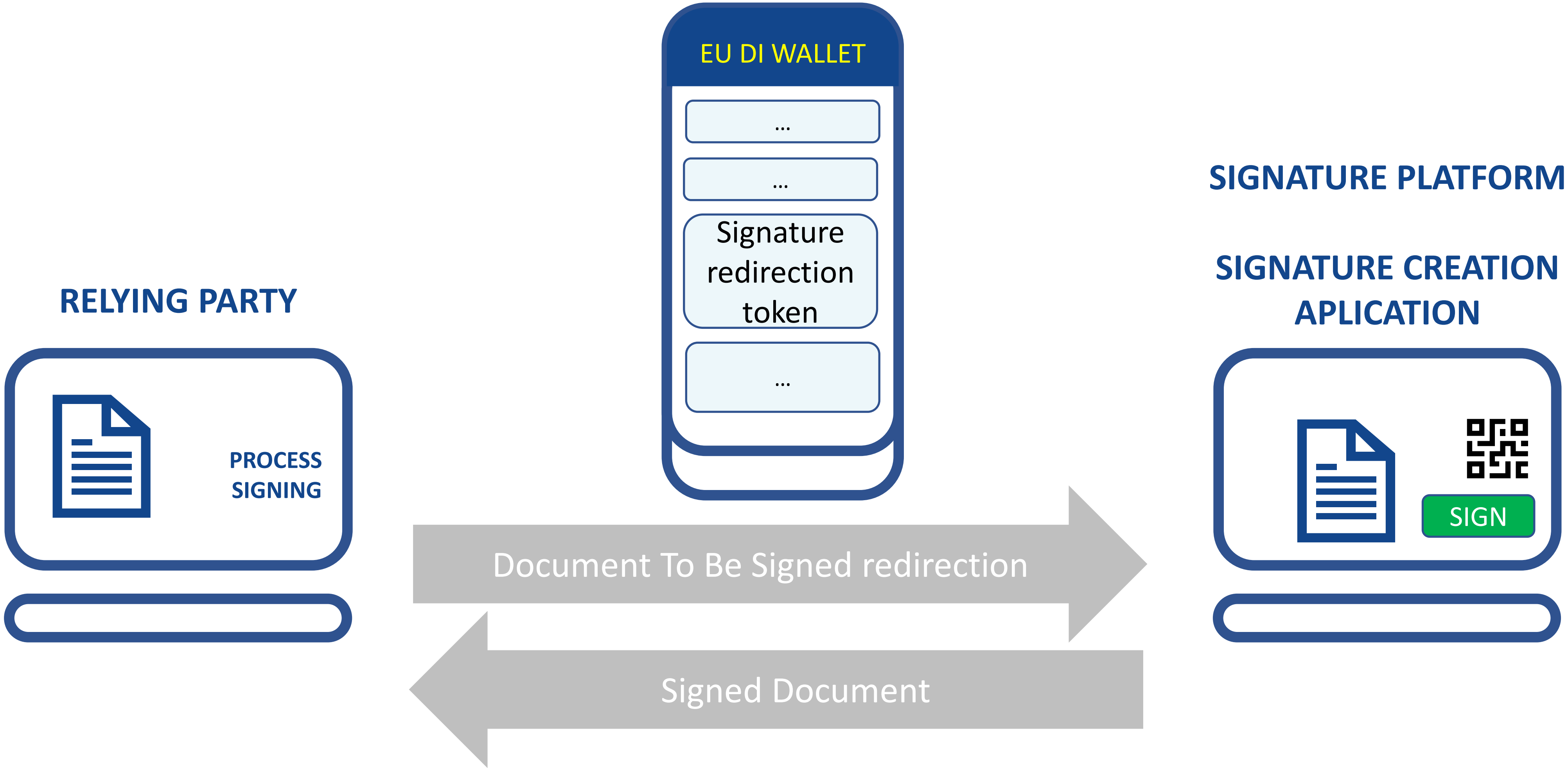
SCA as software included or connected to the wallet solution directly

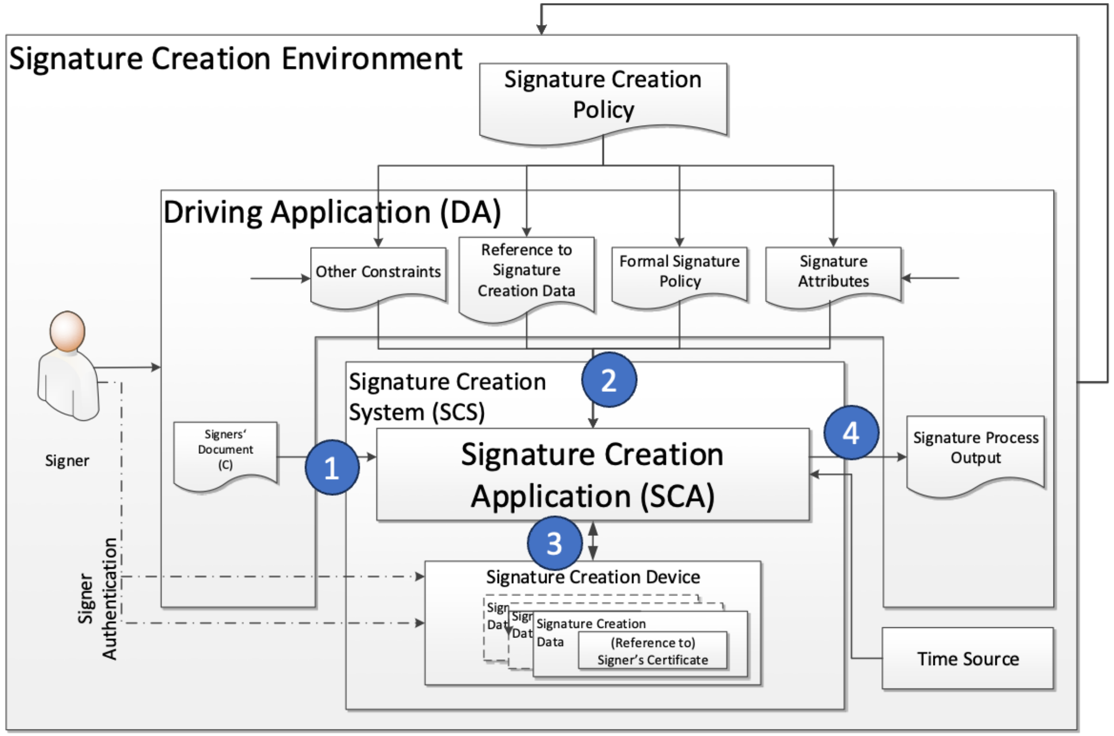
Local and remote signature



SCA on the wallet uses wallet to interact with QSCD

Document to be signed redirection to SCA

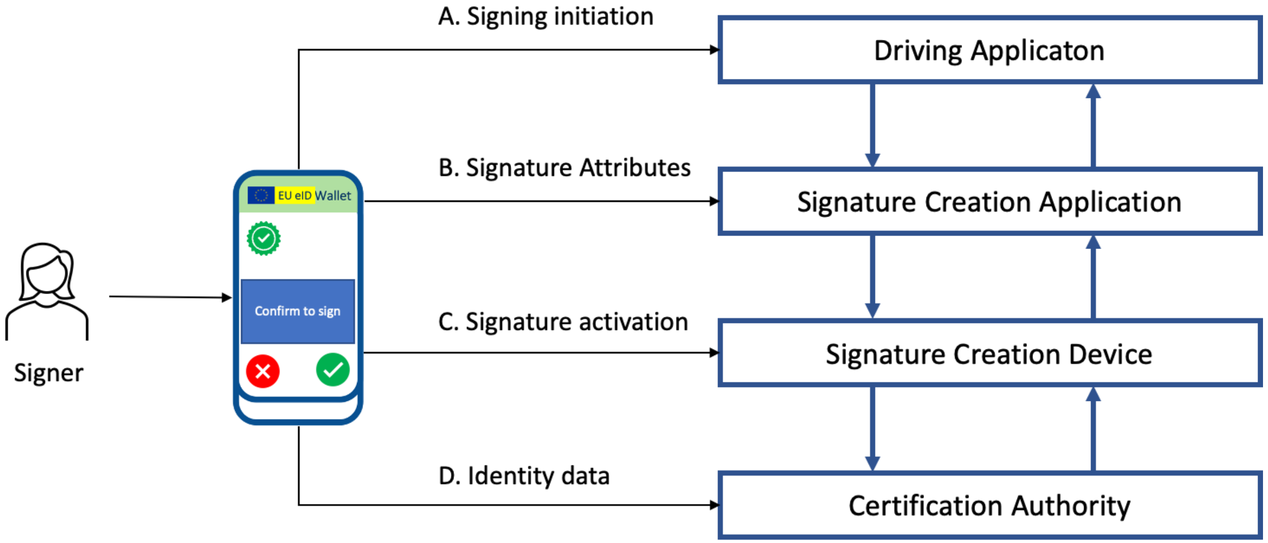

EU DI WALLET
...
...
Signature redirection token
...
RELYING PARTY
PROCESS SIGNING
SIGNATURE PLATFORM
SIGNATURE CREATION APLICATION
SIGN
Document To Be Signed redirection
Signed Document


Signature Creation Environment
Signature Creation Policy
Driving Application (DA)
Other Constraints
Reference to Signature Creation Data
Formal Signature Policy
Signature Attributes
Signer
Signers' Document (C)
Signature Creation System (SCS)
Signature Creation Application (SCA)
Signature Process Output
1
2
3
4
Signature Creation Device
Signature Creation Data
(Reference to) Signer's Certificate
Time Source
Signer Authentication

Functional Model of Signature Creation

(Source: ETSI EN 319 102-1)

Signature creation data data



ETSI TS 119 432

Cloud Signature Consortium API

ETSI EN 319 431-2

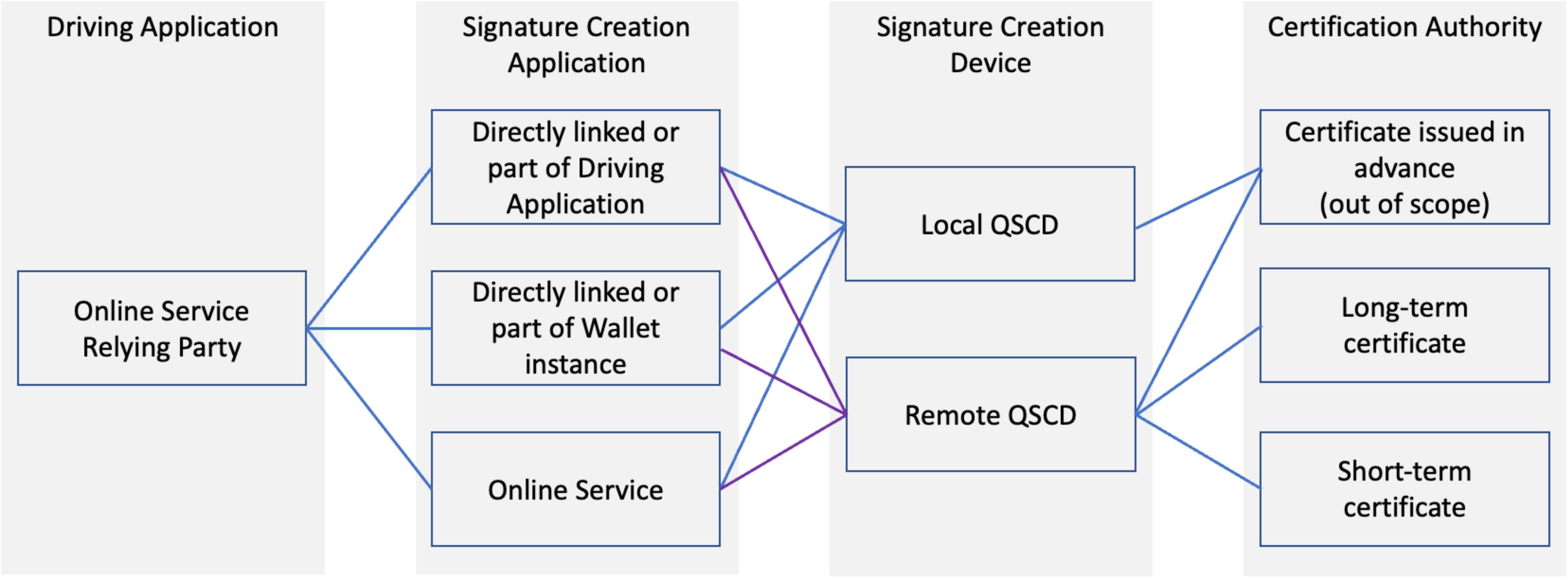
OID4VP

ETSI EN 319 102-1

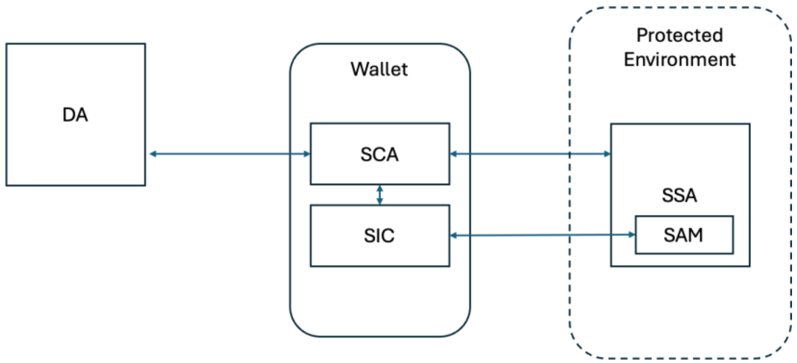
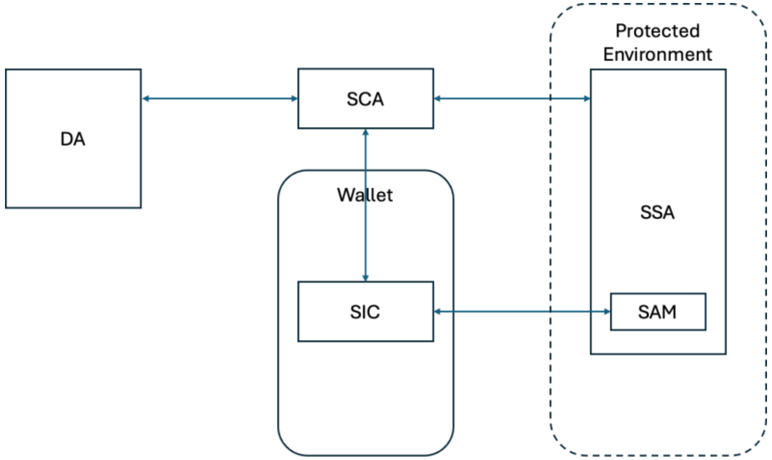
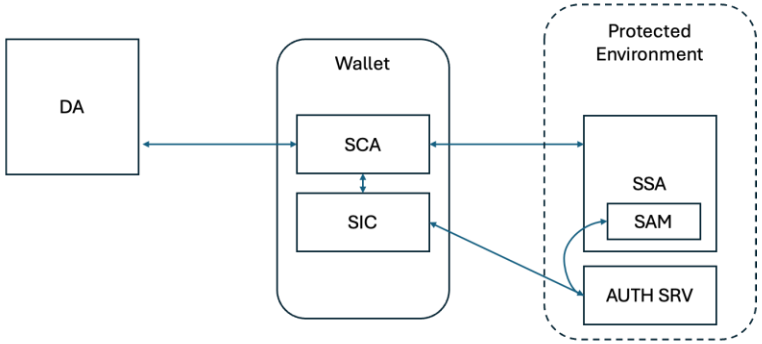
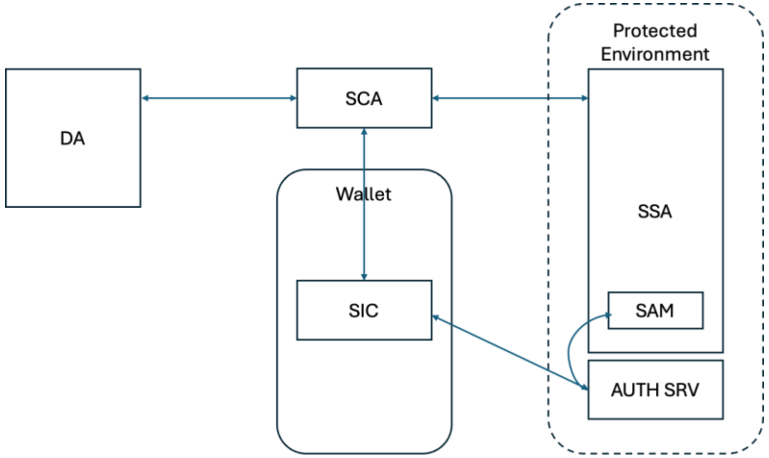
ETSI EN 319 411-1

ETSI EN 319 411-2

Siganture cration scenarios


Driving Application
Online Service Relying Party
Signature Creation Application
Directly linked or part of Driving Application
Directly linked or part of Wallet instance
Online Service
Signature Creation Device
Local QSCD
Remote QSCD
Certification Authority
Certificate issued in advance (out of scope)
Long-term certificate
Short-term certificate

Remote signature creation models

	SCA directly linked to the Wallet	SCA is remote application
Wallet as SIC directley generates SAD		
SAD generated outside of the Wallet		

Thank you!

OBSERWATORIUM.BIZ

Michał Tabor

Partner

✉ michal.tabor@obserwatorium.biz

☎ +48 501557094