Presentation
Ubiqu

Implementation of EUDIW Assurance Level High

We envision a world where digital identity is the cornerstone of a thriving society, where people can securely and confidently interact, access services, and contribute to the common good.

We believe that securing digital identity is the highest priority for enabling trust, privacy, and empowerment in the digital age.

We are committed to providing innovative and reliable solutions for creating and verifying digital identities that are aligned with the highest standards of security, ethics, and human rights.

ubiqu

EU regulation *accelerates* Qualified Trust Services from 2024

eIDAS 2.0 impacts, enriches and secures all digital interactions

1) Identity verification

2) Digital signatures

3) Banking and Payments

Other:

- Identity and Access management
- Blockchain and Self-Sovereign Identity

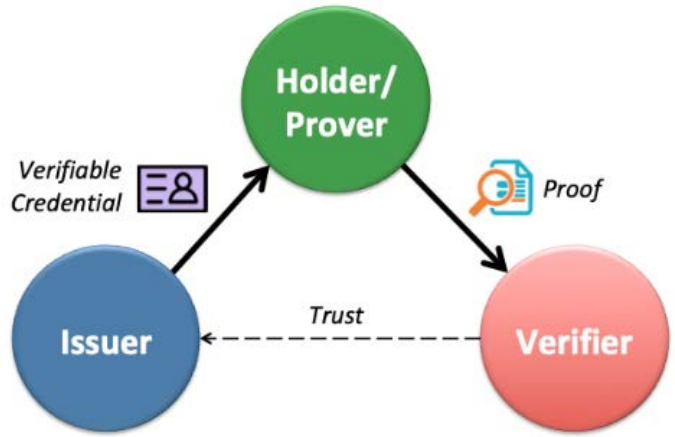
Qualified Trust Services

ISSUERS

WALLETS

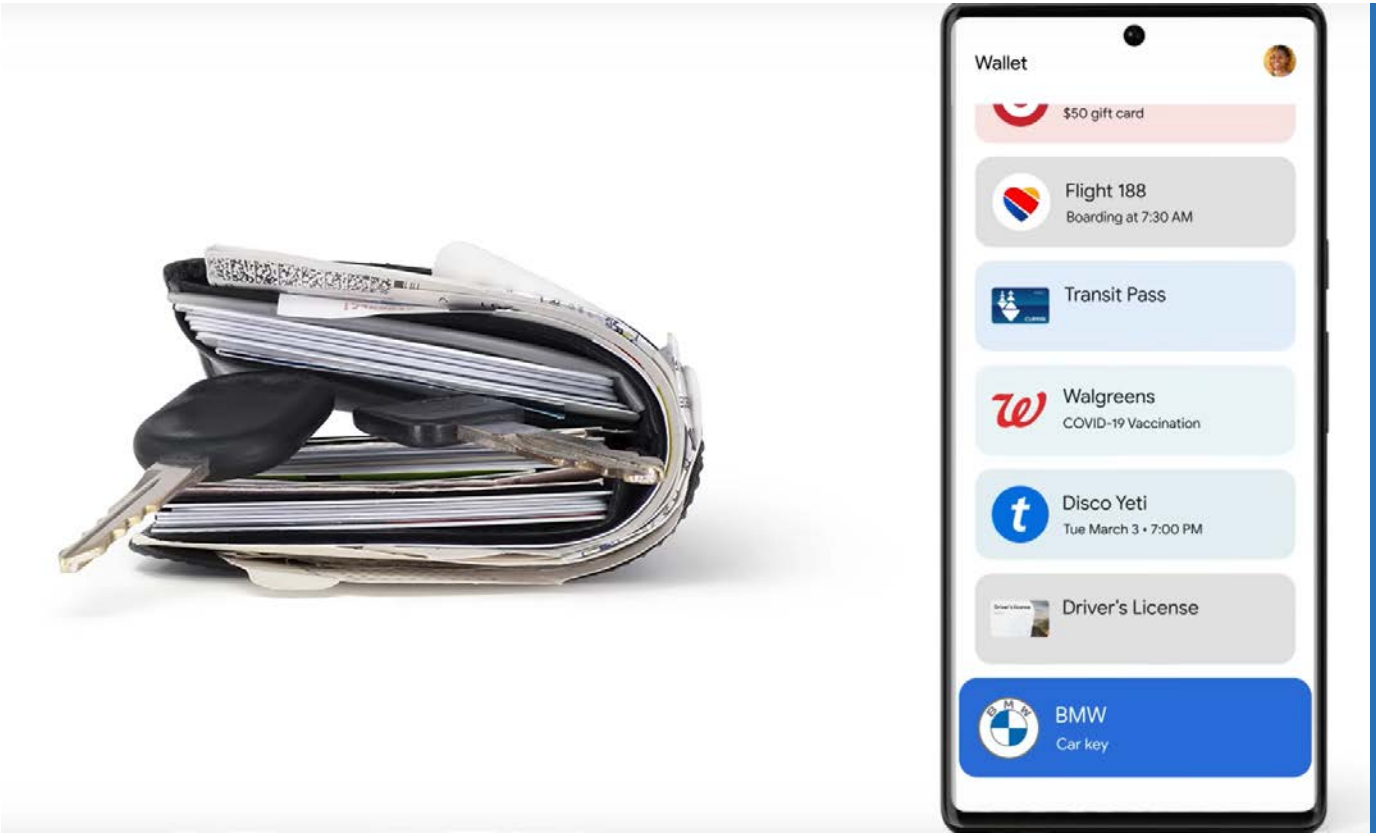
QUALIFIERS

Highest level of compliance in process & tech



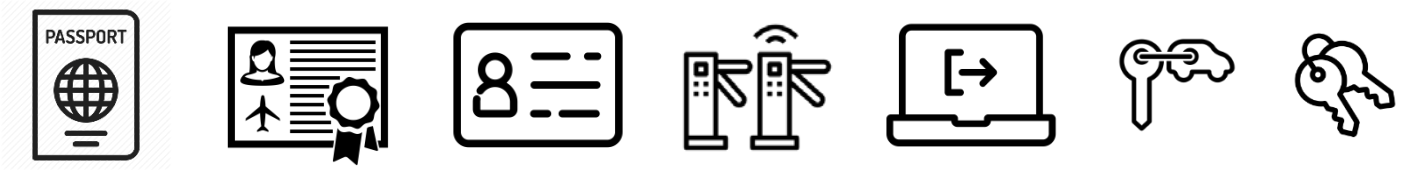
ubiqu

Qualified Trust Services needs *eIDAS high* compliant wallets



eIDAS High “sole control” requires a (hardware) security solutions And identity proofing

Use cases requiring Qualified trust services and wallet



ubiqu

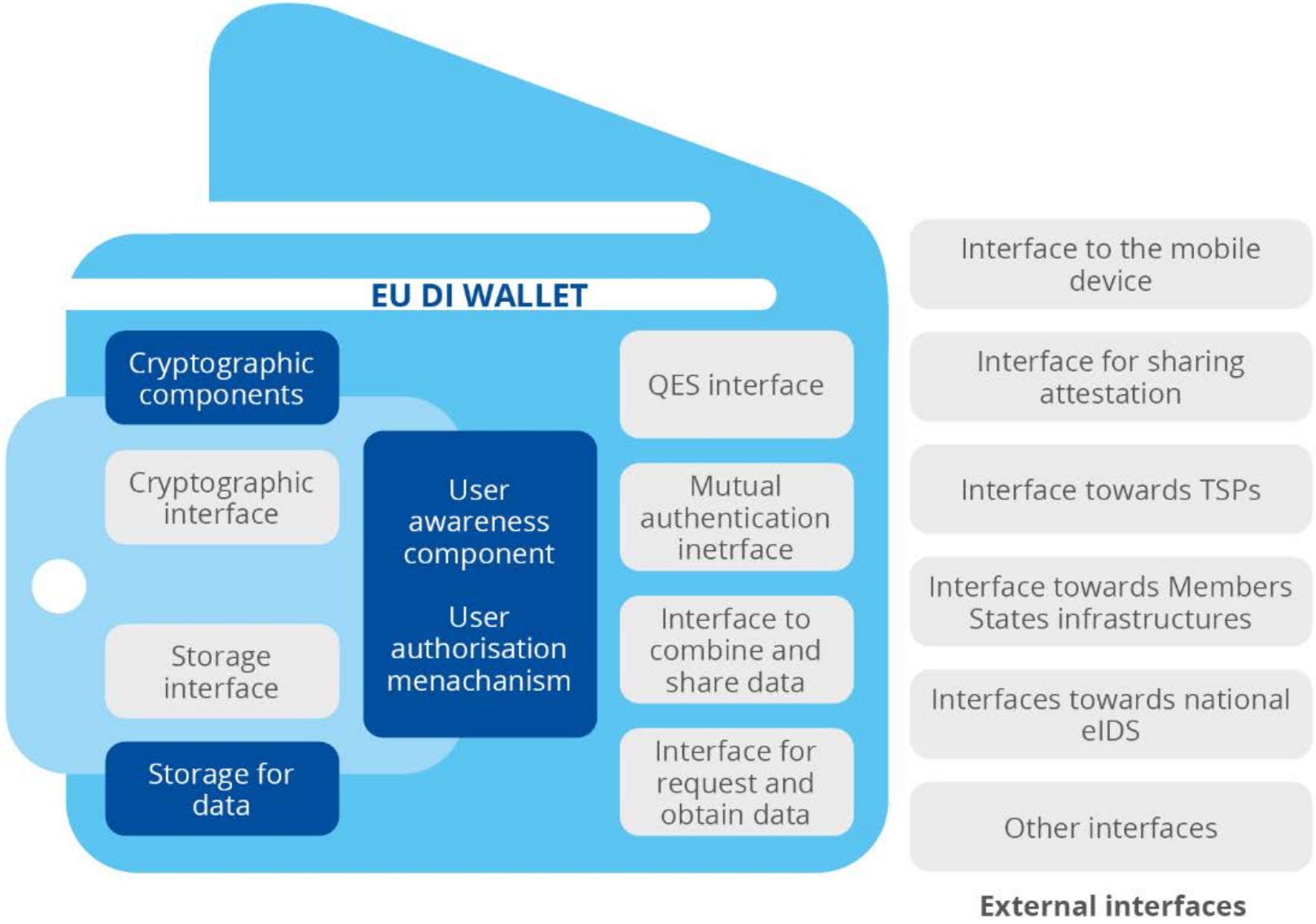
Creating a scalable solution means

- **Remote unattended** issuing if a wallet and Identity credential

- **Remote unattended** identity proofing

ubiqu

What is a wallet



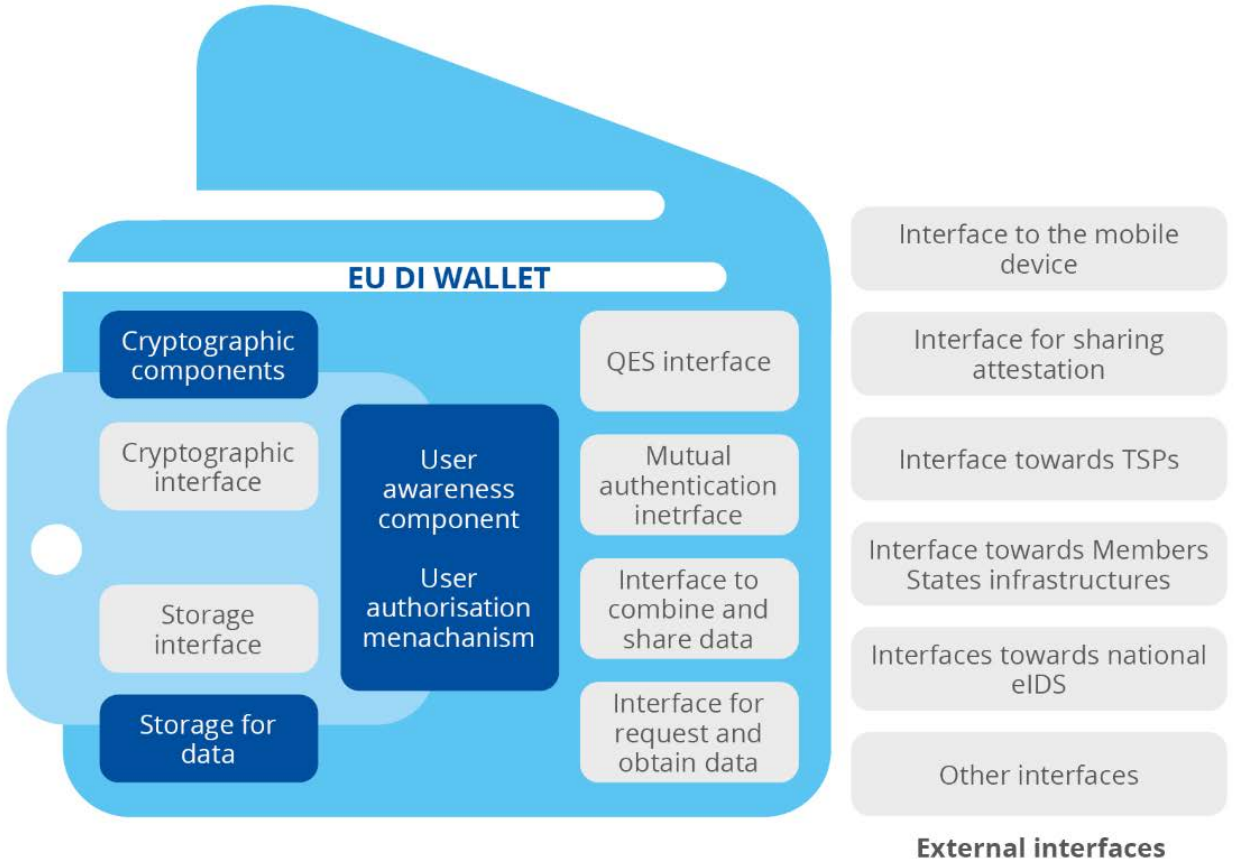
Source enisa: https://www.enisa.europa.eu/publications/digital-identity-standards/

ubiqu

Two Challenges for scale

1. Cryptographic components

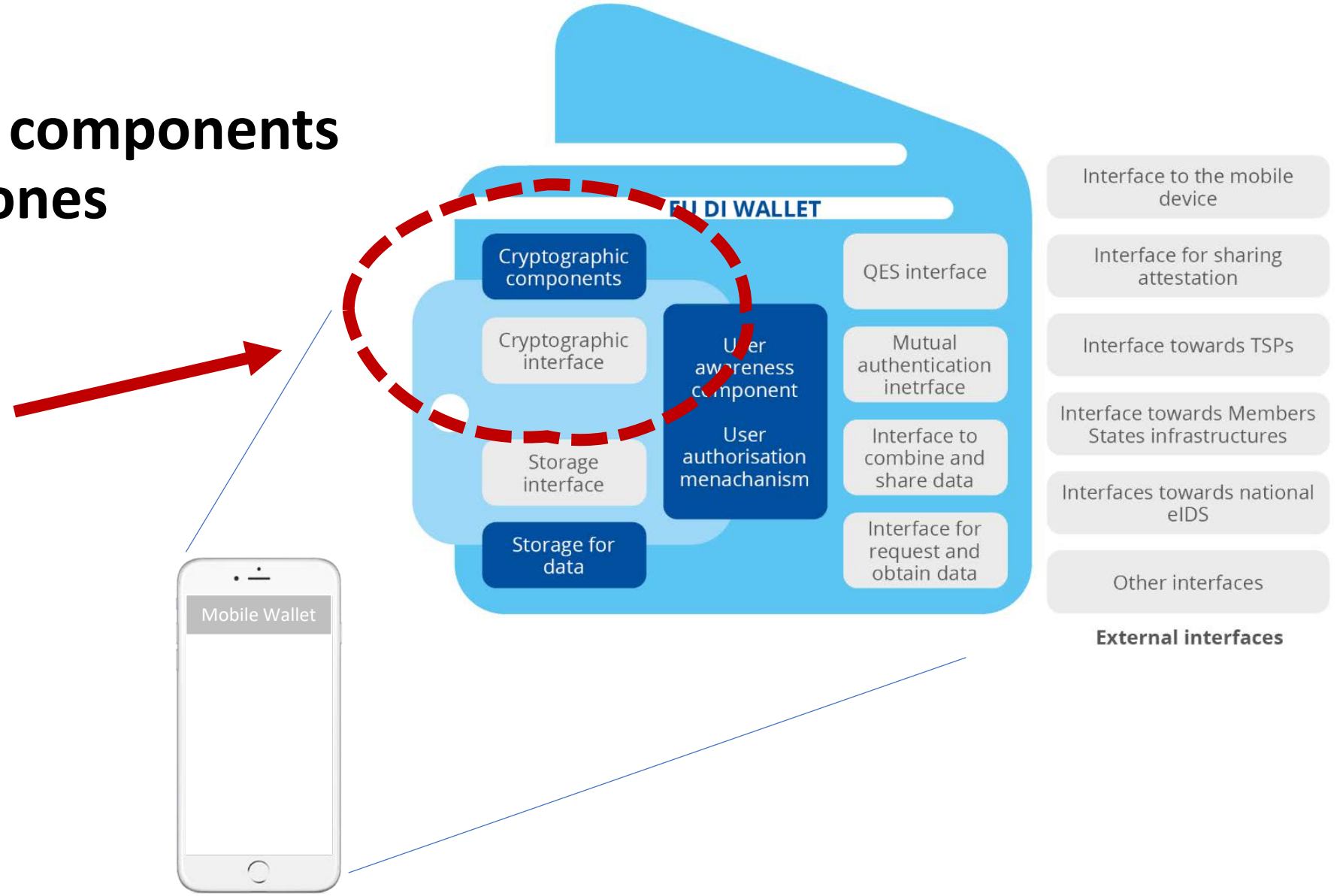
2. linking a wallet to an identity proofing event



Source enisa: https://www.enisa.europa.eu/publications/digital-identity-standards/

ubiqu

Cryptographic components for mobile phones



Source enisa: https://www.enisa.europa.eu/publications/digital-identity-standards/

ubiqu

hardware security elements: 5 options

Physical secure elements
(smart card, usb token, Embedded Secure element)

Secure, but **complex ecosystem, logistics and high cost**

Local trust environment
(secure enclave, Trustzone, TEE)

Lack features such as recovery and introduces serious vulnerabilities in time thus **cannot provide 100% coverage**.

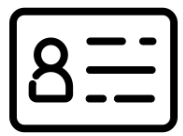
Secure software solution
(wallet, DRM, encrypted computation, obfuscation)

Great UX, Feature rich and flexible and crypto agile, but **lacks security**

Cloud Hardware security module
(HSM, QSCD, eSeal, payload signing systems)

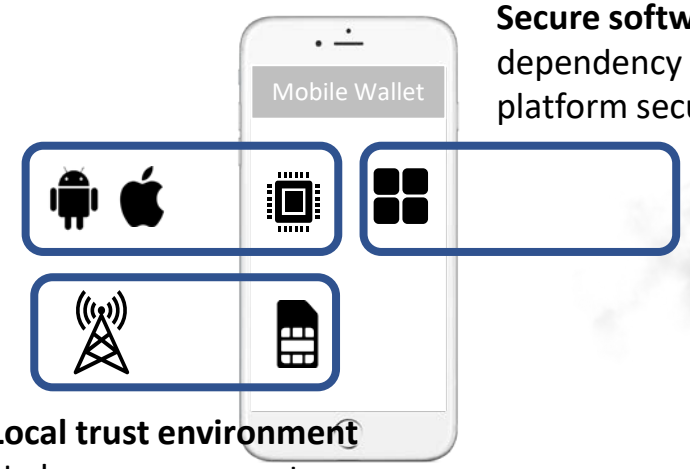
Ubiquitous application, but **only for signing** and still needs an authentication solution

Remote Secure element from ubiqu
- ✓ **Secure**
- ✓ **Unlimited**
- ✓ **Unhindered**
- ✓ **Ubiquitous**



Smart card
NFC Recuired

USB key
expensive



Secure software solution
dependency on device platform security

Local trust environment
No key management, dependency on device manufacturer and platform security

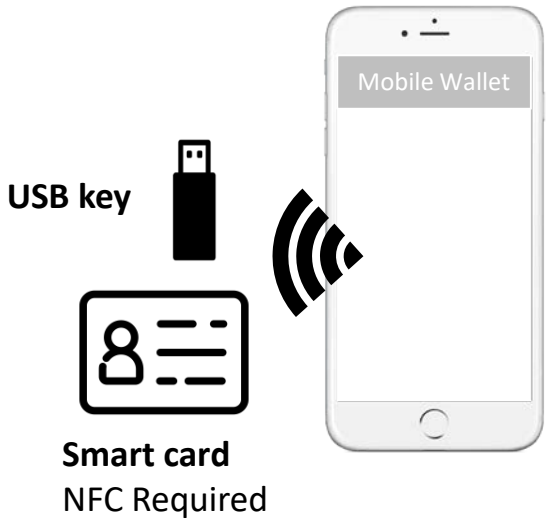
Cloud Hardware security module(HSM)
Only for signing

ubiqu

(hardware) security elements : Option 1 - External

Physical secure elements
(smart card, usb token, Embedded Secure element)

Secure, but **complex ecosystem, logistics and high cost**



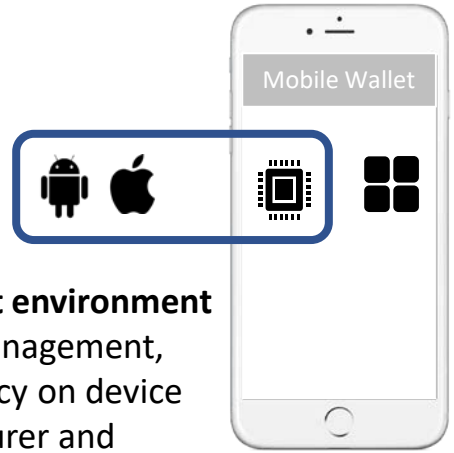
1. eIDAS 2.0 compliant v
2. Scalable ?
3. User friendly X
4. Robust- crypto agile X
5. Independent v
6. Fast Roll-out v

ubiqu

local hardware elements : Option 2a TEE/ eSE

Local trust environment
(secure enclave, Trustzone, TEE)

Lack features such as recovery and introduces serious vulnerabilities in time thus **cannot provide 100% coverage**.



Local trust environment
No key management, dependency on device manufacturer and platform security

1. eIDAS 2.0 compliant X
2. Scalable V
3. User friendly V
4. Robust- crypto agile X
5. Independent X
6. **Fast Roll-out** X

Current Apple, Samsung and Google only FIPS

Will take at least a decade to roll-out

3811	Apple Inc.	Apple Secure Key Store Cryptographic Module, v10.0	Hardware	02/05/2021 03/11/2021

Currently only IOS 13 and older newer in process

4574	Google, LLC.	Titan Security Key, Chip Boundary	Hardware	08/31/2023

Currenty only Pixel phones

S3FV9RR/S3FV9RQ/S3FV9RP/S3FV9RK 32-bit RISC Microcontroller for Smart Card with optional AE1 Secure Libraries including specific IC Dedicated software

Currenty only one or two models

Hardware secure elements : Option 2b – SIM/eSIM/eSE

Local trust environment
(SIM, eSIM, eSE)

Complex eco-system.

Local trust environment
No key management, dependency on device manufacturer and platform security

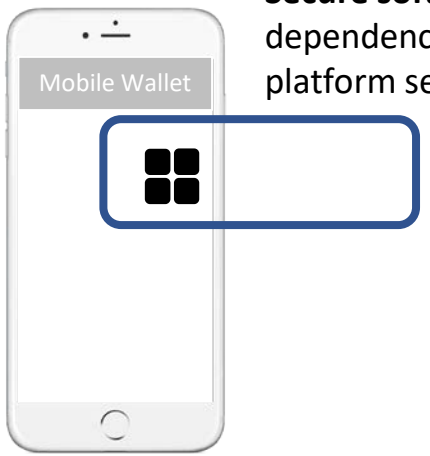
1. eIDAS 2.0 compliant v
2. Scalable v
3. User friendly v
4. Robust- crypto agile ?
5. Independent X
6. Fast Roll-out ?

ubiqu

Option 3 – No hardware Whitebox crypto software

Secure software solution
(wallet, DRM, encrypted computation, obfuscation)

Great UX, Feature rich and flexible and crypto agile, but **lacks security**



Secure software solution
dependency on device platform security

1. eIDAS 2.0 compliant X
2. Scalable v
3. User friendly v
4. Robust- crypto agile v
5. Independent v
6. Fast Roll-out v

ubiqu

Option 4: Remote hardware security module (QES)

Cloud Hardware security module
(HSM, QSCD, eSeal, payload signing systems)

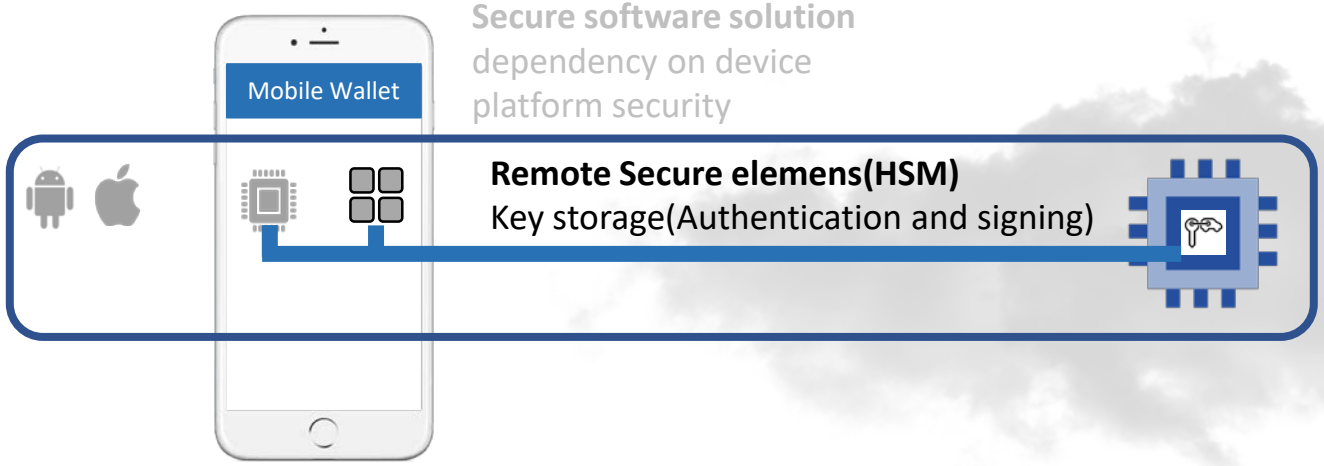
Ubiquitous application, but **only for signing** and still needs an authentication solution

Needs an authentication solution

ubiqu

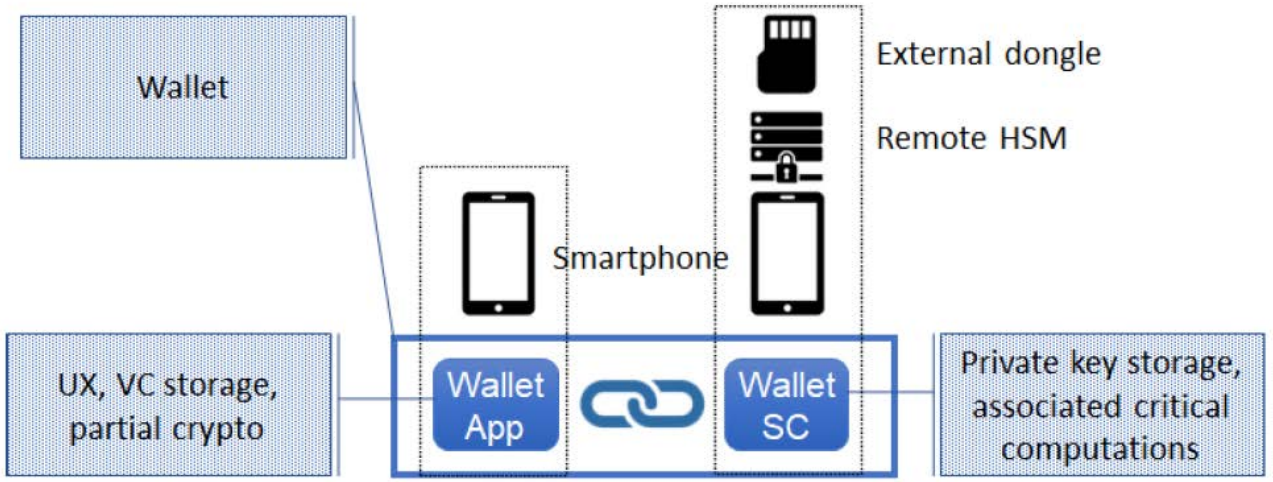
Remote Secure Element – Cryptographic backend for wallets

Remote Secure element from ubiqu
- Secure
- Unlimited
- Unhindered
- Ubiquitous



1. eIDAS 2.0 compliant v
2. Scalable v
3. User friendly v
4. Robust- crypto agile v
5. Independent v
6. Fast Roll-out v

Why does it work –
Separation of “device key” from user “cryptographic keys”



Separation of “device key”

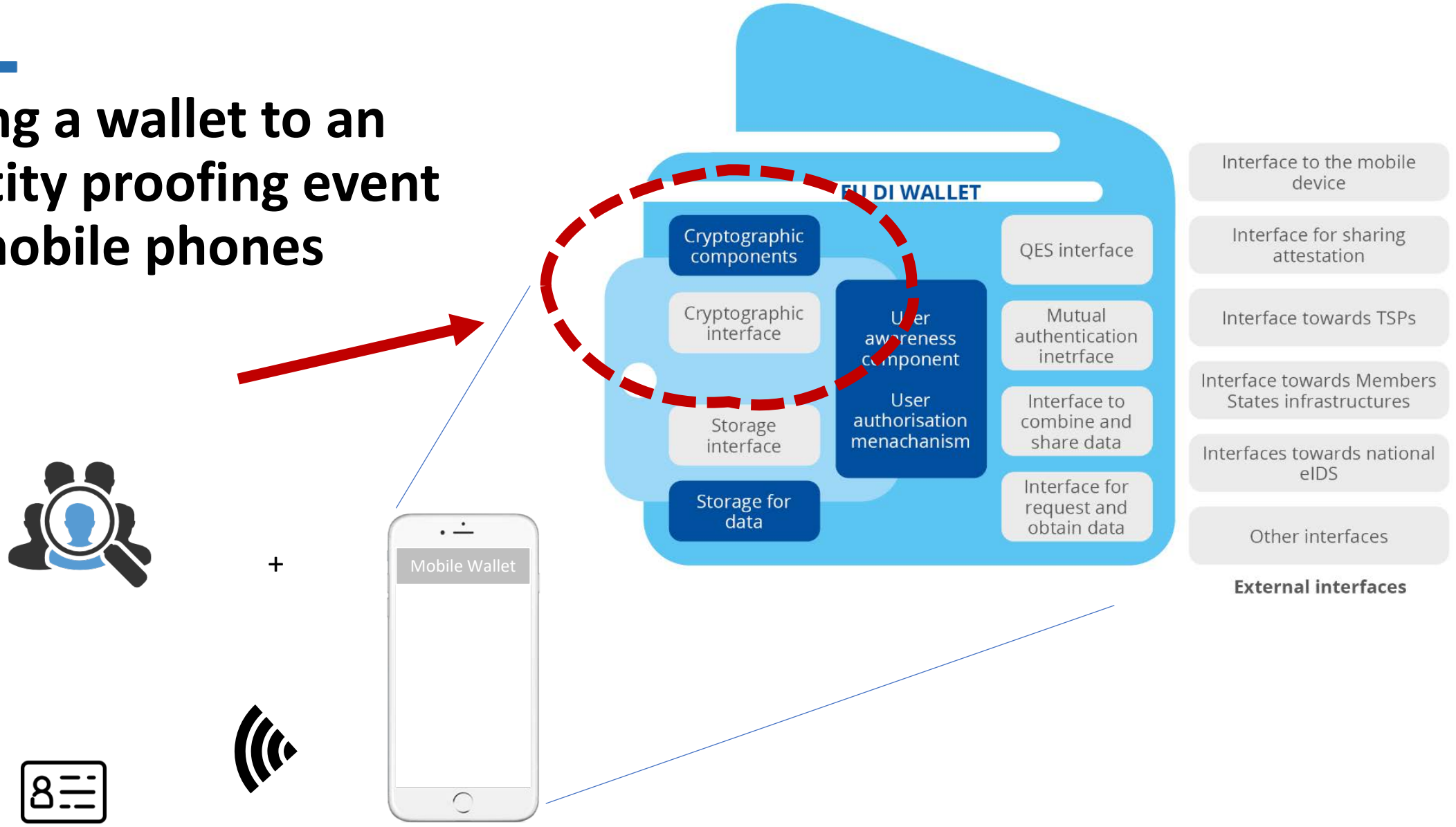
from user cryptographic keys

Device key protects user keys and vice- versa

Source GSMA: https://www.gsma.com/gsmaeurope/resources/architecture-considerations-for-eidas-2-0/

ubiqu

linking a wallet to an identity proofing event for mobile phones



Source enisa: https://www.enisa.europa.eu/publications/digital-identity-standards/

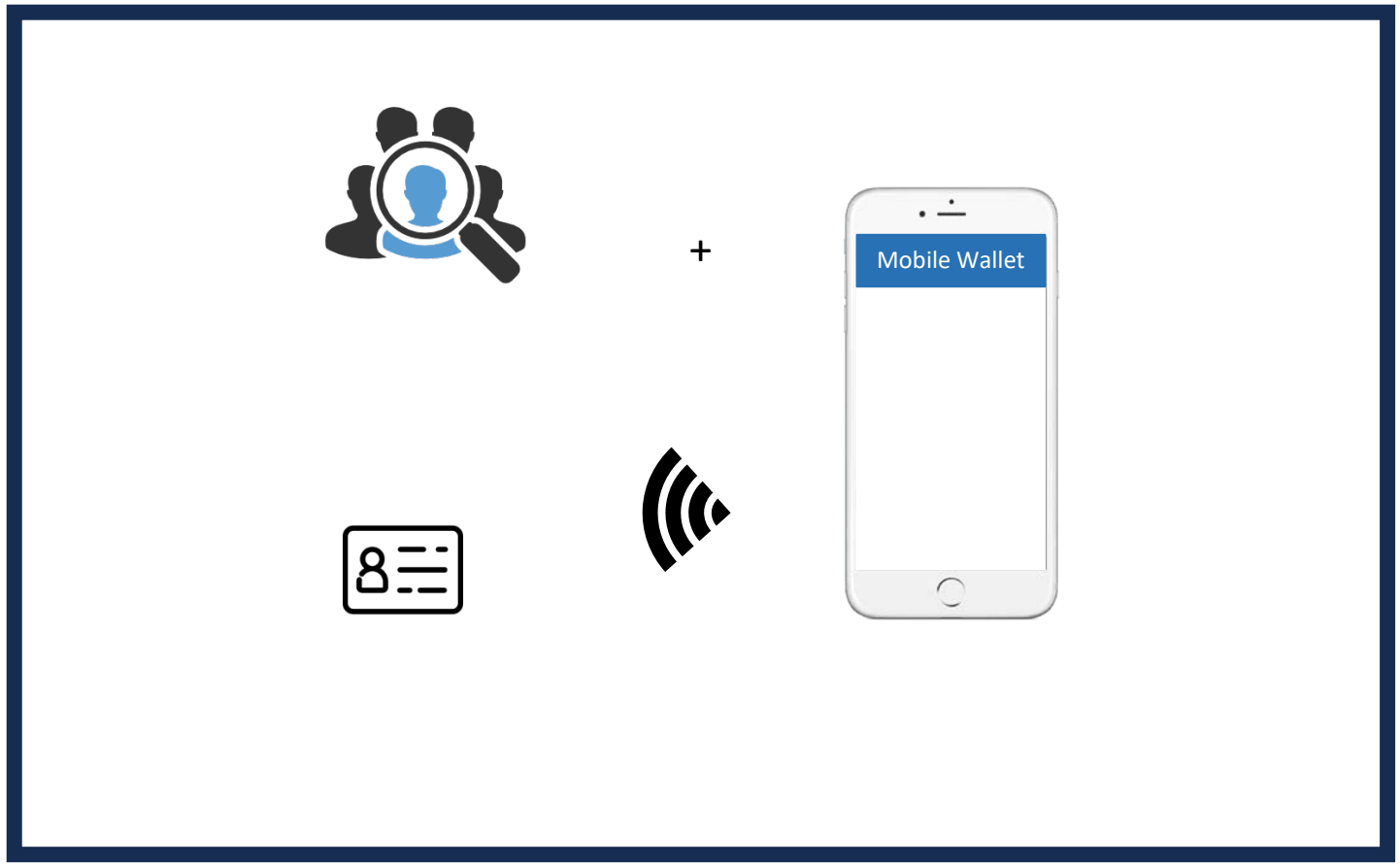
ubiqu

ETSI TS 119 461 Use cases for identity proofing of natural person

1. Physical presence of the applicant
2. Attended remote
3. **unattended remote**
4. by authentication using eID means
5. using digital signature with certificate

ubiqu

Linking a wallet to identity proofing event using “NFC + selfie” to a wallet bu issuing a “identity” credential



All components:

- NFC read of ICAO ID Document
- Liveliness/biometric
- Issuing of identity credential

must be part an integrated part of the wallet and cannot be separate services, from a security and linkability point of view

ubiqu

Summary: Creating a scalable solution means

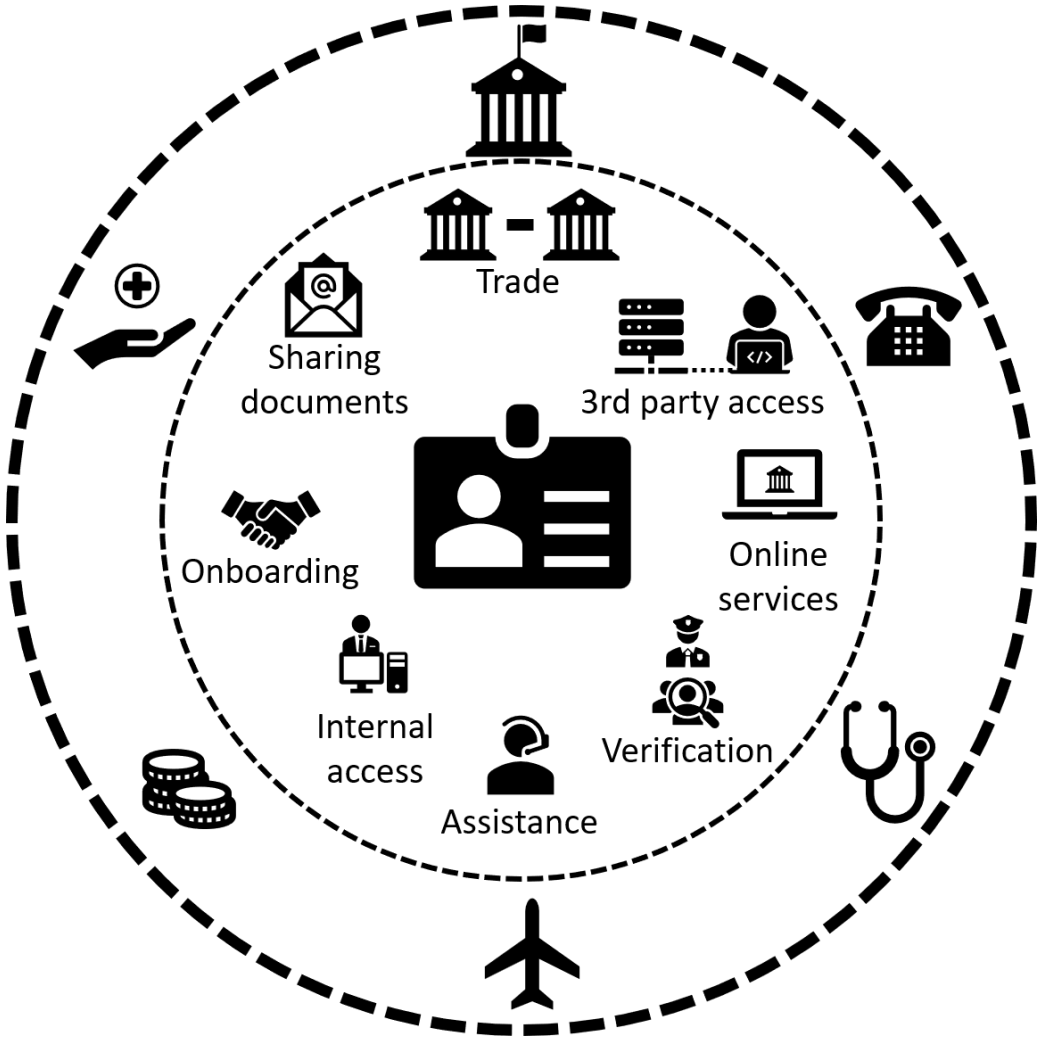
- Remote unattended issuing if a wallet and Identity credential

- Remote unattended identity proofing

At a minimum but also other options, for edge cases

ubiqu

What happens once e have rolled-out our scalable digital identity?



Orchestration of attributes to Identities and wallets

Physical tokens have a **secure element**

A secure element is needed on mobile phones, but **all current solution fall short**

Introducing…
a **remote** secure element for any (mobile) device
For scale

From physical tokens

Digital wallet

Secured by a remote secure element

ubiqu

Goal – Globally scalable digital identities and data provenance

1

Identity verification

Uniquely link a <u>person</u>
to a device,
the KYC event

2

Digital Identity issuance

Uniquely link a new account
to a <u>person</u> using the device
and the previous KYC event

3

Digital Identity use (sign-in and sign)

Uniquely link an action
to a <u>person</u> using the device
and the KYC event

4

Trust

Digital Trustflow

Build better digital systems using data provenance

5

Wallet

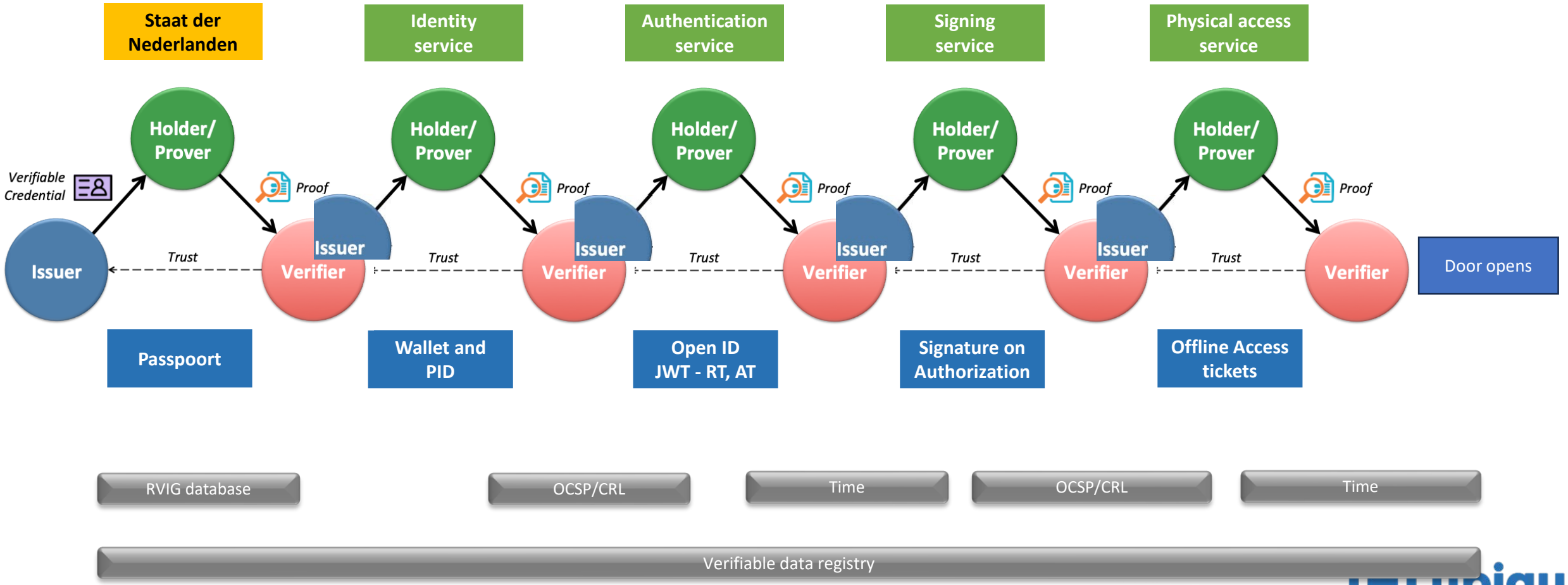
Digital Wallet (online and offline attributes)

Use Digital wallet to play in any context:

1. mDL 18013-5
2. ISO 23220
3. eIDAS
4. Open ID
5. PSD2/SCA/KYC

Real world Example: From identity to access

The opening of the door has provenance in the identity checking.



Real world Example: Real estate transaction

Personal Wallet

Personal Wallet

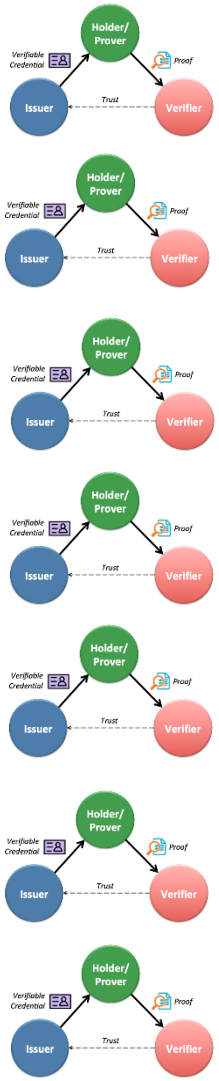
Sign

Eseal

Eseal

Personal Wallet

Attribute service



Seller =? owner √

Buyer √

Contract with buyer and seller signatures √

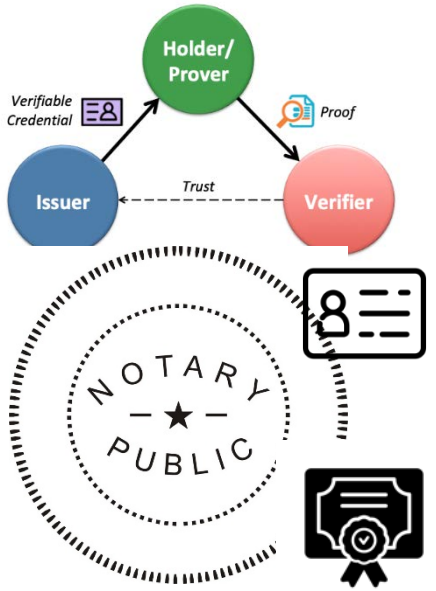
Land registry --> Owner √

Bank mortgage offer of proof of means √

Value appraisal √

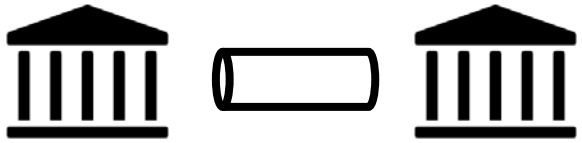
Value appraiser

Value appraiser registry



Introducing Data provenance - Zero trust for data and content

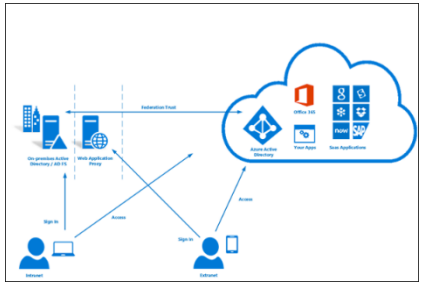
Secure connections



PKI

Create secure connections using PKI, TLS, IPSEC, VPN etc.

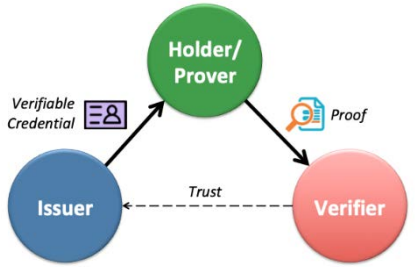
Federation



Zero trust

Trust another connections. i.e SAML, Oauth, Kerberos. Verify everything but content and data.

Zero trust for data



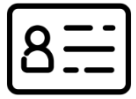
Trust in secured data

Secure the provenance of the data, AI accelerated the need for content and data provenance

Introducing Data provenance

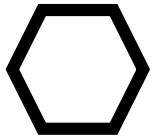
Data track and trace and audience management

Onboarding and Recovery



ID Verification(KYC) and issuing of wallets and Credentials to wallets

Wallet SDK



Issuer API's

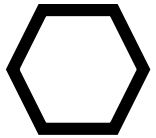
Transaction and Data integrity

Signing API

Qualified eSeal and electronic attribute API

Verification API's

Audience management



Encryption API

Sharing API

Decryption API

Infra structure: CA,OCSP, CRL, TSS, Remote Secure element etc.(products specific etsi 319 411-1/2 etc)

Platform for trustworthy systems (ETSI 319 401, ISO 27001/2)

Thank you

CEO Boris Goranov

www: www.ubiqu.com
Email: boris@ubiqu.com
Tel: +31 642 521 605