iDunion

Concepts for Wallet Security in SSI

Paul Bastian, Bundesdruckerei

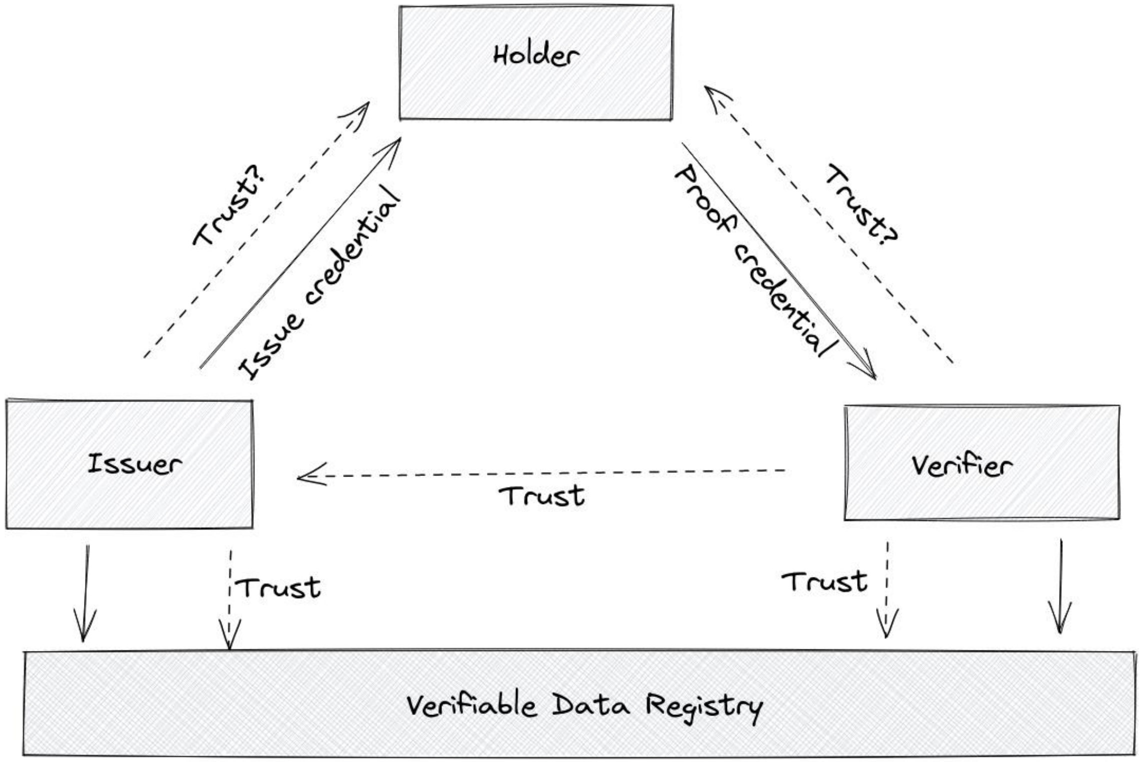
Agenda

1. Motivation & Requirements
2. Wallet Architectures
3. Differential Credential Security
4. Context of Holder binding
5. Three Pillars of Wallet Security
   1. Integrity of the Credential
   2. Authenticity of the Holder
   3. Authenticity of the Wallet
6. Mobile Wallet Security Approach (DIF)
7. Next Steps and Outlook

Motivation: The Overlooked Trust Relation

Trust in the SSI Triangle

- Trust relationship to the holder / wallet is mostly overlooked so far
- More security-relevant use cases demand new requirements



Issuer

How can I prevent or hinder missuse of my issued credentials and maintain my credibility at all costs?

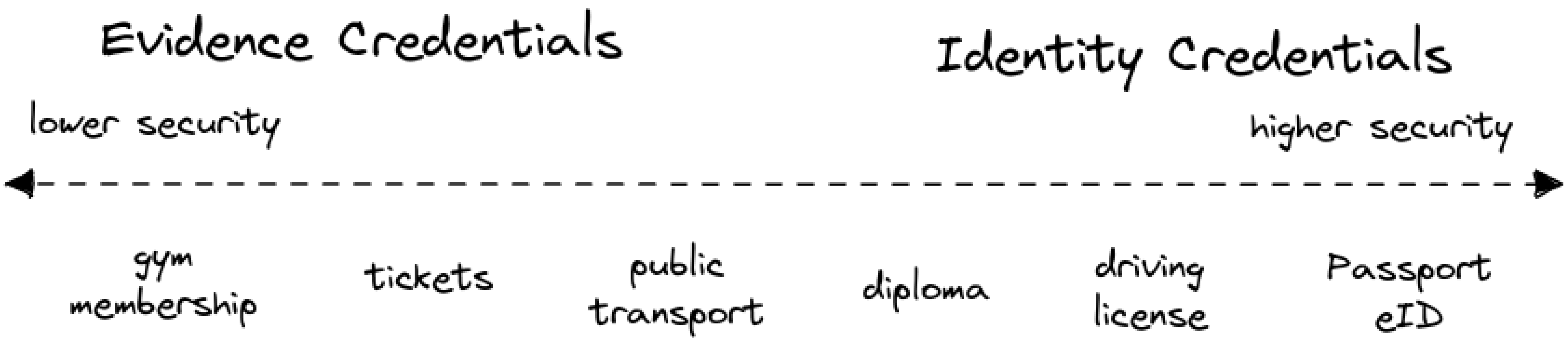
Verifier

Is the holder the rightful owner of this credential and to what degree can he plausibly prove that?

Is the holder‘s authentication strong enough to meet the requirements of my regulated use case?

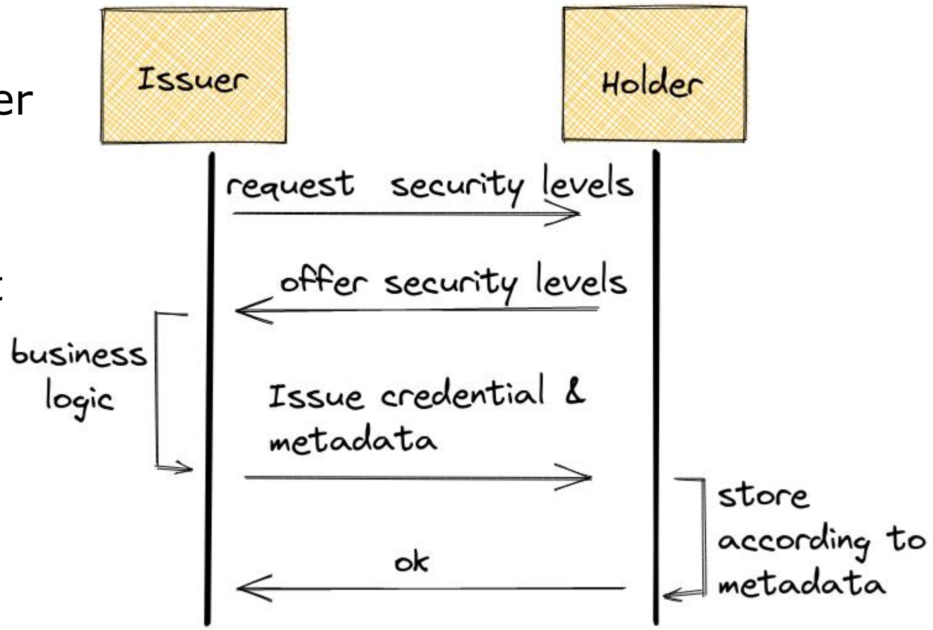
Differential Credential Security

DIF Wallet Security WG



Motivation

- SSI ecosystems brings use cases from different domains together
  - Regulated and non-regulated issuers have different security requirements
- Differential Credential Security model is a core feature for wallet security to address this flexibility
  - Wallet offers multiple LoA based on existing os/hardware
  - Issuer selects an option based on his usecase



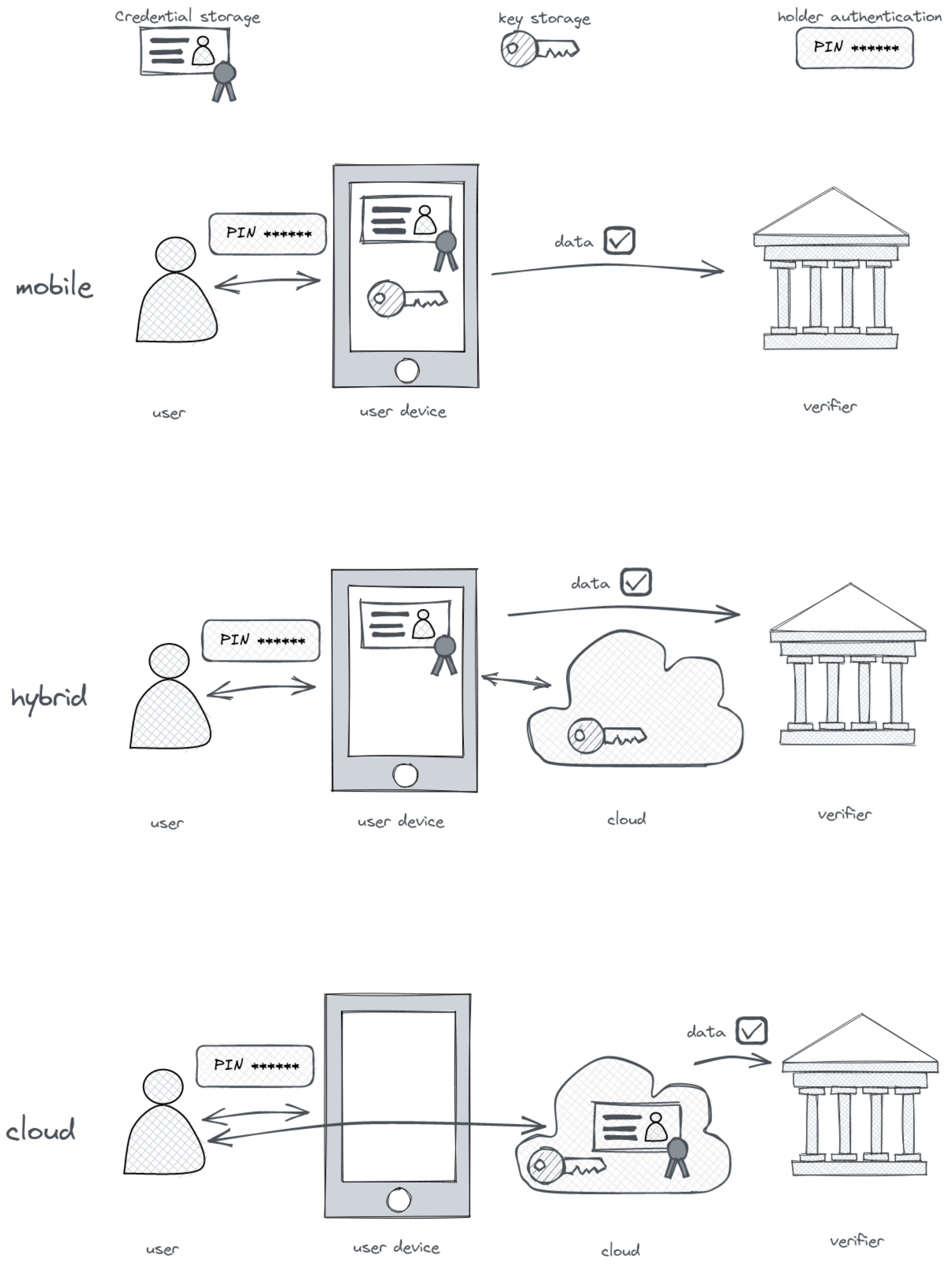
Wallet Security Architectures

Wallet Architectures differentiated by

- VC storage location
- Key storage location
- User authentication

Wallet Architectures implications

- Backup and recovery
- Multidevice support
- Privacy implications
- Offline support
- User interface
- Level of assurance



Wallet Security Architectures

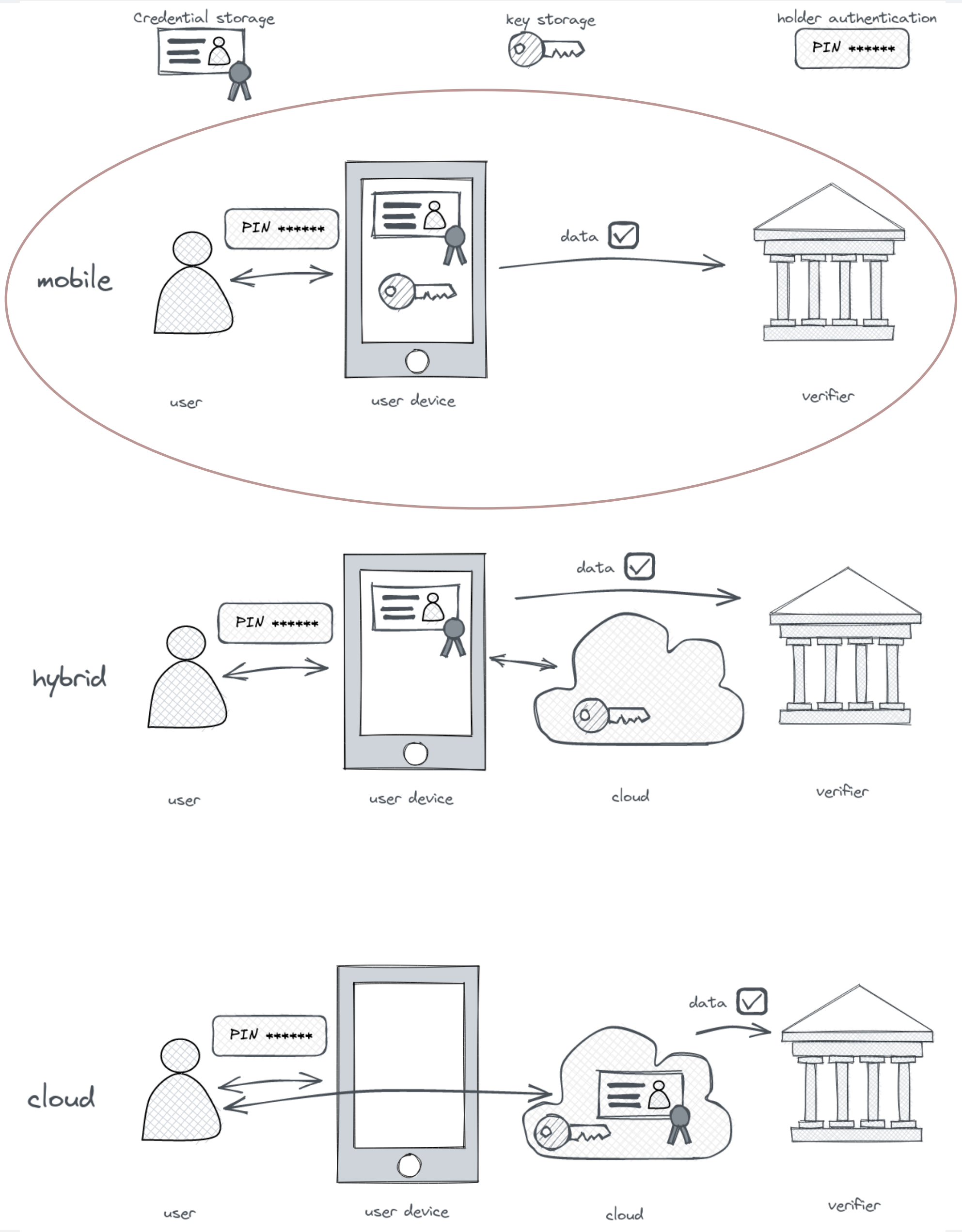
Wallet Architectures differentiated by

- VC storage location
- Key storage location
- User authentication

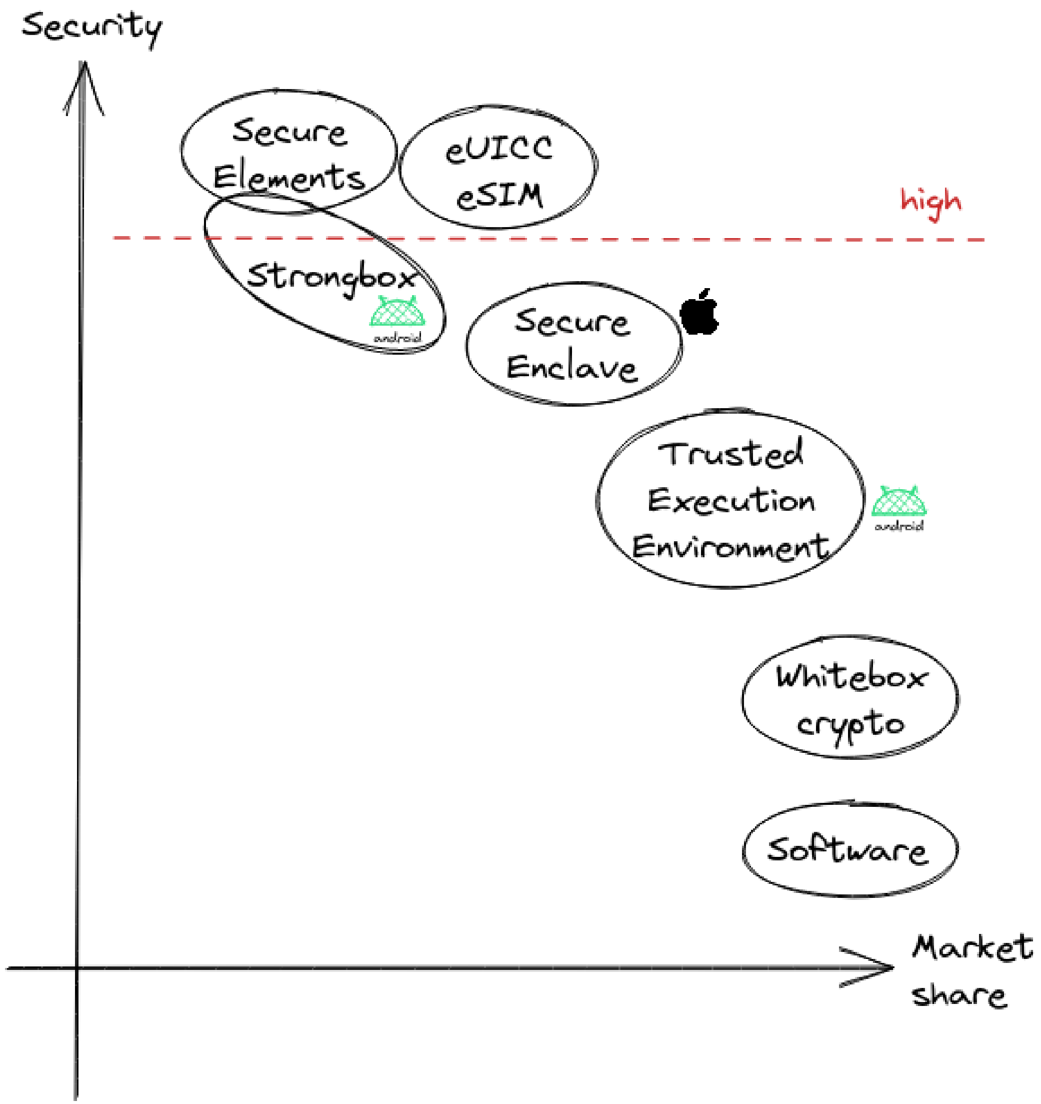
Wallet Architectures implications

- Backup and recovery
- Multidevice support
- Privacy implications
- Offline support
- User interface
- Level of assurance

- **Focus of the DIF work**
- Mobile, native App



The Existing Tools



Mobile Market

- The mobile device market is heavily fragmented
- This makes it difficult to build solutions for high market share
- Different solutions for secure storage
- Relying (partly) on OS security mechanism

Device binding

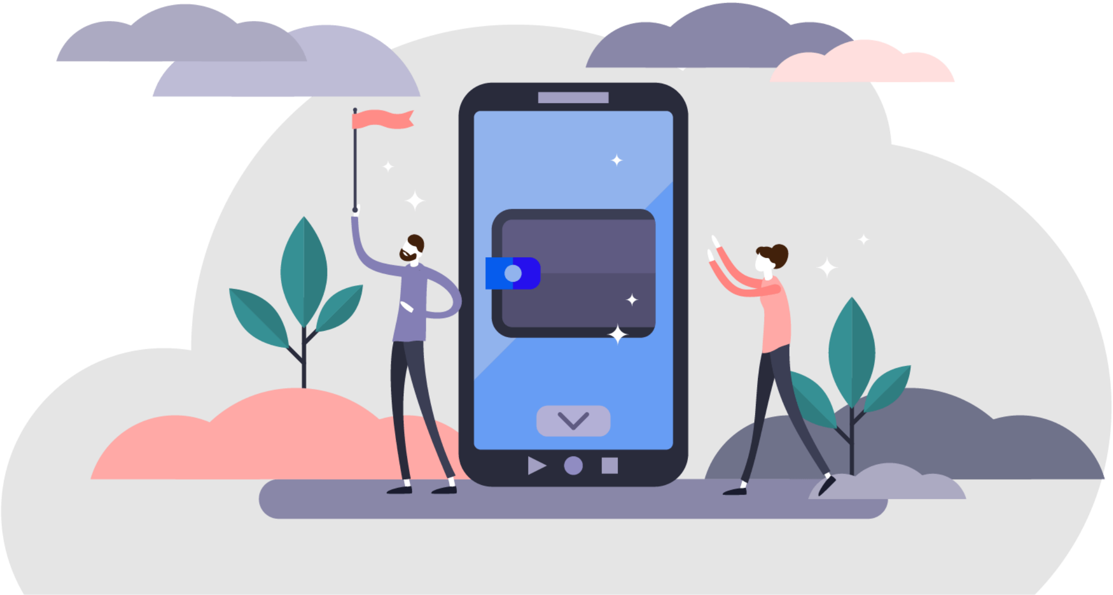
(authentication factor possession)

Holder binding

(authentication factor knowledge/biometry)

Wallet authentication

(integrity and authencity of the wallet)



Device Binding

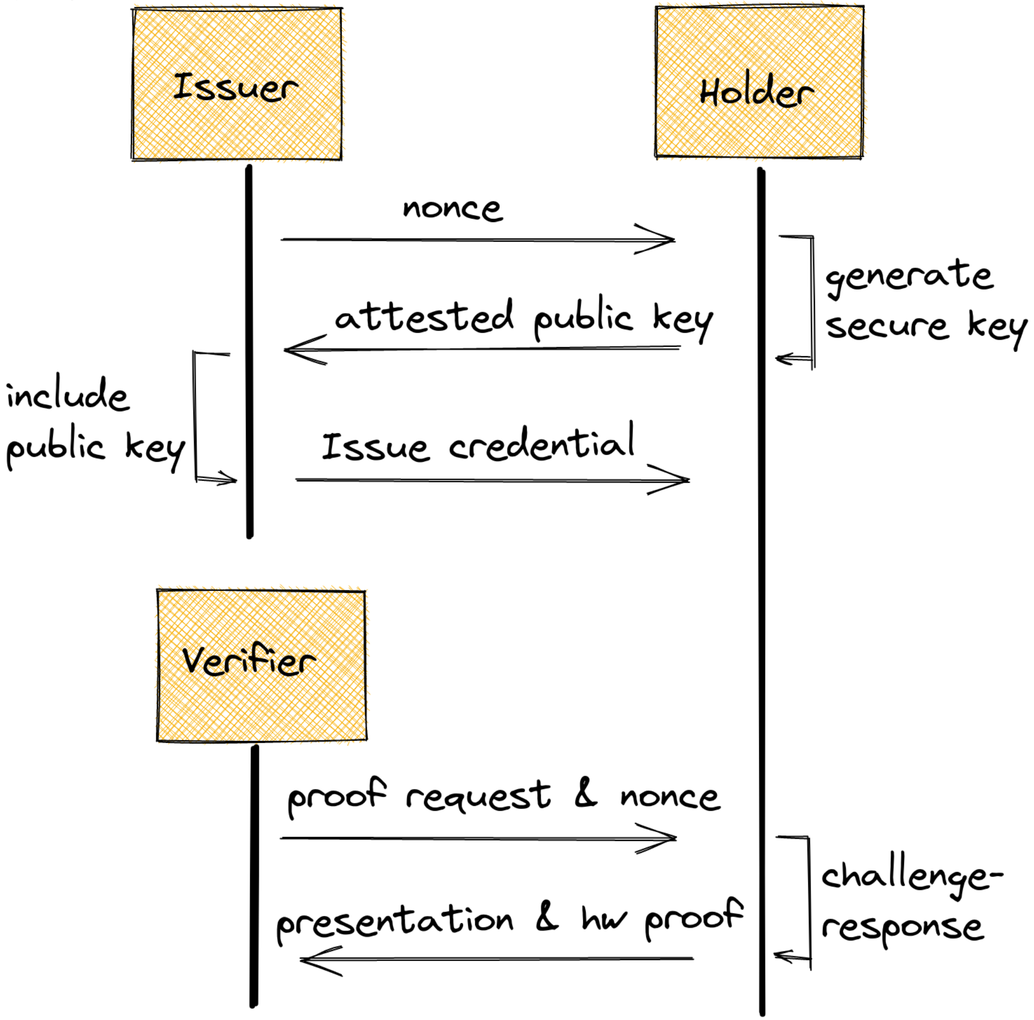
Device Binding Solution

- Smallest common denominator for all hardware-backed crypto systems
  - Elliptic Curve NIST P256 with ECDSA-SHA256 and similar
- Pro:
  - simple, well-understood crypto system
- Contra:
  - No backup & recovery strategy possible (more on this later)
  - Adding a unique, trackable attribute

Device Binding with ZKP

- ZKP in mobile hardware takes 5-10 (?) years

DIF Wallet Security WG



Holder binding/authentication

Enable Two-factor-authentication

- Knowledge factor (e.g. PIN)
- Inherence factor (e.g. biometrics)

Binding holder to the wallet

- Holder’s authentication reference data is stored in the wallet
- Holder authentication check is performed internally in the wallet
- Wallet is a trusted device that the issuer and verifier must rely on
- better protection for biometric data, but requirement for trusted wallet

Best practices

- Biometry on mobile phones is easy to circumvent and not yet sufficient for regulated use cases
  - BSI TR-03166 Technical Guideline for Biometric Authentication Components in Devices for Authentication
- PIN is a secure and necessary method
  - System-PIN (operating system)
  - separate App-PIN or SE-PIN

Authenticity of the Wallet

Wallet Authentication

- mobile OS presents a less-trusted, complex layer in front of trusted, high secure hardware key storage
- use existing mechanisms to verify and increase trust into the mobile phone
  - **Android SafetyNet**
  - **iOS device check**
- use **key attestations** to proof keys were generated in trusted hardware
- additional certification processes are possible
  - Hardware key storage
  - Accompanying mobile phone app

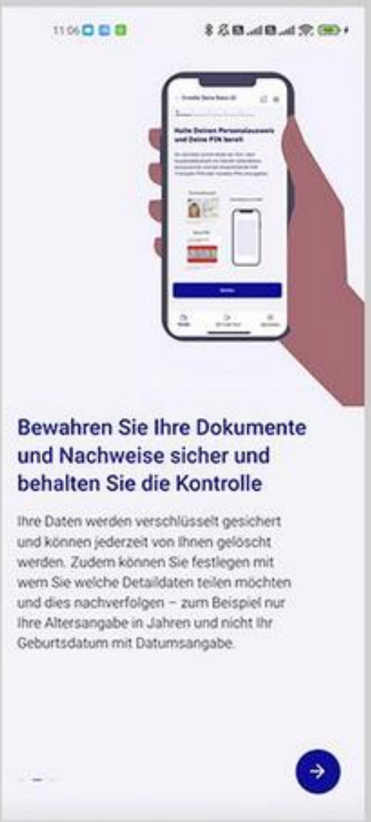
Gaining Experiences from german Chancellary Project (2021)

ID Wallet for Driving License credentials

- Implement device binding and wallet authentication
- Issuing ~20.000 credentials within 2 days

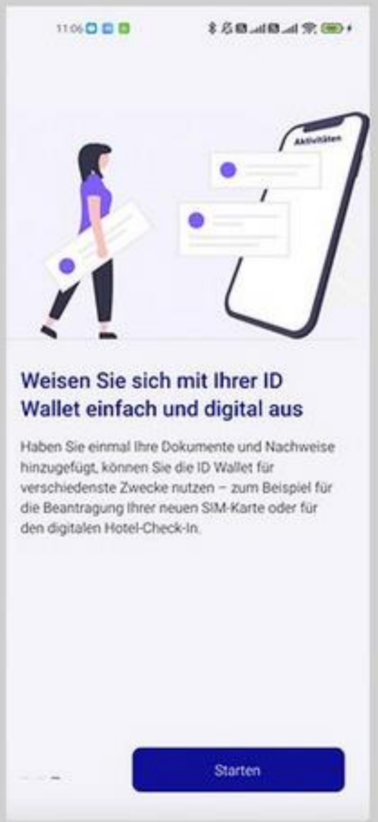
Learnings

- Live status was halted due to massive overload and missing concepts for trusted verifiers
- Wallet Security concepts worked well
- Mechanisms were proprietary for the project and not standardized for use of wider community



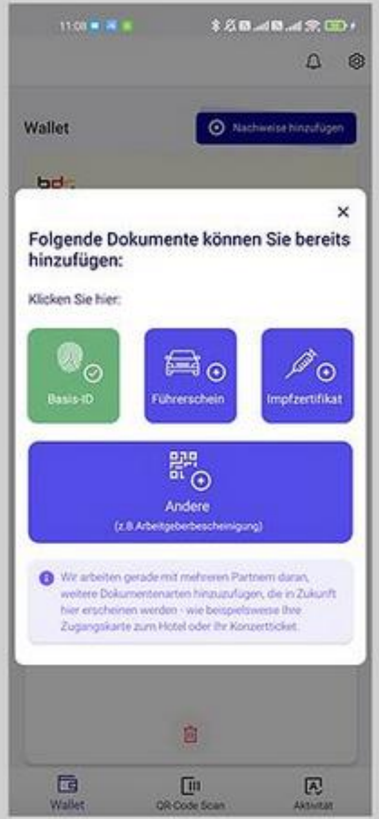
Bewahren Sie Ihre Dokumente und Nachweise sicher und behalten Sie die Kontrolle

Ihre Daten werden verschlüsselt gesichert und können jederzeit von Ihnen gelöscht werden. Zudem können Sie festlegen mit wem Sie welche Detaildaten teilen möchten und dies nachverfolgen – zum Beispiel nur Ihre Altersangabe in Jahren und nicht Ihr Geburtsdatum mit Datumsangabe.



Weisen Sie sich mit Ihrer ID Wallet einfach und digital aus

Haben Sie einmal Ihre Dokumente und Nachweise hinzugefügt, können Sie die ID Wallet für verschiedenste Zwecke nutzen – zum Beispiel für die Beantragung Ihrer neuen SIM-Karte oder für den digitalen Hotel-Check-In.



Folgende Dokumente können Sie bereits hinzufügen:

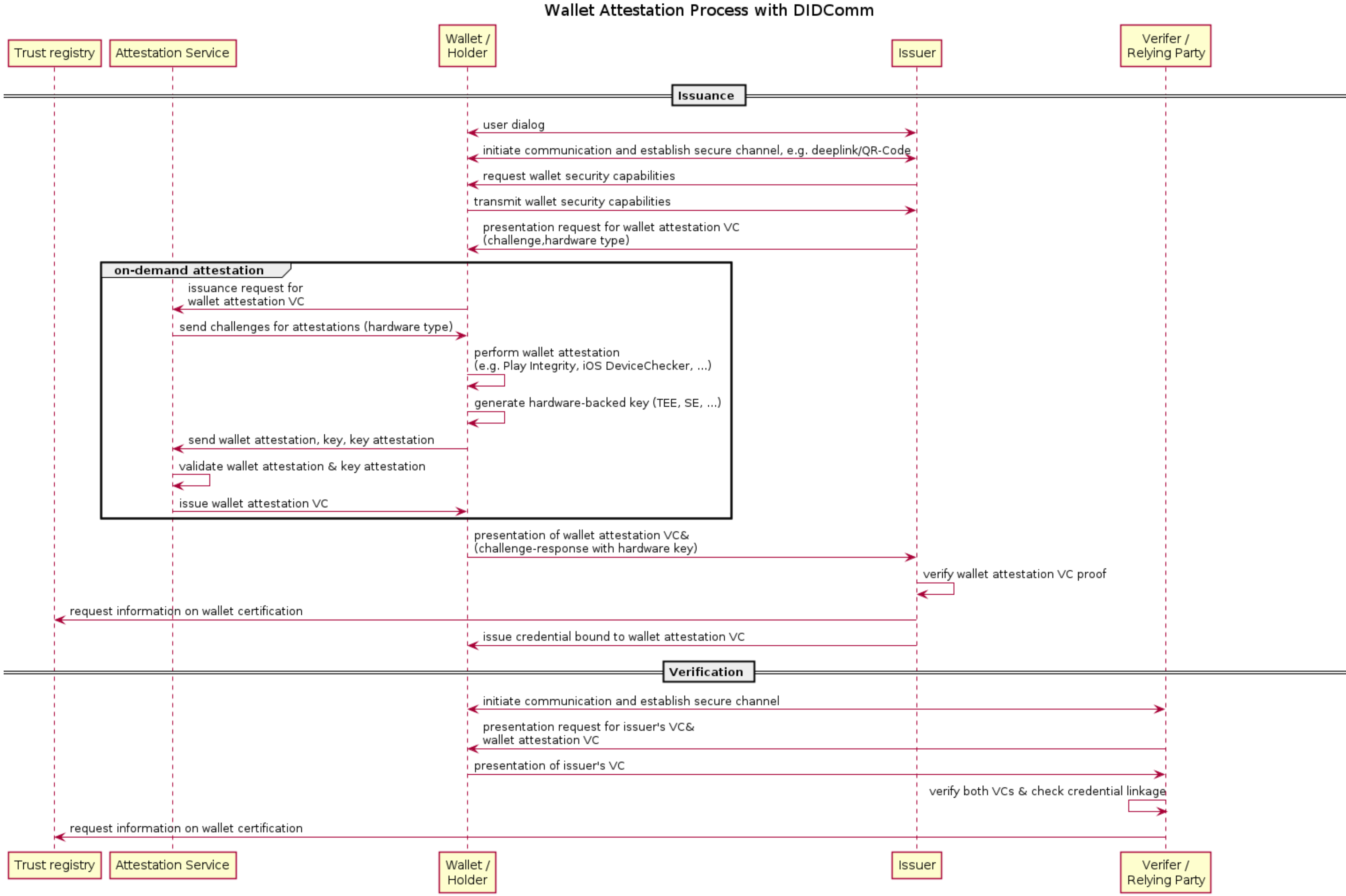
Klicken Sie hier:

Wir arbeiten gerade mit mehreren Partnern daran, weitere Dokumentenarten hinzuzufügen, die in Zukunft hier erscheinen werden - wie beispielsweise Ihre Zugangskarte zum Hotel oder Ihr Konzertticket.

DIF Wallet

Security Approach

DIDComm – like flow



Wallet Attestation Process with DIDComm

Trust registry

Attestation Service

Wallet / Holder

Issuer

Verifer / Relying Party

Issuance

user dialog

initiate communication and establish secure channel, e.g. deeplink/QR-Code

request wallet security capabilities

transmit wallet security capabilities

presentation request for wallet attestation VC (challenge,hardware type)

on-demand attestation

issuance request for wallet attestation VC

send challenges for attestations (hardware type)

perform wallet attestation (e.g. Play Integrity, iOS DeviceChecker, ...)

generate hardware-backed key (TEE, SE, ...)

send wallet attestation, key, key attestation

validate wallet attestation & key attestation

issue wallet attestation VC

presentation of wallet attestation VC& (challenge-response with hardware key)

verify wallet attestation VC proof

request information on wallet certification

issue credential bound to wallet attestation VC

Verification

initiate communication and establish secure channel

presentation request for issuer's VC& wallet attestation VC

presentation of issuer's VC

verify both VCs & check credential linkage

request information on wallet certification

Trust registry

Attestation Service

Wallet / Holder

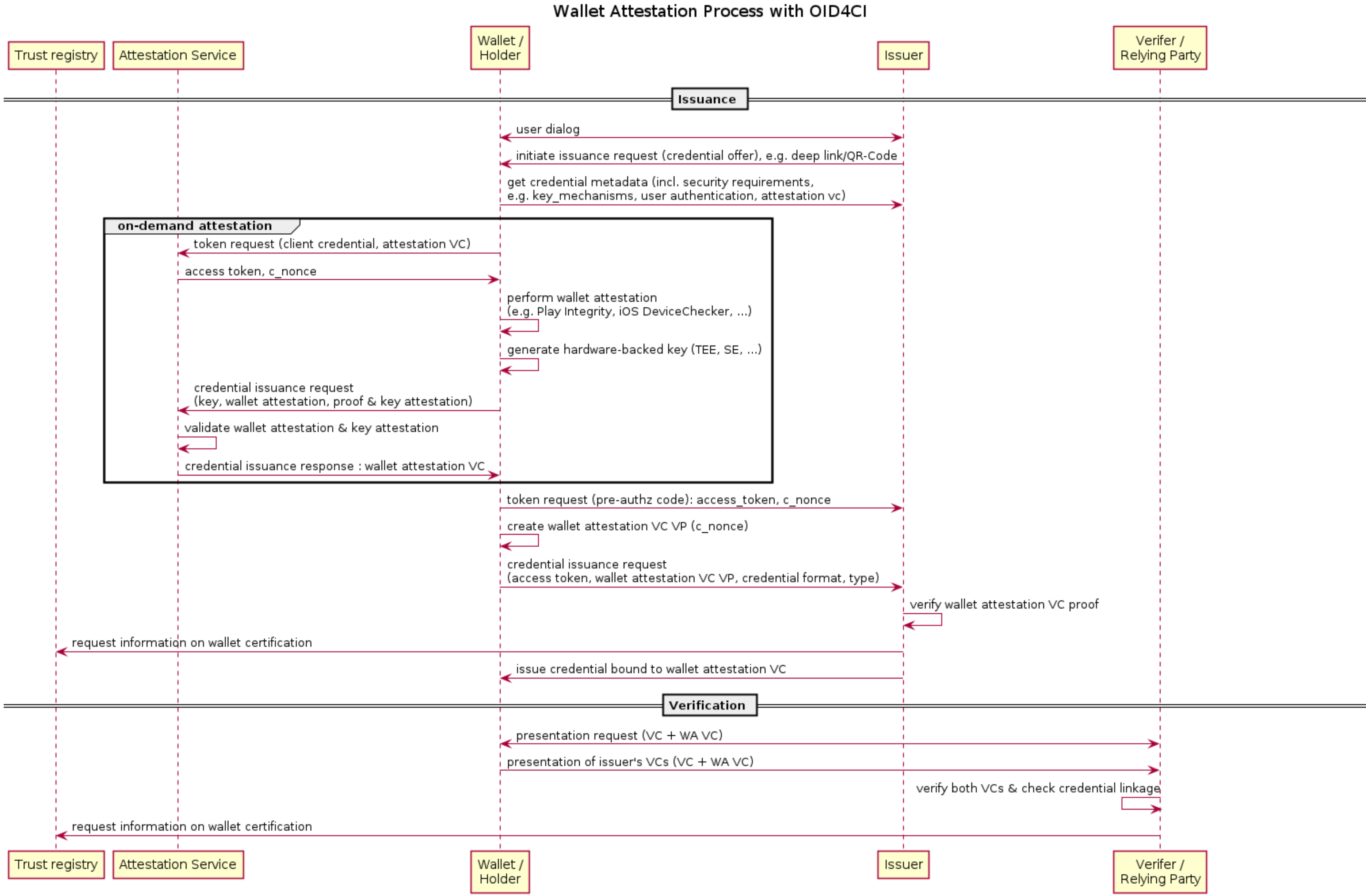
Issuer

Verifer / Relying Party

iDunion

DIF Wallet Security Approach

OID4CI – like flow



Wallet Attestation Process with OID4CI

Issuance

user dialog

initiate issuance request (credential offer), e.g. deep link/QR-Code

get credential metadata (incl. security requirements, e.g. key_mechanisms, user authentication, attestation vc)

on-demand attestation

token request (client credential, attestation VC)

access token, c_nonce

perform wallet attestation (e.g. Play Integrity, iOS DeviceChecker, ...)

generate hardware-backed key (TEE, SE, ...)

credential issuance request (key, wallet attestation, proof & key attestation)

validate wallet attestation & key attestation

credential issuance response : wallet attestation VC

token request (pre-authz code): access_token, c_nonce

create wallet attestation VC VP (c_nonce)

credential issuance request (access token, wallet attestation VC VP, credential format, type)

verify wallet attestation VC proof

request information on wallet certification

issue credential bound to wallet attestation VC

Verification

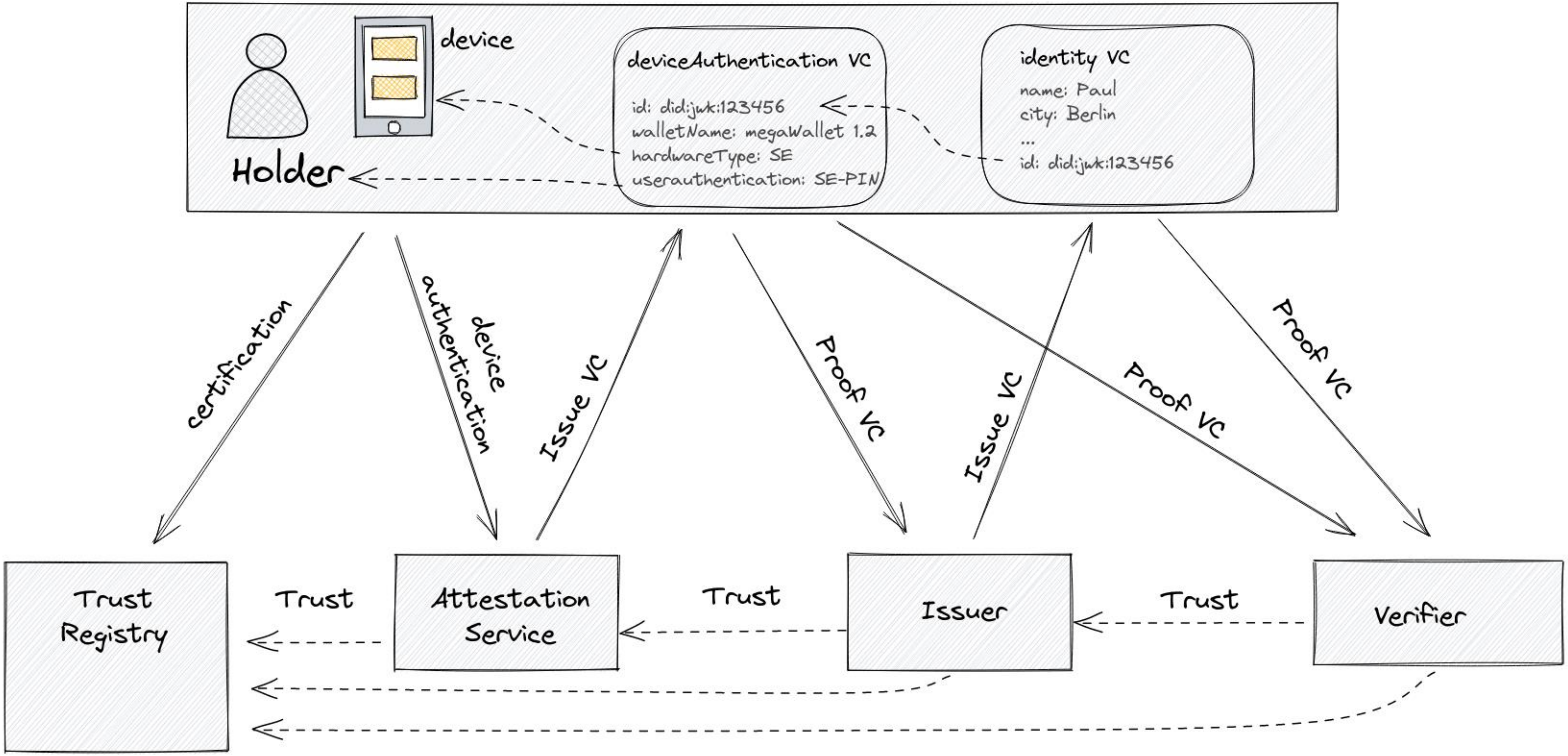
presentation request (VC + WA VC)

presentation of issuer's VCs (VC + WA VC)

verify both VCs & check credential linkage

request information on wallet certification

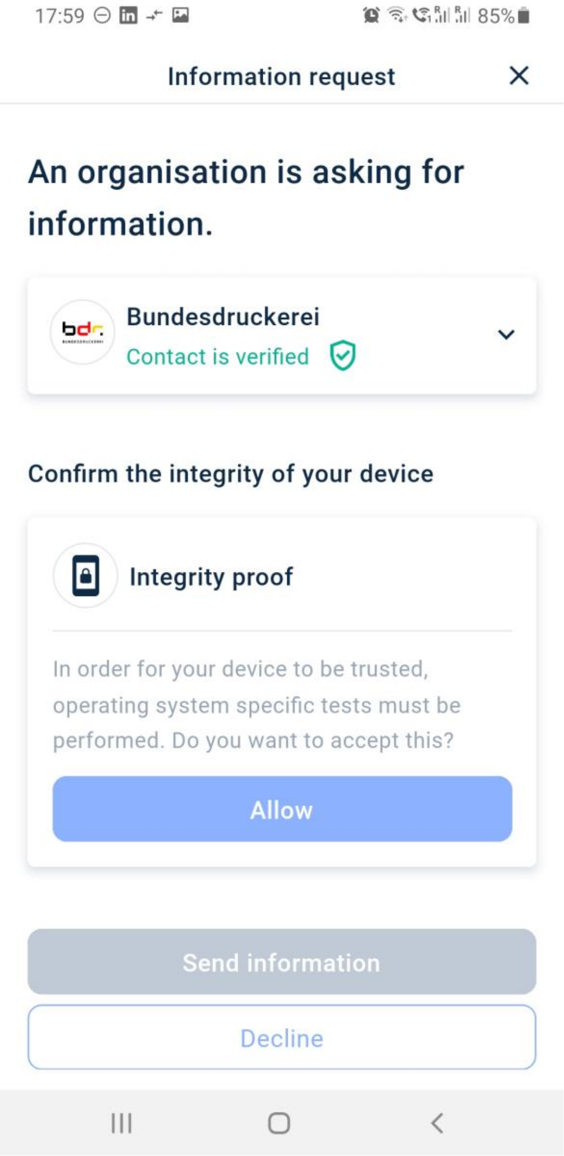
- **Trust Model**


device
Holder
deviceAuthentication VC
id: did:jwk:123456
walletName: megaWallet 1.2
hardwareType: SE
userauthentication: SE-PIN
identity VC
name: Paul
city: Berlin
...
id: did:jwk:123456
certification
device authentication
Issue VC
Proof VC
Issue VC
Proof VC
Proof VC
Trust Registry
Trust
Attestation Service
Trust
Issuer
Trust
Verifier

• Attestation VC Example

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2022/credentials/walletAuthentication/v1"   ],
  "id": "https://example.com/id/123456789",
  "credentialSchema": {
    "id": "https://www.schema.org/examples/deviceAuthentication.json",
    "type": "WalletAuthenticationSchema"   },
  "type": ["VerifiableCredential" , "WalletAuthenticationCredential"],
  "issuer": "https://example.com/issuers/14",
  "issuanceDate": "2021-09-11T16:02:04Z",
  "expirationDate": "2021-12-11T16:02:04Z",
  "credentialSubject": {
    "id": "did:jwk:123",
    "deviceAuthentication": {
      "walletName": "Example Wallet",
      "walletVersion": “Android 1.3.0",
      "hardwarePublicKey": "did:jwk:123",
      "holderAuthentication": ["FaceID", "PIN"],
     }
  }
}
```

- **Demo with Lissi**



17:59 85%

Information request

An organisation is asking for information.

Bundesdruckerei
Contact is verified

Confirm the integrity of your device

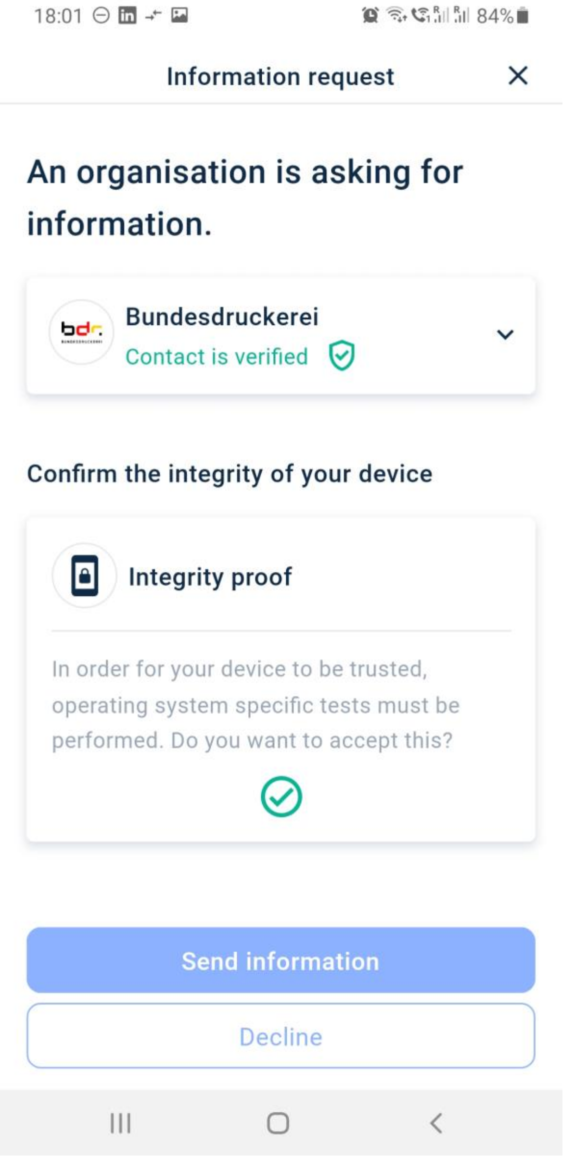
Integrity proof

In order for your device to be trusted, operating system specific tests must be performed. Do you want to accept this?

Allow

Send information

Decline



18:01 84%

Information request

An organisation is asking for information.

Bundesdruckerei
Contact is verified

Confirm the integrity of your device

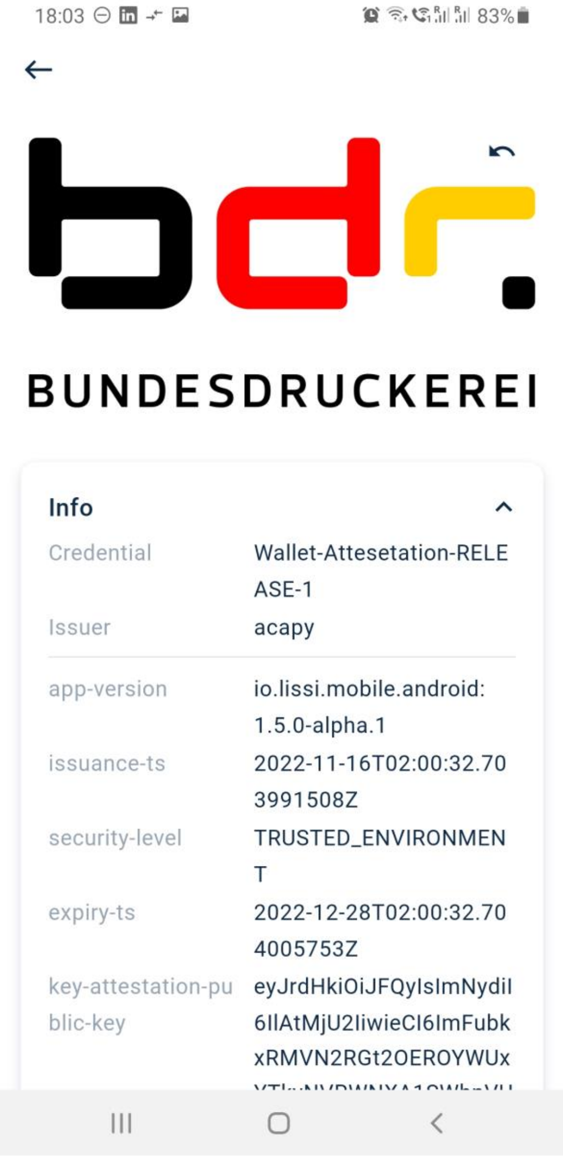
Integrity proof

In order for your device to be trusted, operating system specific tests must be performed. Do you want to accept this?

✓

Send information

Decline



18:03 83%

BUNDESDRUCKEREI

Info

Credential	Wallet-Attesetation-RELEASE-1
Issuer	acapy
app-version	io.lissi.mobile.android:1.5.0-alpha.1
issuance-ts	2022-11-16T02:00:32.703991508Z
security-level	TRUSTED_ENVIRONMENT
expiry-ts	2022-12-28T02:00:32.704005753Z
key-attestation-public-key	eyJrdHkiOiJFQyIsImNydiI6IlAtMjU2IiwieCI6ImFubkxRMVN2RGt2OEROYWUx

DIF Wallet Security Approach

Advantages

- Generic model usable for all issuers and verifiers
- Works with W3C and Anoncreds, DIDComm and OID4VC
- Wallet Attestation as W3C VC including device binding and wallet authentication
- Complexity of key/wallet attestations is handled by the attestation service, not by the issuers/verifiers
- Design respects privacy of the holder, scaling and limits of attestations

Disadvantages

- Hardware-bound keys prevent backup&recovery
- Additional tracking risk

Open Topics

- How is Wallet Attestation triggered? By the issuer or by the holder wallet?
- Should the issuer link the attestation VC or directly copy the device-bound key? Does the holder show the Attestation VC to the Verifier?

Summary and Next Steps

Summary

- Successfully developed and tested remote attestation service
- Improved wallet security for SSI ecosystem

Next steps

- Whitepaper coming in ~2 weeks
- Continue the work with W3C VCs
- Continue the work for OID4VC

Thanks!

Paul Bastian, Bundesdruckerei GmbH
paul.bastian@bdr.de

in @idunion

@IDunion_SCE

✉ contact@idunion.org

https://www.idunion.org/