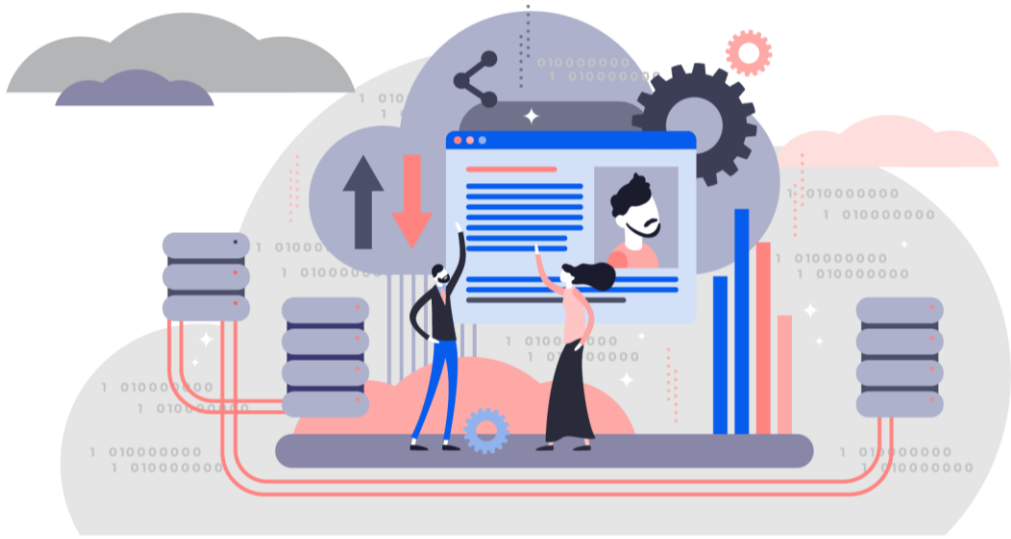
Framework for Wallet Security in Identity Ecosystems

Paul Bastian, Bundesdruckerei/IDunion

Agenda

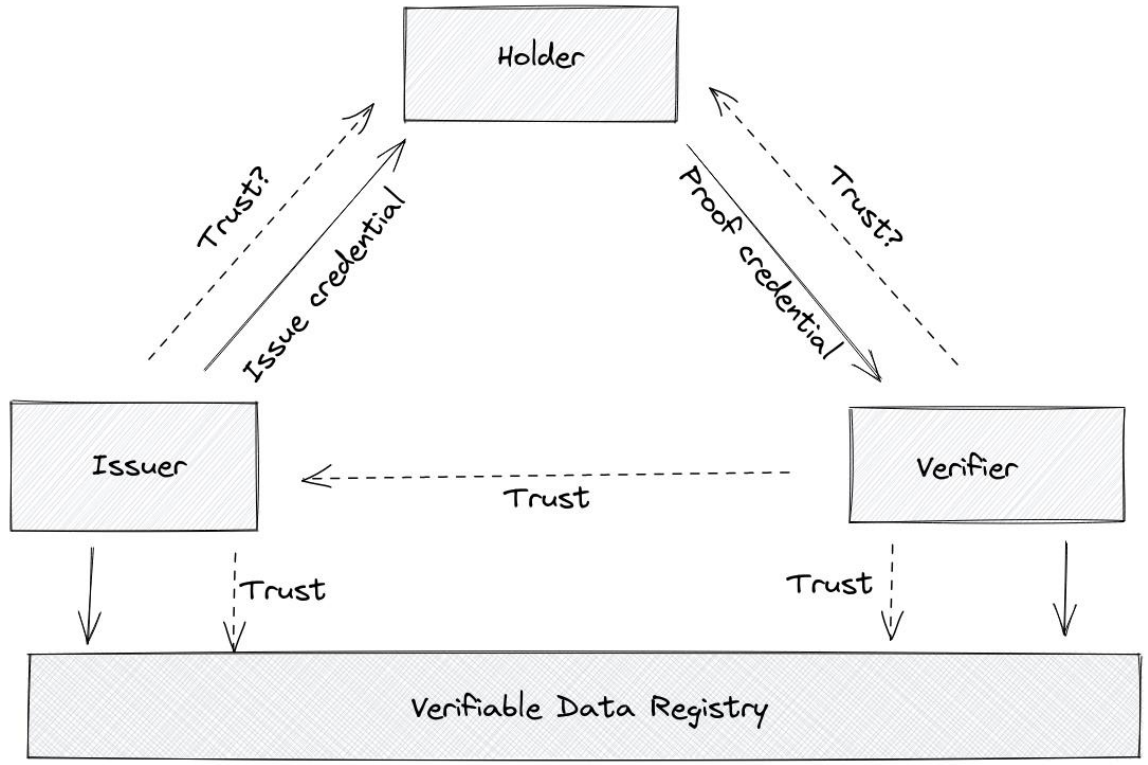


1. Motivation & eIDAS 2.0
2. Wallet Architectures
3. The Journey
4. Regulations & Tools
5. Three Pillars of Wallet Security
    i. Integrity of the Credential
    ii. Authenticity of the Holder
    iii. Authenticity of the Wallet
6. Attestation Process and Trust Model
7. Demo
8. Next Steps and Outlook

Motivation: The Overlooked Trust Relationship

Trust in the Verifiable Credentials Ecosystem

- Traditional trust relationship between Issuer/Verifier and towards the Verifiable Data Registry
- Trust relationship to the Holder/Wallet is not as mature



Issuer

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

Verifier

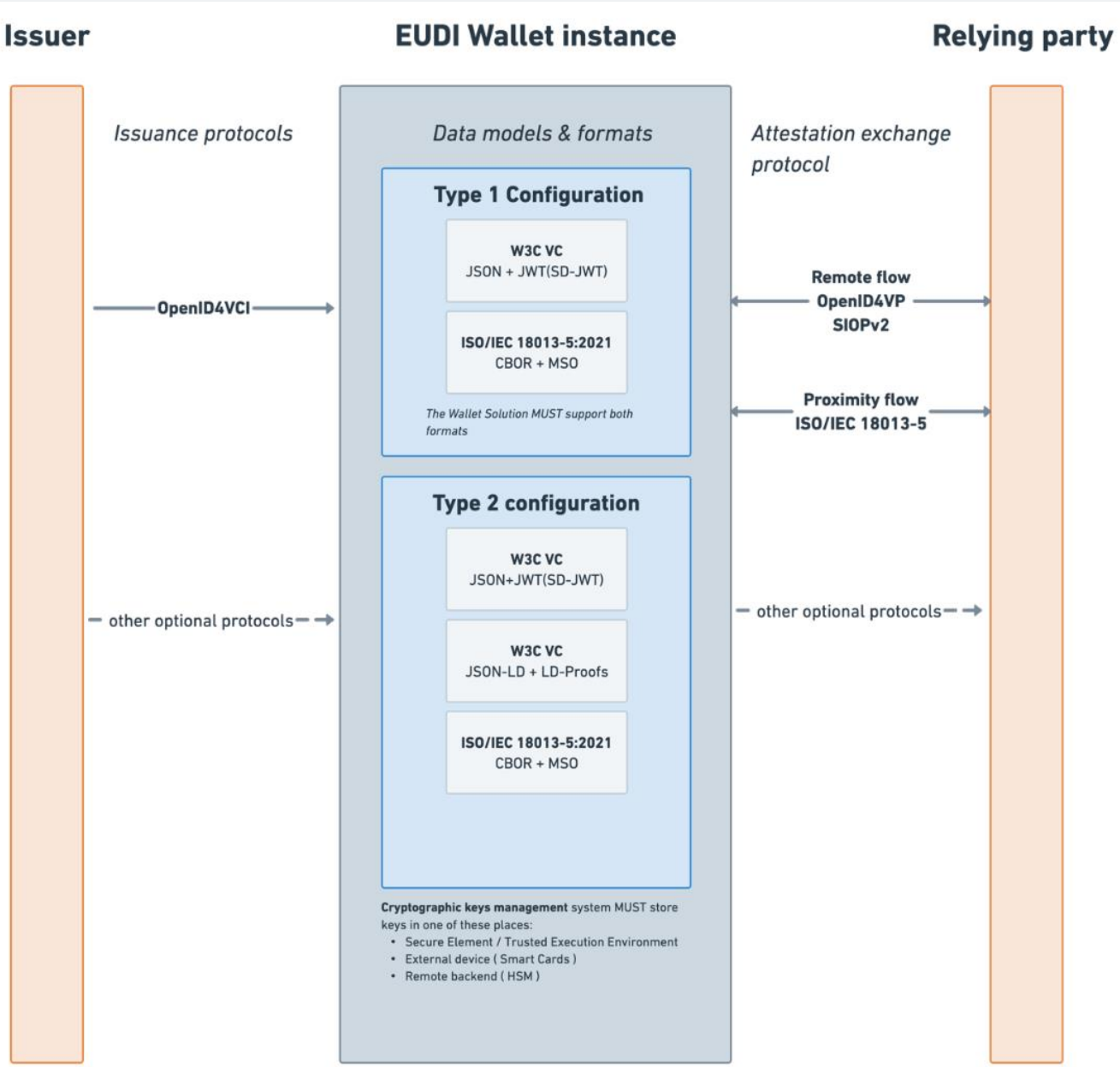
Is the holder the rightful owner of this credential and to what degree can he plausibly prove that?

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

eIDAS 2.0 ARF

Motivation

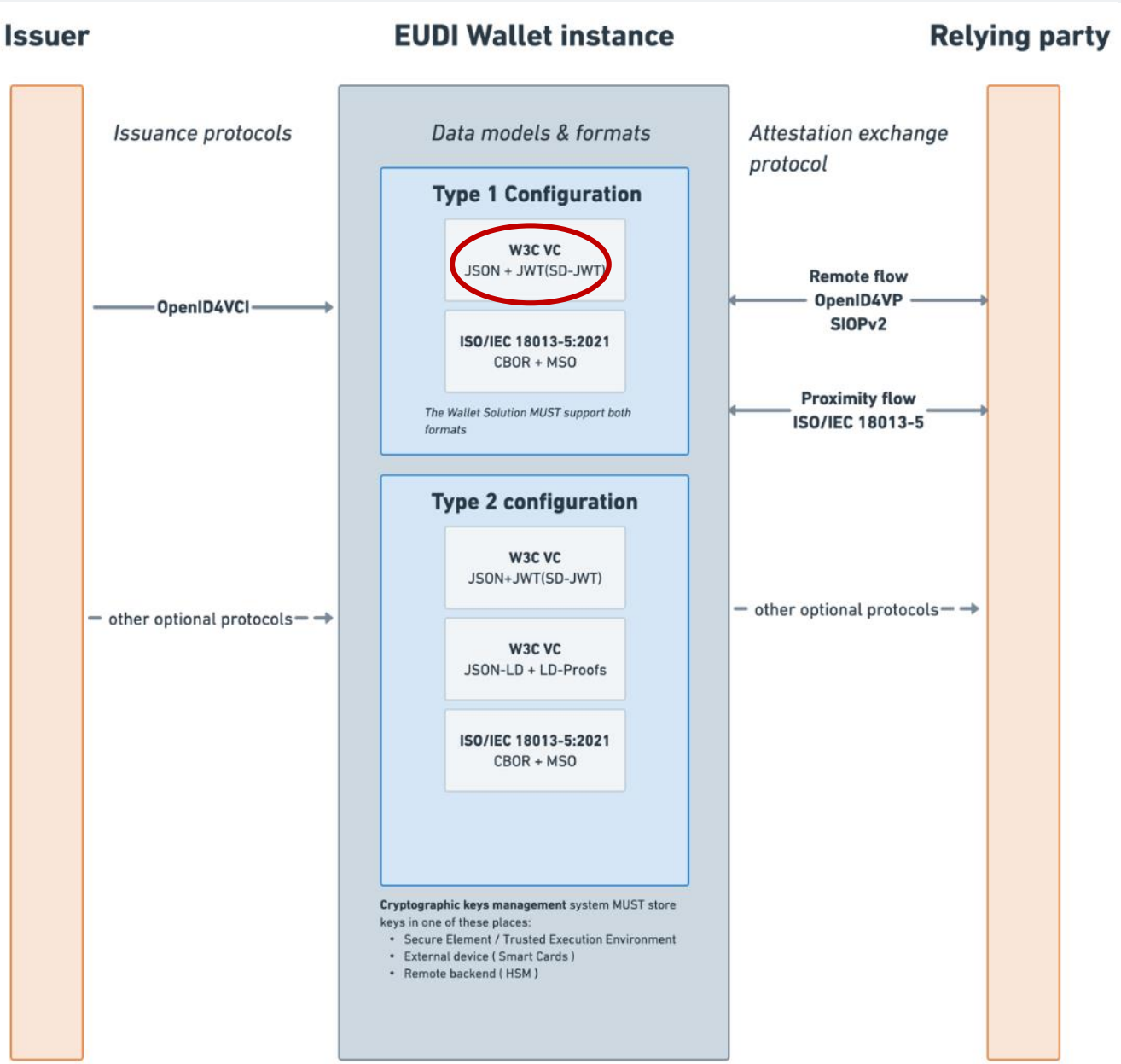
- Decentralized identity ecosystems brings use cases from different domains together
  - Regulated and non-regulated issuers have different security requirements
- eIDAS ARF address these requirements
  - Type 1 Configuration for “high-security credentials” (hardware-bound)
  - Type 2 Configuration for “other credentials” (backup & portability enabled)



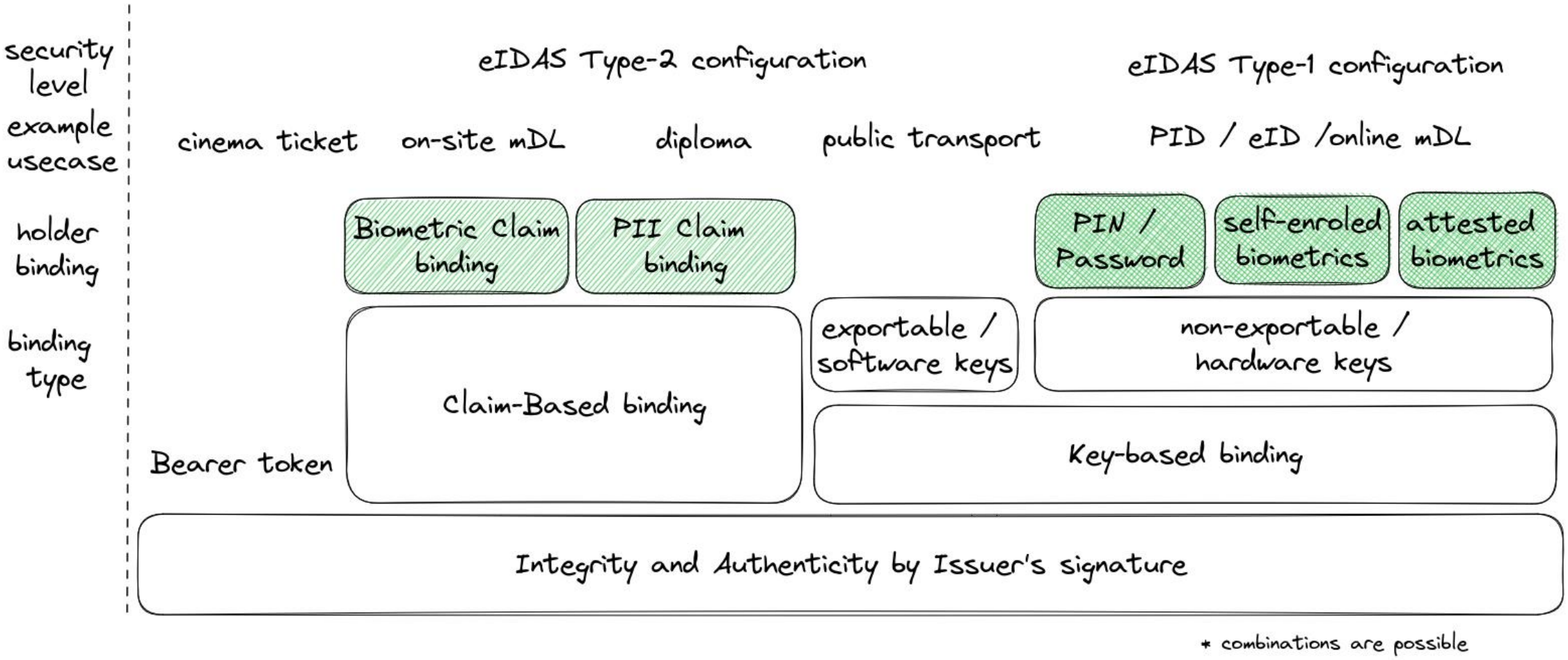
eIDAS 2.0 ARF

Motivation

- Decentralized identity ecosystems brings use cases from different domains together
  - Regulated and non-regulated issuers have different security requirements
- eIDAS ARF address these requirements
  - Type 1 Configuration for “high-security credentials” (hardware-bound)
  - Type 2 Configuration for “other credentials” (backup & portability enabled)



• Binding Types for PID & EAAs



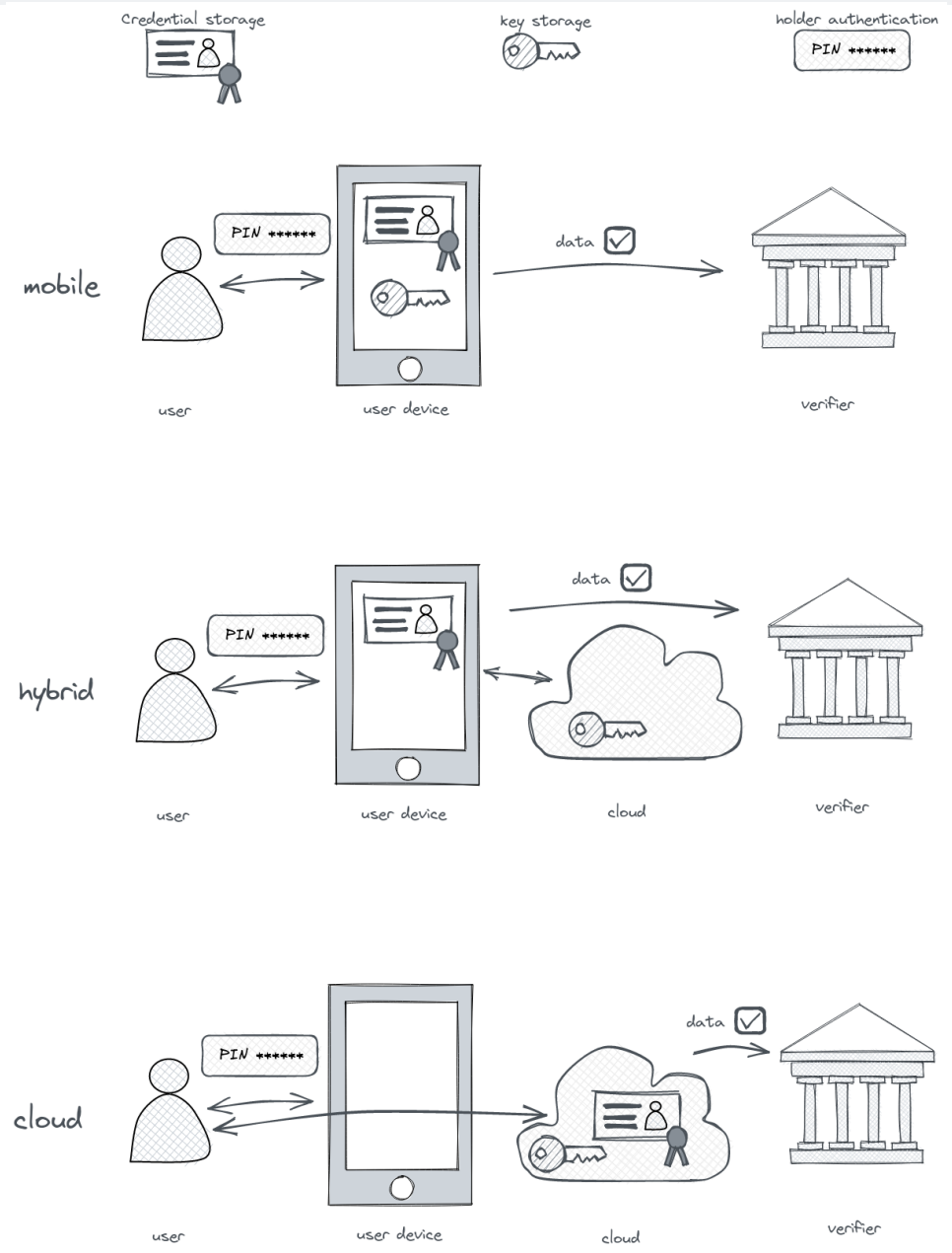
Wallet Security Architectures

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

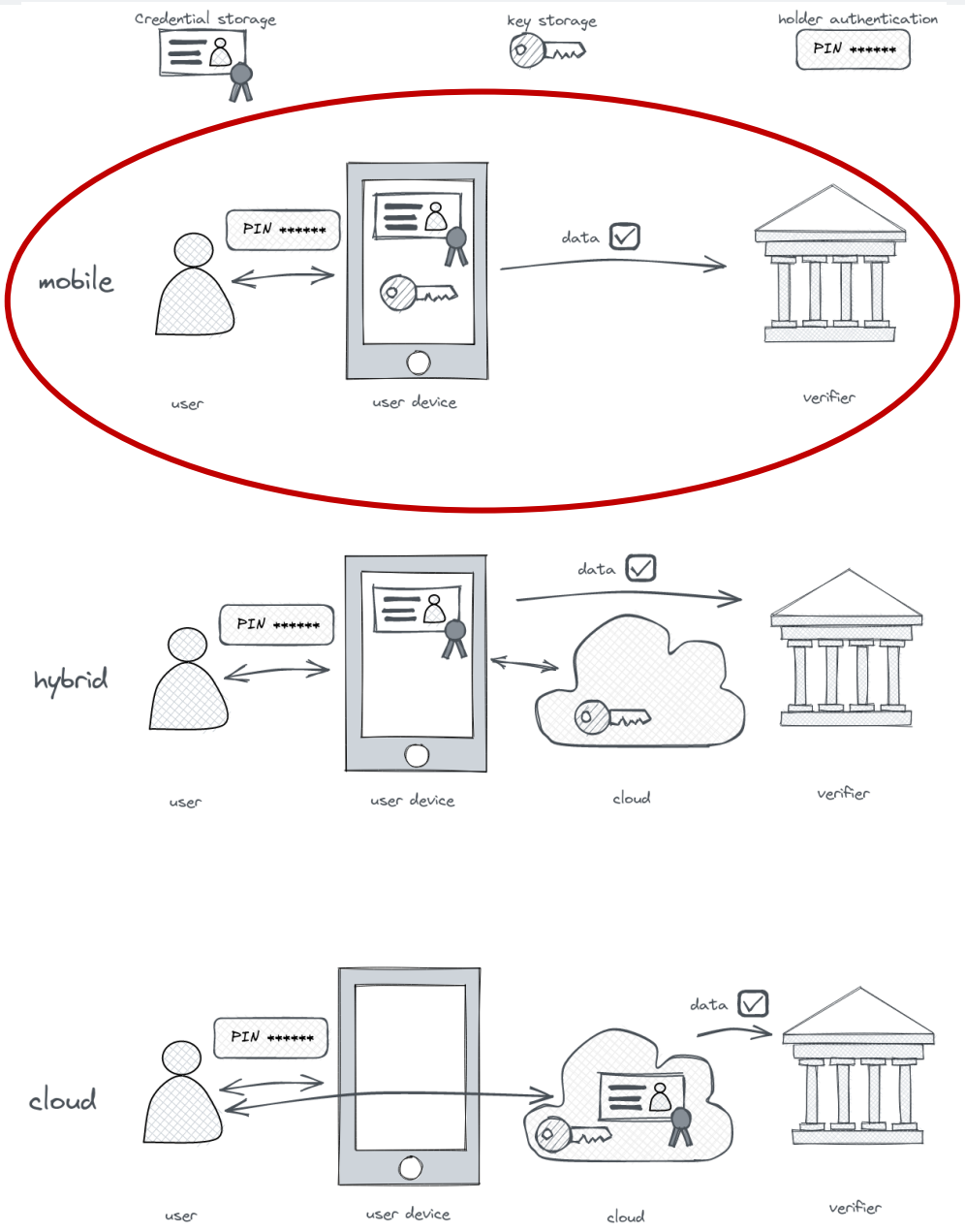
Wallet Architectures differentiated by

- 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

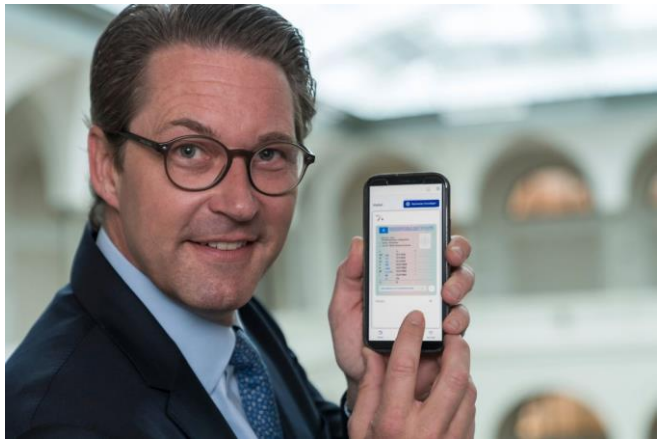
- **Focus of the our work**
- Mobile, native App



The Journey

Timeline

- 2021
  - prototyping and implementing proprietary wallet attestation for German Chancellary project “ID Wallet”
  - Short-lived project provided valueable learnings
- 2022
  - starting the DIF Wallet Security Working Group
  - Drafting ideas for standardized approach
  - Prototype with Lissi (based on DIDComm&Anoncreds)
  - RWOT#11 paper on W3C VCDM holder binding
- 2023
  - Paper “Concepts for Secure Wallets in Decentralized Identity Ecosystems” published for HMD journal
  - First successful End-to-End demonstration with Lissi using OpenID4VCI
  - VCDM PR for confirmation methods



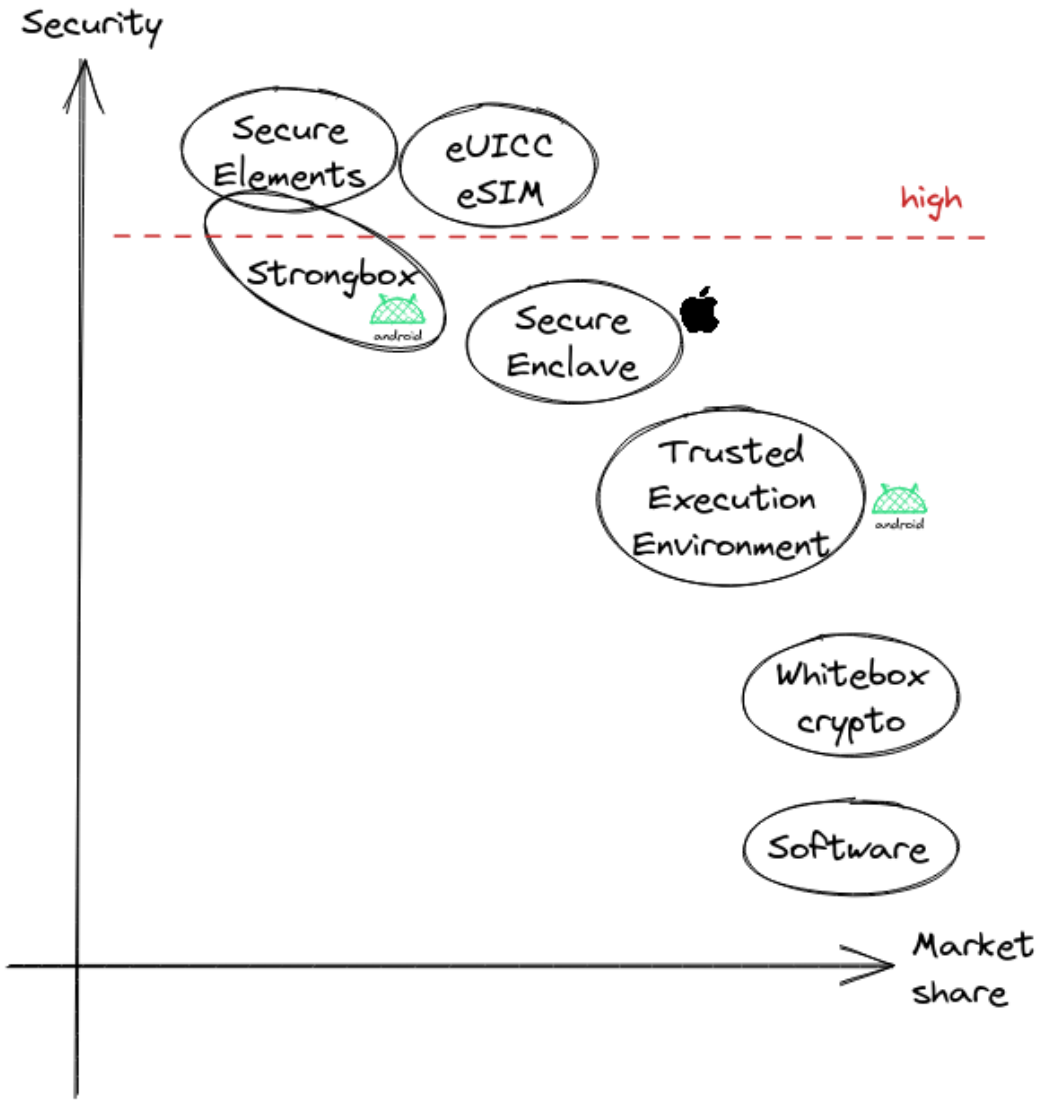
The Existing Tools

Regulatory requirements

- protection against
  - credential duplication/theft (extraction)
  - online/offline guessing (impersonation)
  - others.. (not wallet relevant)
- the wallet enables the issuer to achieve a certain level of assurance (LoA)

Mobile Market

- market of secure cryptographic key storage is very fragmented
- relying (partly) on OS security mechanism



Device binding

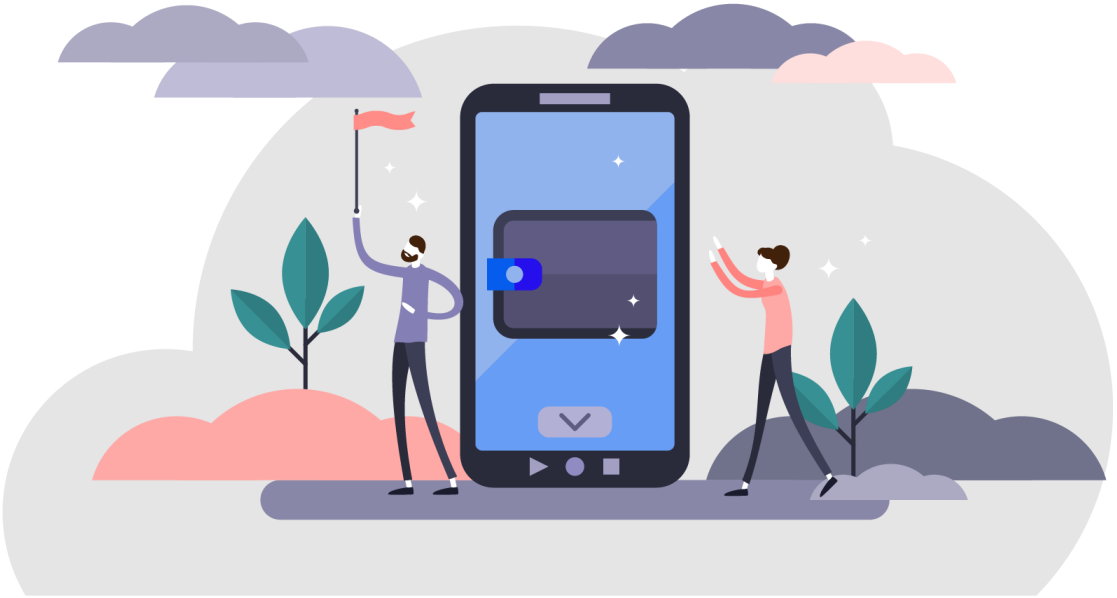
(authentication factor possession)

User binding

(authentication factor knowledge/biometry)

Wallet authentication

(integrity and authencity of the wallet)



Solution Components

Device Binding

- hardware-backed crypto systems are very restrained
  - NIST P256 with ECDSA-SHA256 as the smallest common denominator
  - simple, well-understood crypto system
  - SD-JWT, crypto agility by JOSE, (theoretically) PQC ready
- No backup & recovery strategy possible
- ZKP in mobile hardware is not available and might take 5-10 (?) years

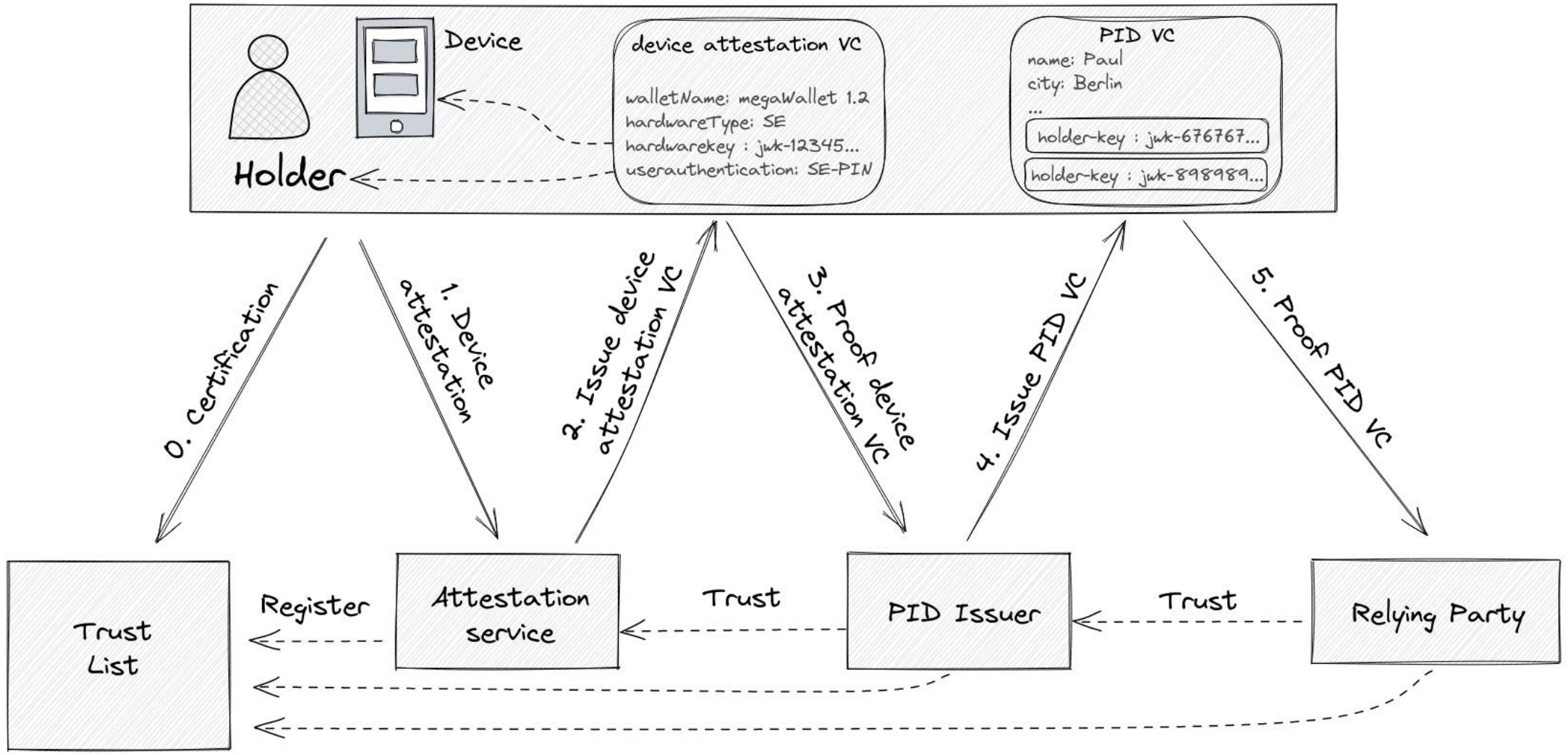
User/Holder Binding

- Local, on-device authentication
- Biometrics have many challenges and security issues (weak sensors, unknown FAR/FRR, attested enrolment, privacy..)
- Regulators are still in favour of PINs (some problems here as well, System-PIN vs App/SE-PIN)

Wallet Authentication

- mobile OS presents a less-trusted, complex layer in front of trusted, high secure hardware key storage
- Use existing technology by mobile OS: iOS Device Check, Android SafetyNet/Integrity API
- Use Key attestations (not available on iOS)

- **Trust Model**


Device
Holder
device attestation VC
walletName: megaWallet 1.2
hardwareType: SE
hardwarekey : jwk-12345...
userauthentication: SE-PIN
PID VC
name: Paul
city: Berlin
...
holder-key : jwk-676767...
holder-key : jwk-898989...
0. certification
1. Device attestation
2. Issue device attestation VC
3. Proof device attestation VC
4. Issue PID VC
5. Proof PID VC
Trust List
Register
Attestation service
Trust
PID Issuer
Trust
Relying Party

Attestation VC Example

```
{
  "typ": "vc+jwt",
  "alg": "ES256",
  "kid": "1" //from https://attestation-service.ssi.tir.budru.de/.well-known/jwks_uri
}
{
  "iss": "https://attestation-service.ssi.tir.budru.de",
  //no audience here for privacy reasons
  "sub" : "https://lissi.org",
  "iat": 1541493724,
  "exp": 1516247022, //expiration ~30 to 90 days..
  "type": "WalletAttestation",
  "wallet_name": "Lissi Dev",
  "wallet_version": "1.6.0",
  „key_type" : "STRONGBOX",
  "user_authentication" : "APP_PIN_6_DIGITS",
  "supported_LoA" : "https://eu-trust-list.eu/loa/substantial",
  "cnf": {
    "jwk" : {
      "kty": "EC",
      "crv": "P-256",
      "x": "TCAER19Zvu3OHF4j4W4vfSVoHIP1ILilDls7vCeGemc",
      "y": "ZxjiWWbZMQGHVWKVQ4hbSIirsVfuecCE6t4jT9F2HZQ"
    }
  }
}
```

The Wallet Attestation Concept

Advantages

- Point of Interoperability is the attestation VC schema
  - Not the attestation process and protocols between wallet and attestation service
  - Future Proof mechanism independent from specific technology
- Simplify attestations for issuers and verifiers
  - Issuers do not need to parse and analyze complex OS-specific attestation statements
  - Easy integration into existing issuance protocols
- Design respects privacy of the holder, scaling and limits of attestations

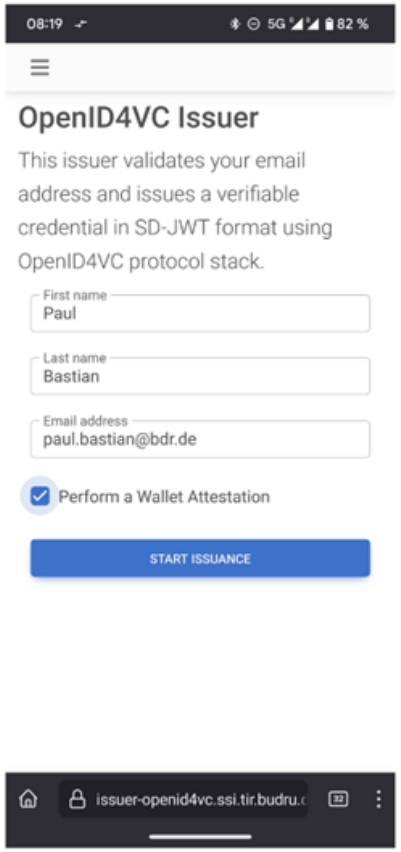
← Official Paper from HMD Journal (german)

Translated paper in English →

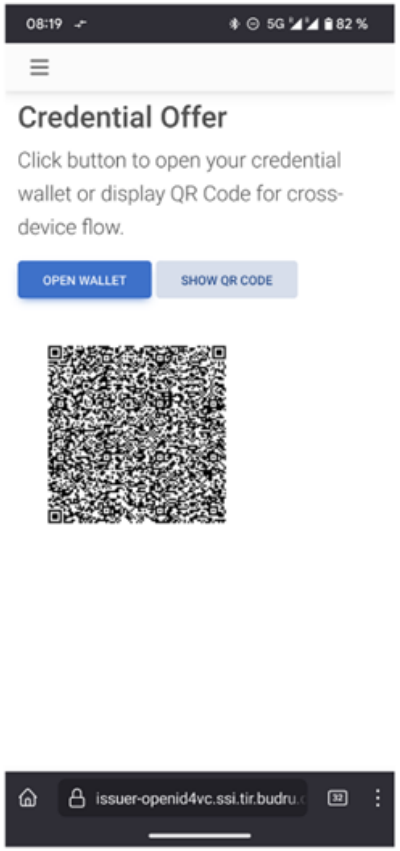
(the paper was submitted by 09/22, so some details have changed)

• IDunion Demo

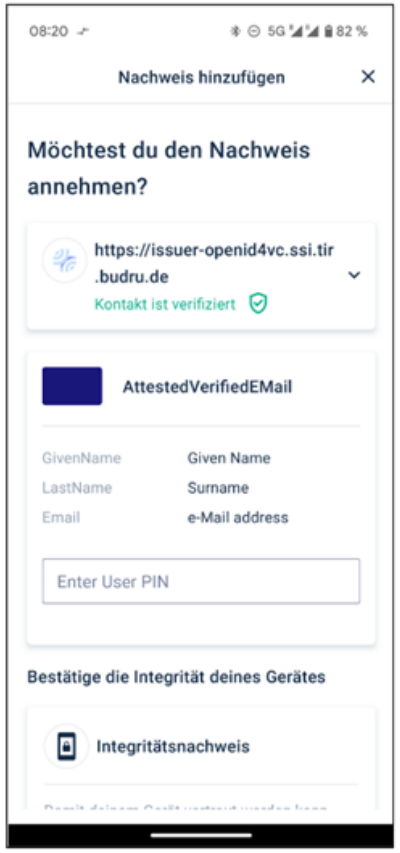
Demo of End-to-End Issuance with Wallet Attestation and Device Binding



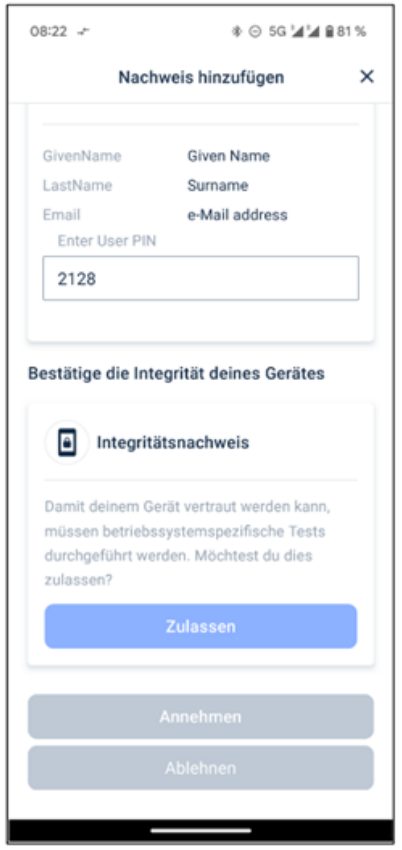
issuer's website as a starting point



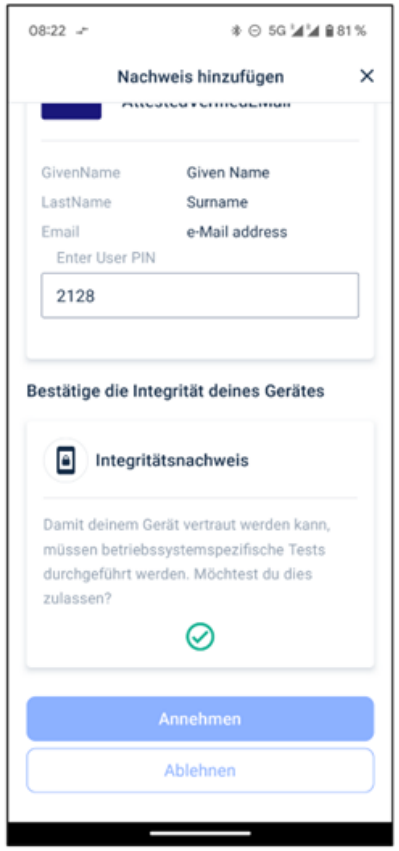
Wallet invocation with deeplink or QR-Code



Issuer Authentication with eIDAS 1 QWAC or EV certificates



UserPIN as a security feature of OpenID4VCI



Wallet Attestation for eIDAS Type-1 high assurance credential

W3C SD-JWT VC issued after validation of wallet attestation

Level of Assurances

Understanding LoAs

- LoAs are attributed for a whole identity system including:
  - Identity proofing
  - Issuance
  - Secure storage and Multi-Factor-Authentication
  - Recovation
  - Cryptography
- Therefore a wallet can support an LoA, but does not have a designated LoA
- LoA is usually accompanied by notarization/testing procedure
- LoA inside a VC can only by a link to a trust list

Next Steps

Summary

- Successful End-to-End Demonstration of Wallet Attestation and Issuance for open identity ecosystems
- Enabling eIDAS (Type-1) configurations

Next steps

- IETF Draft for “Attestation Based Client Authentication for OAuth 2”
- Incorporate the concept into OpenID4VCI
  - Integrate with DPoP Access Tokens
  - Meta data and optional attestation attributes
- Work for OpenID High Assurance Profile
- Specify Holder Binding Types for SD-JWT/VC
- Trust List/Management concept for accredited wallets
- Further interop testing with new wallets and issuers

Thanks!

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

@idunion

@IDunion_SCE

contact@idunion.org

https://www.idunion.org/