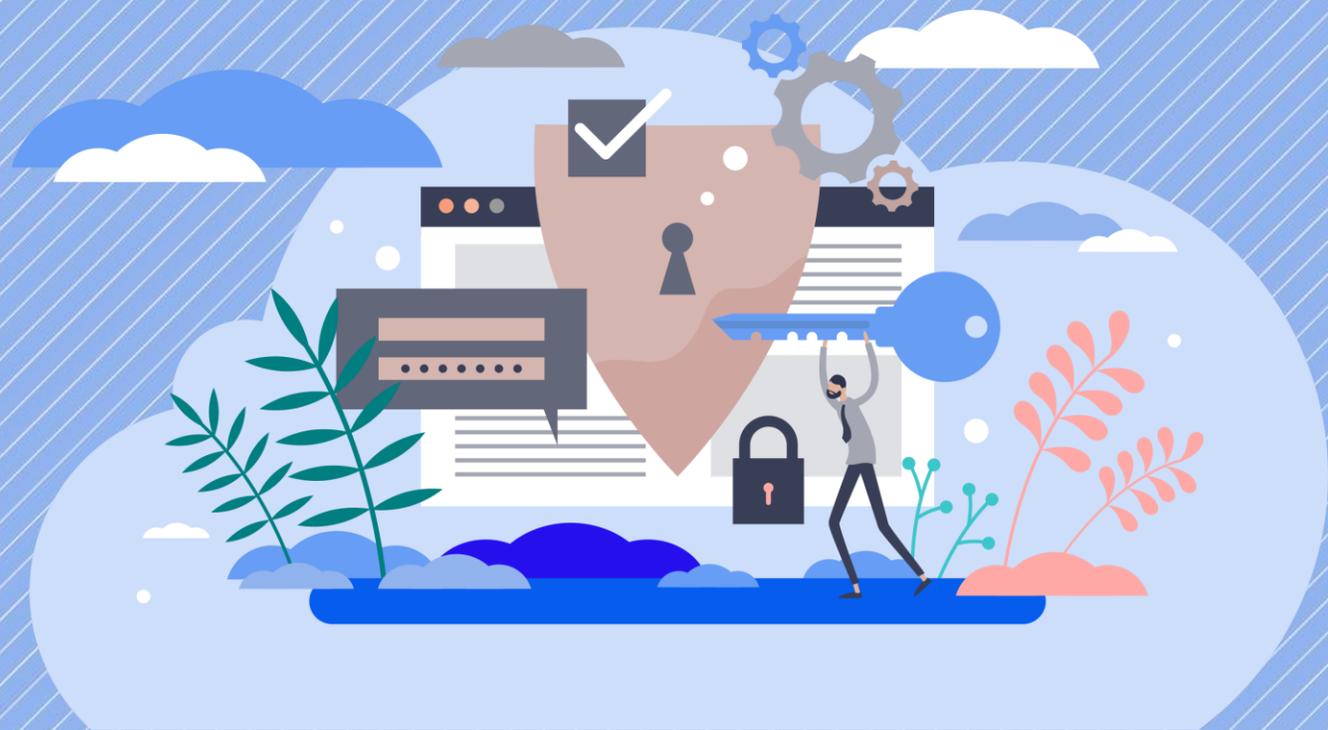
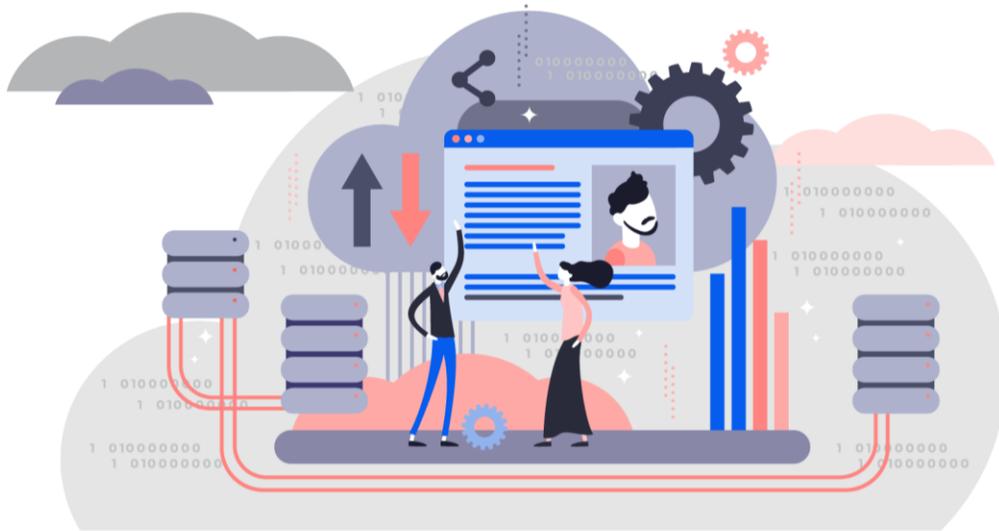


Visions for Wallet Security in SSI

Paul Bastian, Bundesdruckerei

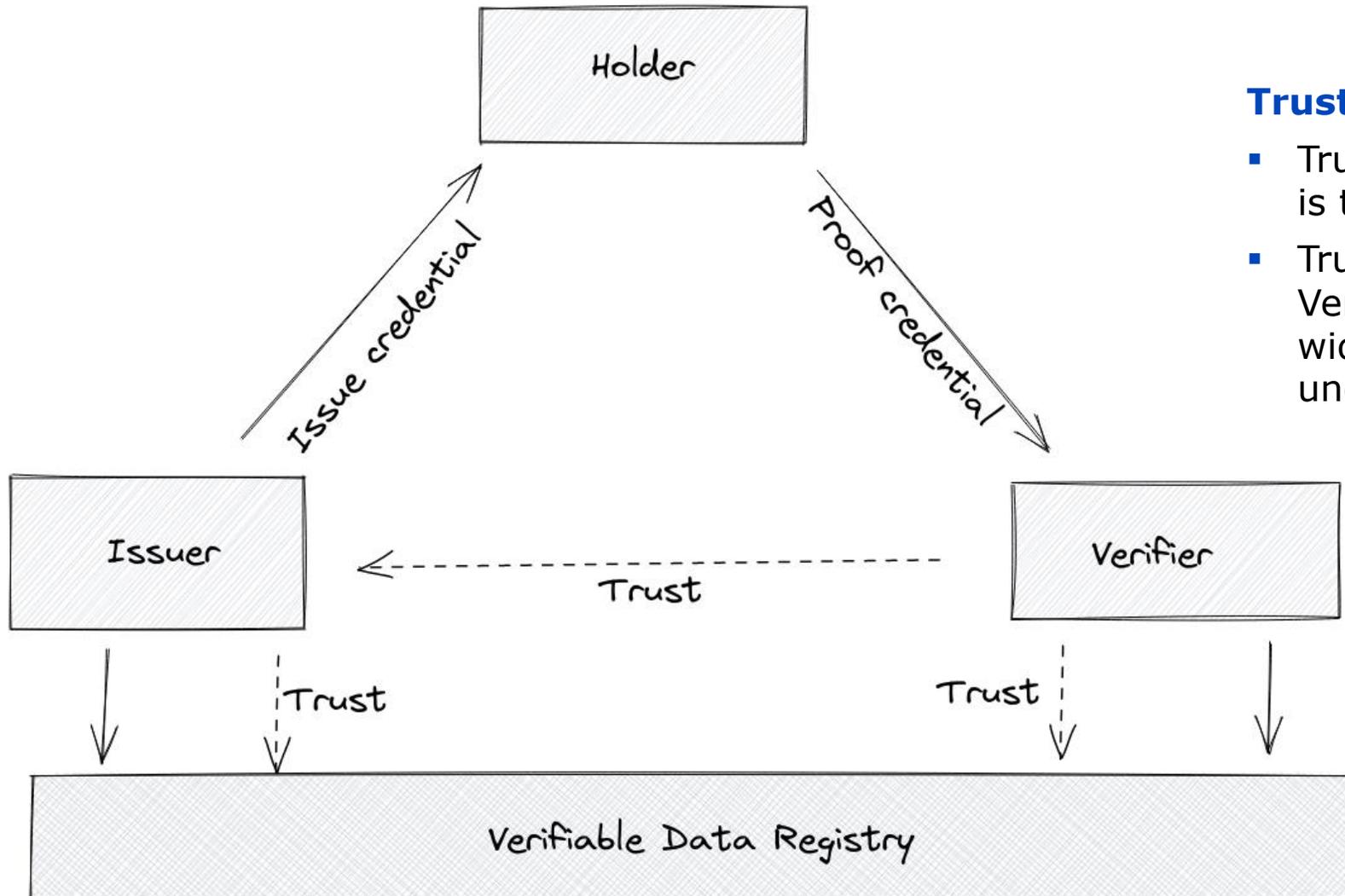


Agenda



1. Motivation & Requirements
2. Three Pillars of Wallet Security
 - i. Integrity of the Credential
 - ii. Authenticity of the Holder
 - iii. Authenticity of the Wallet
3. DIF Wallet Security Approach
4. Differential Credential Security
5. Next Steps and Outlook

Motivation: Status Quo



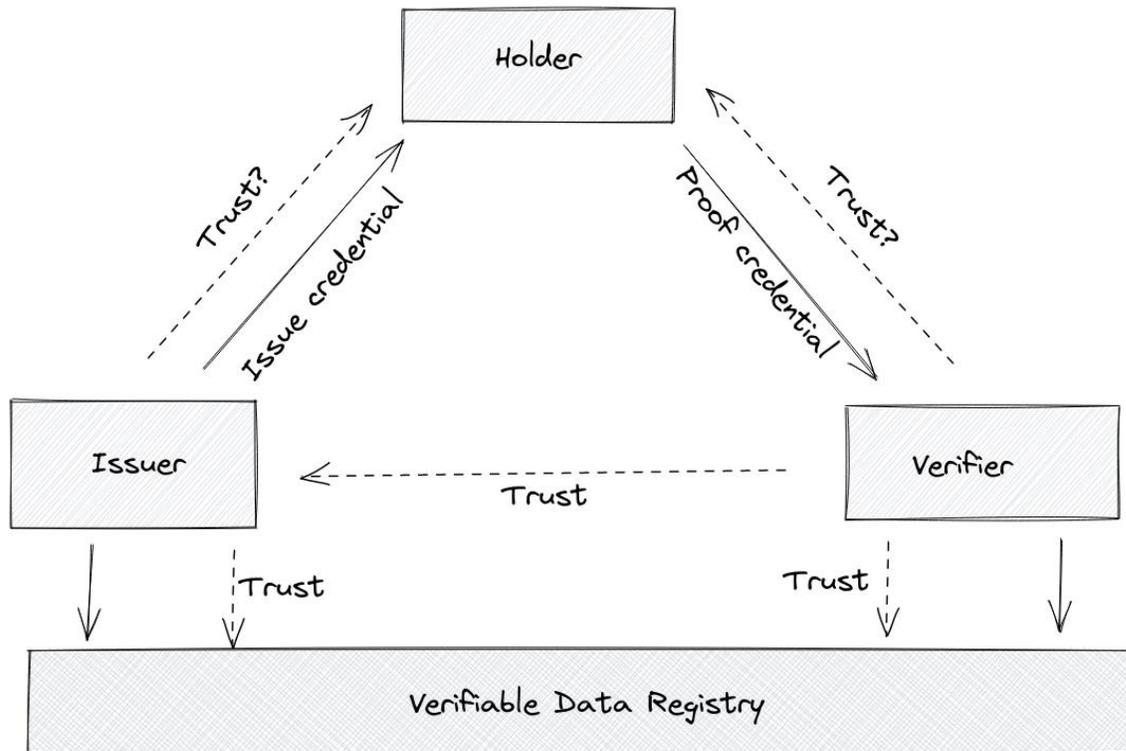
Trust in the SSI Triangle

- Trust relationship to the issuer is the core of SSI
- Trust relationship to the Verifiable data registry is widely established and well understood

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 misuse 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?

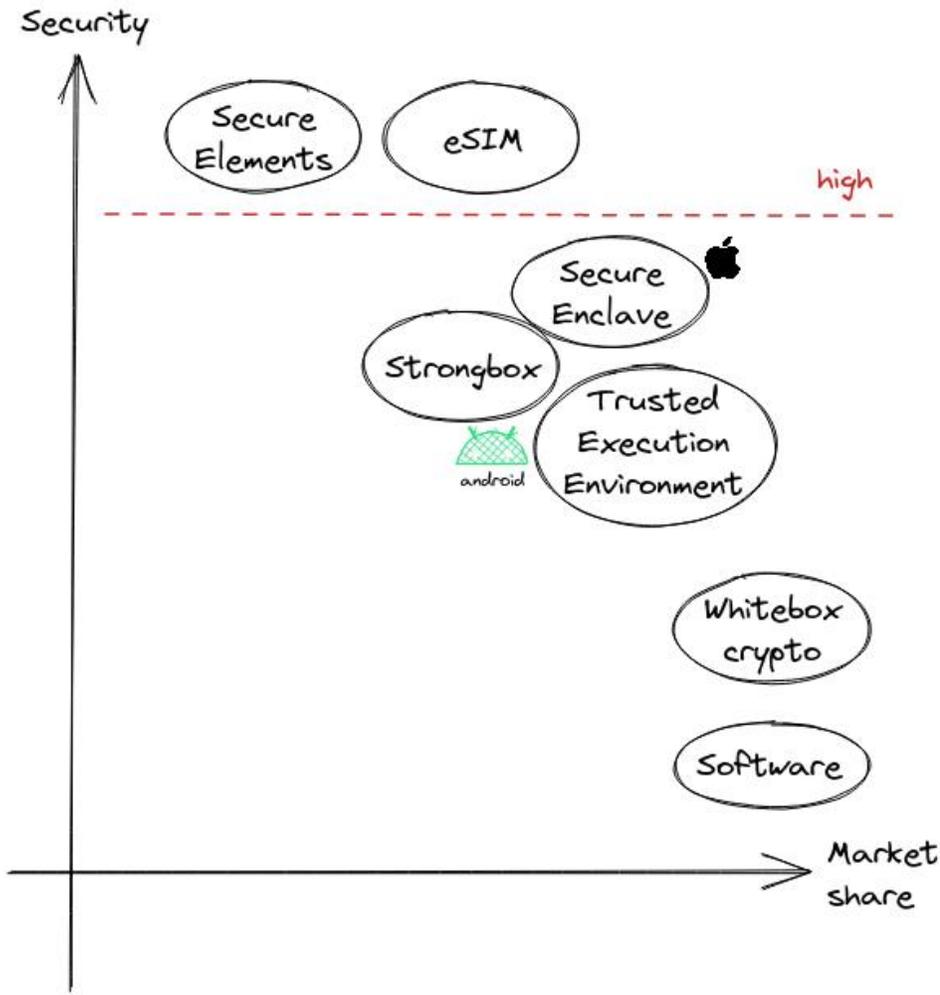
Is the holder's authentication strong enough to meet the requirements of my regulated use case?

Requirements for Identity Credentials

Requirements from Regulations

- eIDAS LoA / TR-03107 Elektronische Identitäten
 - low, substantial, high
- Evaluation factors:
 - Enrolment
 - Proof of identity
 - Issuance security
 - Multi-Factor-Authentication
 - Possession
 - Knowledge
 - Biometry
 - Revocation
 - Communication security
 - Cryptographic algorithms
- Protection according to ISO18045 attack potential
 - ISO29115 attack vectors:
 - Online guessing
 - Offline guessing
 - Credential duplication
 - Credential theft

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

Cloud

- possible with HSM in the cloud
- Hybrid approaches feasible
- eIDAS Toolbox and major players focus on mobile market
- Similar problems to mobile if not entire web-wallet



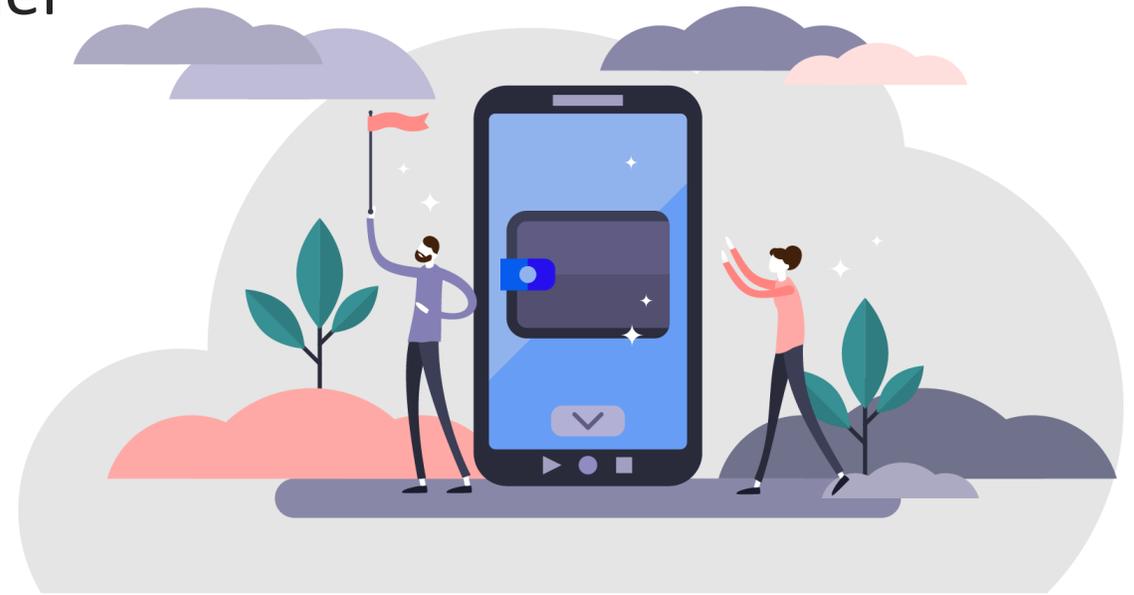
Binding credentials to the wallet



Binding credentials to the holder



Authenticating the wallet



Integrity of the Credential

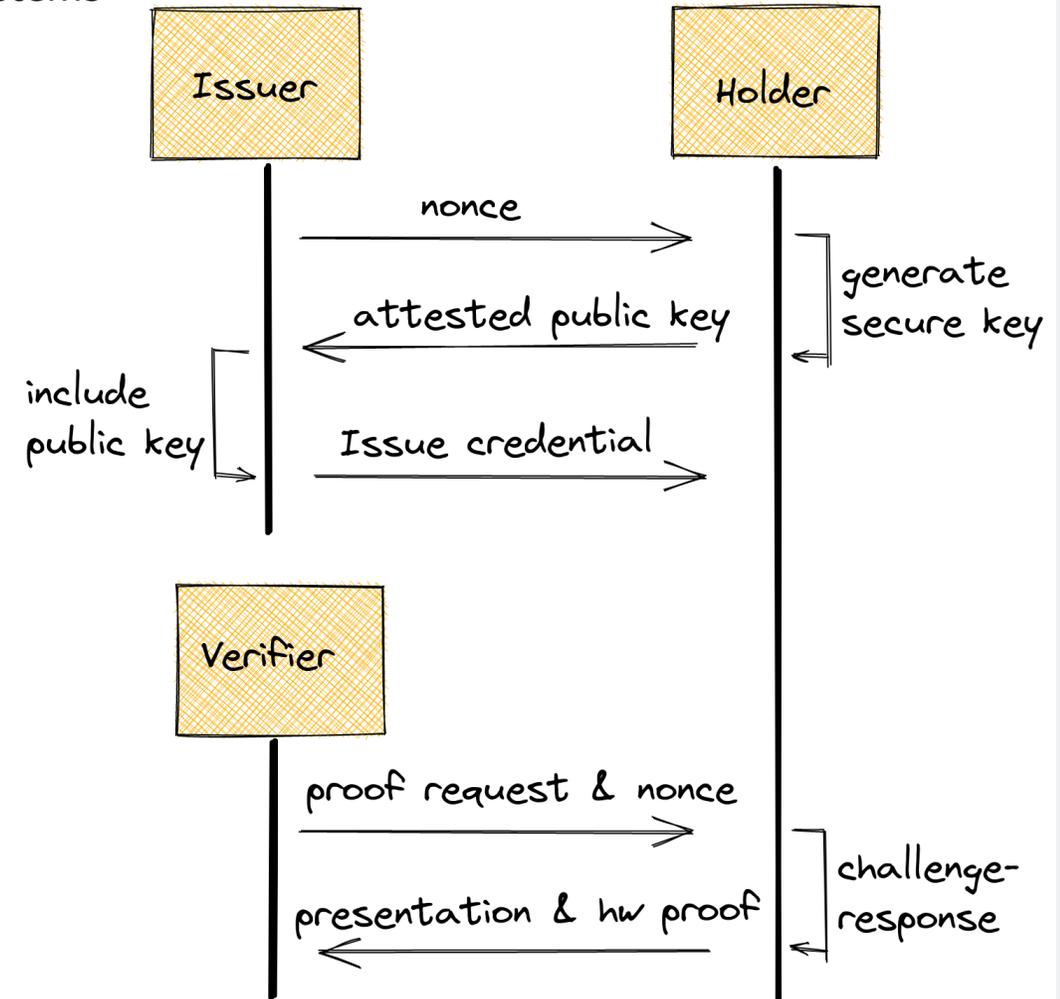
Device Binding Intermediate Solution

- Smallest common denominator for all hardware-backed crypto systems
 - Elliptic Curve NIST P256 with ECDSA-SHA256
 - No support for ZKP in hardware (also for BBS+)
- Simple challenge-response scheme
 - Attested hardware public key as VC attribute
 - Separate challenge-response check
- Pro:
 - DID-method and SSI-stack independent
 - simple, well-understood crypto system
- Contra:
 - No backup & recovery strategy possible (more on this later)
 - Adding a unique, trackable attribute

Device Binding Longterm Solution

- ZKP in mobile hardware takes 5-10 years
- Hybrid cloud?

 **DIF** Wallet Security WG



Authenticity of the Holder

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

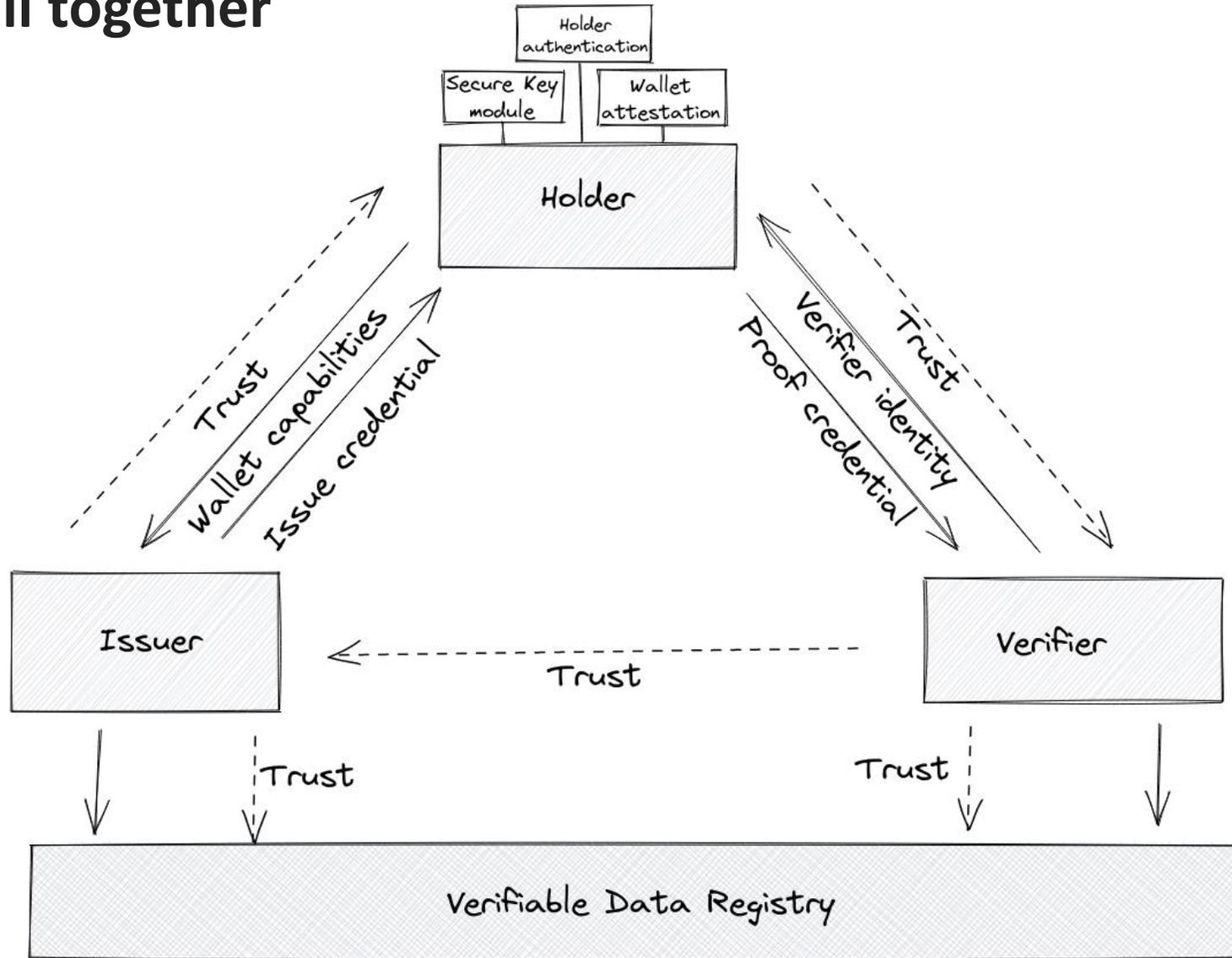
- Biometry on mobile phones is easy to circumvent and not yet sufficient for regulated use cases
 - BSI TR-03166 Technical Guideline for Biometric Authentication Components in Devices for Authentication
- PIN is a secure and necessary method
 - System-PIN (operating system)
 - separate App-PIN or SE-PIN

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

Bringing it all together



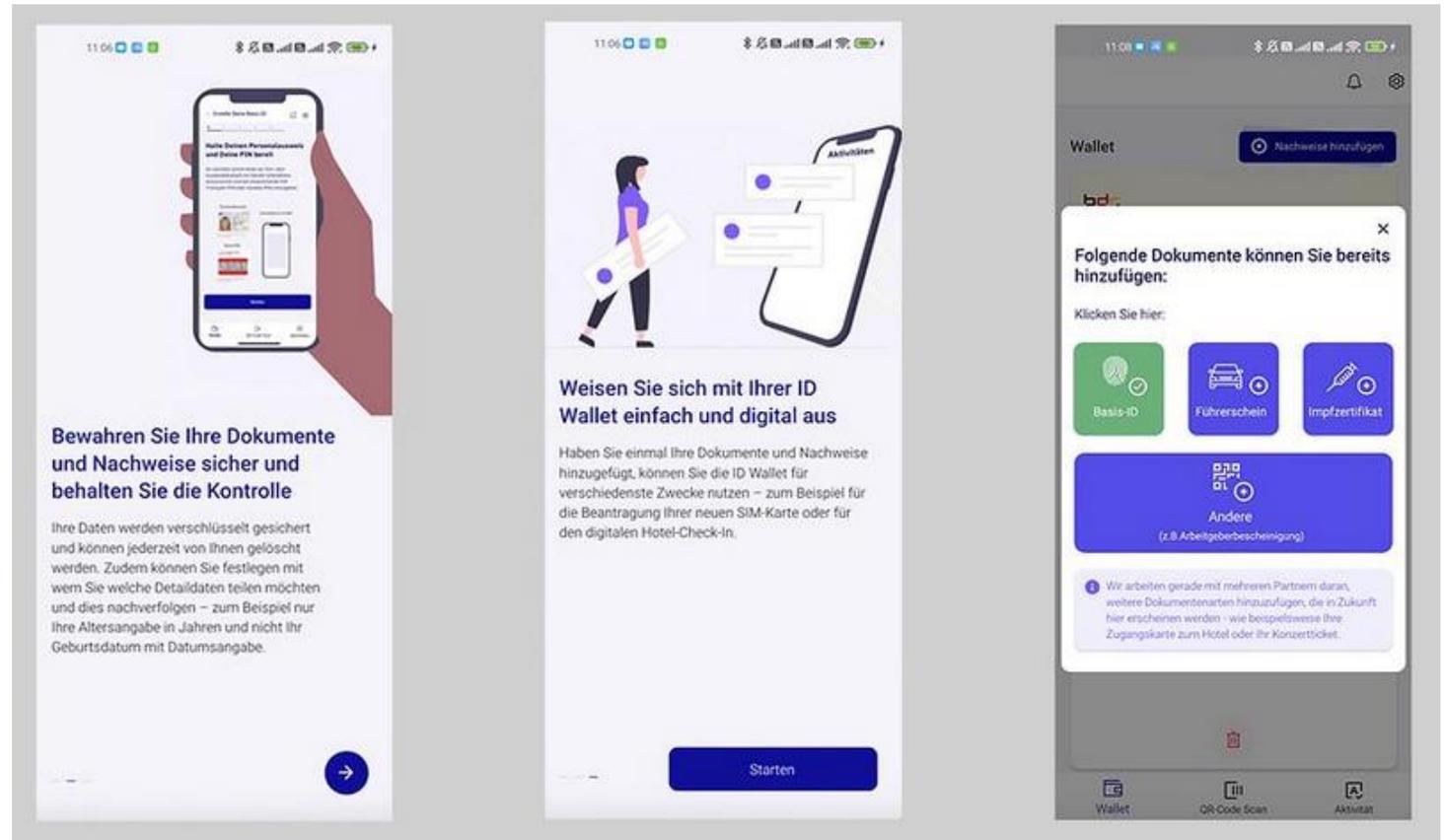
Gaining Experiences from german Chancellery Project

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



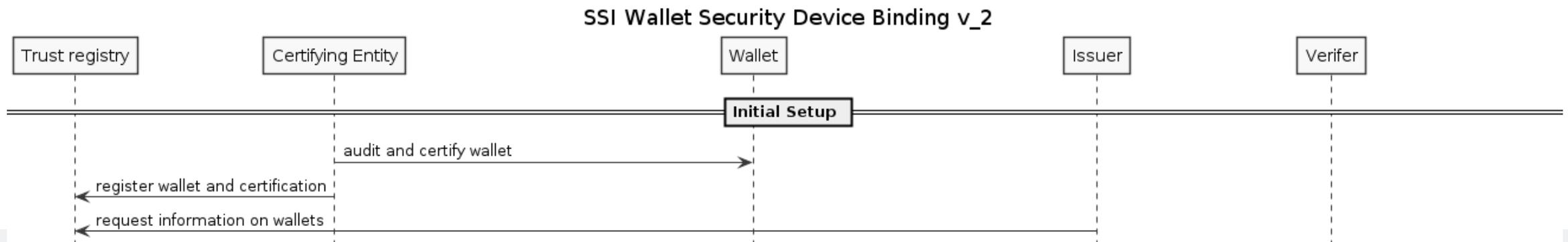
DIF Wallet Security Approach

Combined Approach

- Implement device binding, wallet authentication and holder authentication into one lifecycle
- Legal obstacles(SafetyNet/DeviceChecker) and technical complexity motivate an additional entity to perform the attestations
- Useable with W3C Verifiable Credentials or AnonCreds

Participants in the Lifecycle

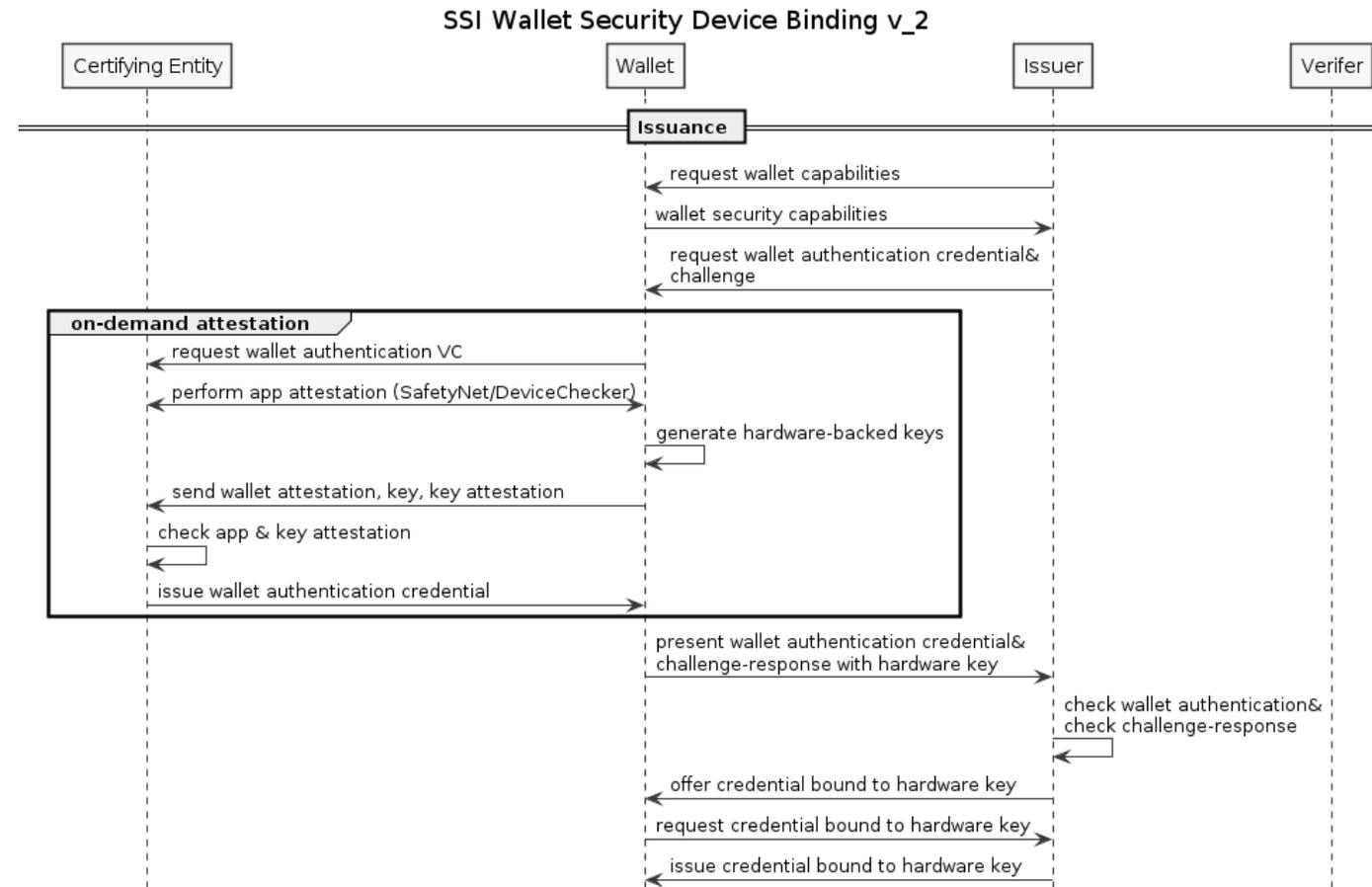
- Issuer / Holder / Verifier
- Certifying entity
 - Attests the device binding and wallet authentication
 - Either the wallet issuer backend service or trust framework-dependent trusted third party
- Trust registry
 - list of multiple wallet issuers and their certification status, legal representation, contact information



DIF Wallet Security Approach

Issuance process

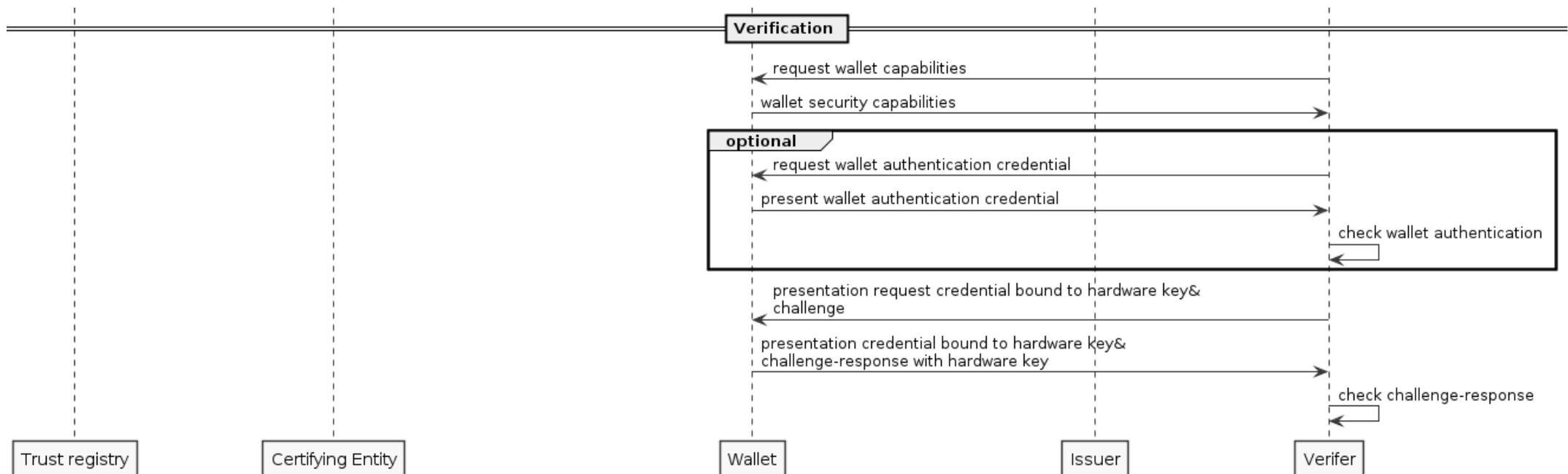
- Integrate the attestation process on-demand instead of upfront at wallet installation
- Use established mechanisms like VC and Present Proof to transmit information
- On-demand advantages
 - Fresh attestations
 - Minimal load on certifying entity
- Interfaces
 - Aries [Device Binding Attachments](#), e.g. for Present Proof v1/v2
 - Certifying Entity <-> Wallet must not be standardized, but can be
- Wallet Authentication VC:
 - identity of the certifying entity
 - wallet name and version
 - hardware public key
 - hardware type and attestation?
 - issuance/expiration date
 - holder authentication mechanism



DIF Wallet Security Approach

Verification process

- Regular Present Proof protocol with Aries RFC0729 Device Binding Attachments
- Verifier framework checks challenge-response and matches public key with hardware-bound credential
- Optionally request Wallet Authentication VC and check attestations (actually not necessary if you trust the issuer)



DIF Wallet Security Approach

Current discussions/Open Questions

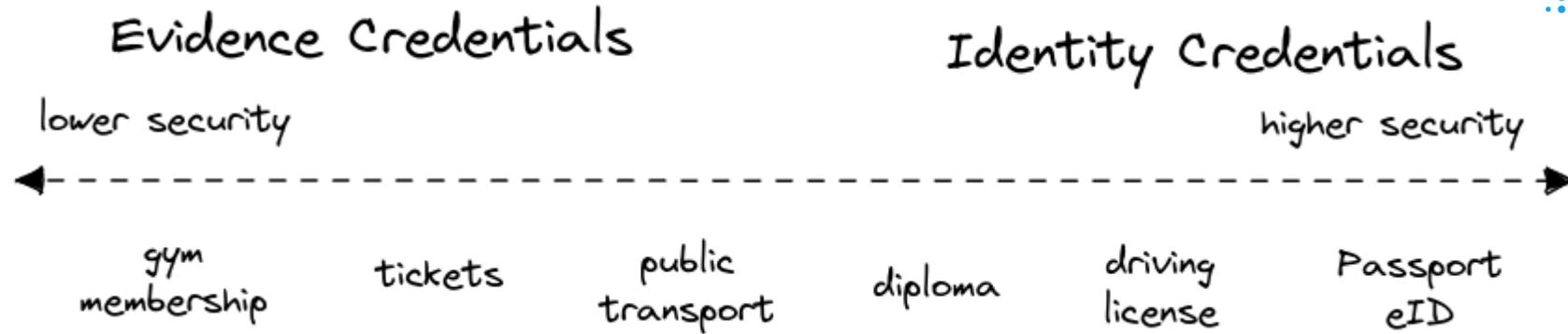
- Key encoding for hardware-bound public key
 - did:key vs JWK vs did:jwk
- Specific questions to W3C VC hardware-binding
- Should the Wallet Authentication VC reference to specific hardware types/holder authentication mechanisms (and let the issuer match to required LoA) or to specific level of assurances from a specific trust framework?
- Should the Wallet Authentication VC reveal the wallet name and version?
- Include the extended key/app attestations into Wallet Authentication VC?
- Implementation and demonstration of Aries RFC 0729
- Mechanisms for OpenID Connect frameworks

- Are we building another boarded-up eID safe?
- Do I really need that much security?
- Is this still self-sovereign identity?

Differential Credential Security Concept



Differential Credential Security

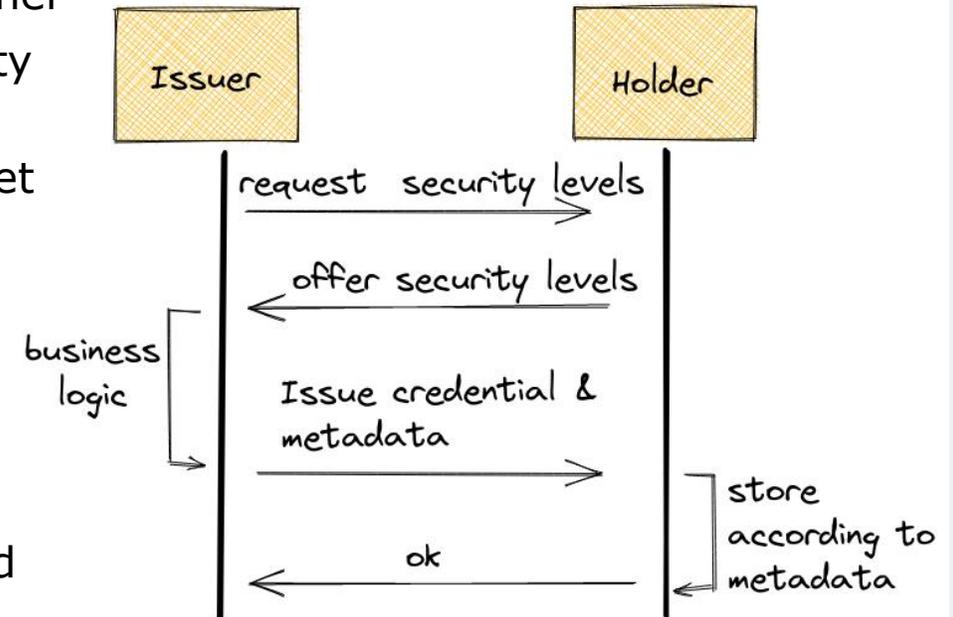


Motivation

- SSSI 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

Goals

- Pain points of regulations only apply to necessary credentials
- Majority of credentials benefits for convenience like backup and biometrics



Summary and Next Steps

Summary

- Successfully developed and tested multiple building blocks
- Improved wallet security for SSI ecosystem

Next steps

- Continue the discussion and work on wallet security
- Bring security mechanisms to standardization at DIF
- implement and test interoperable solutions



Thanks!

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



@idunion



@IDUnion_SCE



contact@idunion.org



<https://www.idunion.org/>

