User Binding for Digital Credentials

Datum	09.04.2024
Ort	TDI conference - Rome
Verfasser	Paul Bastian

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

What is User Binding?

Verifiers validate different properties within presentations of digital credentials

Data Authenticity
Is the issuer authentic?

Data Integrity
Is the data manipulated?

Validity Period
Is the credential expired or revoked?

User Authenticity
Is the credential presented by a legitimate person?

…

Digital Credentials and User Binding

Which Credential enable proofing the user authenticity through user binding

Identity Credentials

PID*

employee badge

- enable proof of identity
- require proofable user binding (authentication)

Attestation Credentials

diploma

criminal record

- confirm attributes about a subject
- user binding possibly through association to an identity credential

Was the credential presented by the legitimate person?

Were two credentials bound to the same person?

Verifier Service

* PID = Person Identification Data (eIDAS 2.0)

Four Categories of User Binding

analogue and digital

Biometric Binding

Claim-based Binding

digital

Cryptographic Binding
with proof-of-possession

Cryptographic Binding
with *proof-of-association*

🟦 self-sufficient binding for

Identity Credentials

🟦 association binding for

Attestation Credentials

Biometric Binding

Process

- Issuers embed biometric reference as a claim in the credential
- Verifiers compare biometric probe with reference

Challenges

- privacy and impact of leaked biometrics
- security and authenticity of the biometric data (low assurance)
- compatibility of biometric components
- lacking standardization for VCs

Benefits

- established, well-understood mechanism from analogue world

Primary Use Cases

- proximity use cases, e.g. visual check with mDL
- closed loop use cases (issuer = verifier), e.g. physical access to gym with face biometry

Claim-based Binding

Process

- Issuers embed comparable data into credentials as claims (usually PII)
- Verfiers compare these claims with Identity Crednetials or existing master data/registry

Challenges

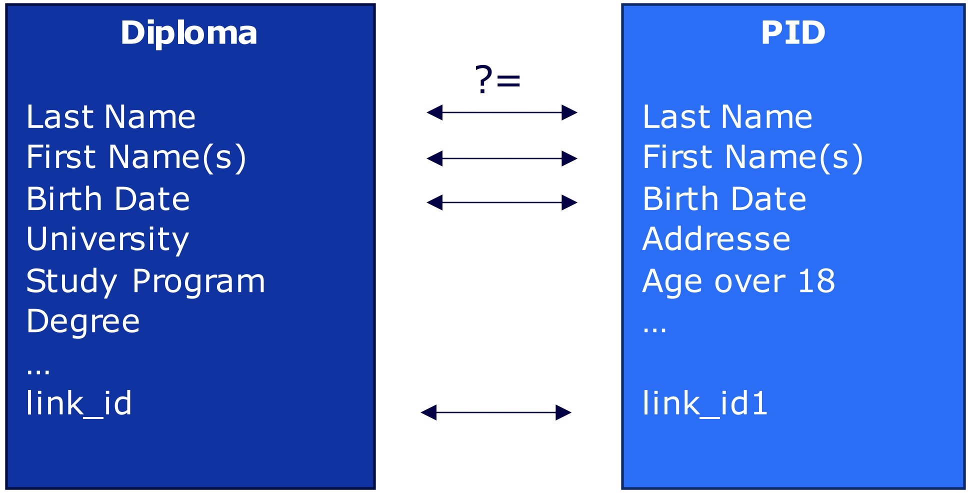
- requires disclosing many claims (privacy issue)
- lacking standardization and semantics
  => automatic Comparison may be prone to errors

Primary Use Cases

- majority of all existing analogue and digitized processes

Privacy-enhancing Variation

- Usage of dedicated linking attributes instead of PII data
  => current research topic within IDunion project



Diploma

Last Name
First Name(s)
Birth Date
University
Study Program
Degree
…
link_id

?=

PID

Last Name
First Name(s)
Birth Date
Addresse
Age over 18
…

link_id1

* pb-Daten= personenbezogene Daten

Cryptographic Binding with *proof-of-possession*

Process

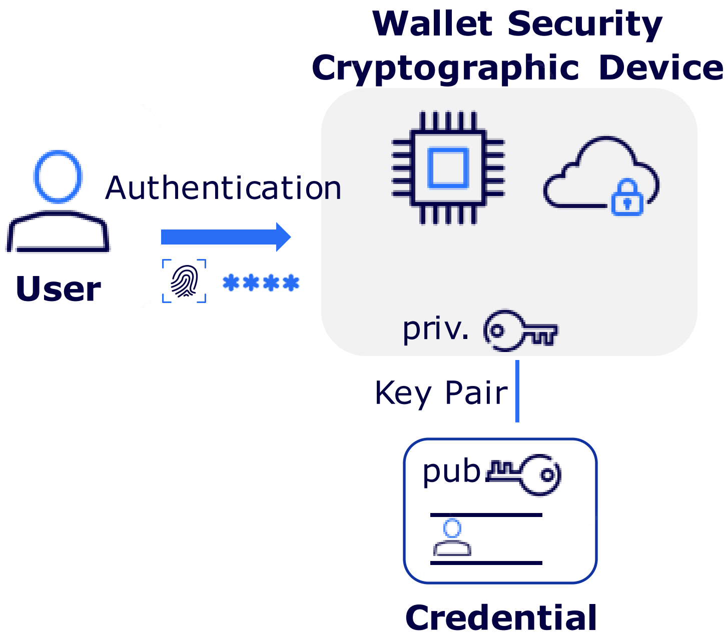
1. Issuers bind Credential to asymetric key pair
   - public key embedded as attribute in credential
   - private key under control of the user inside WSCD
2. *proof-of-possession* for presentation of the credential

Security-relevant Factors

- Storage and execution of the private key
  => Exportability and Duplication
- Unlocking of key usage through user authentication
  - PIN, local biometrics, retry counter

Challenges

- Level of Assurance (LoA) => increasing security requirements to WSCD
- Credential is bound to the Lifecycle of the WSCD
- Portability / Change of Wallets is difficult



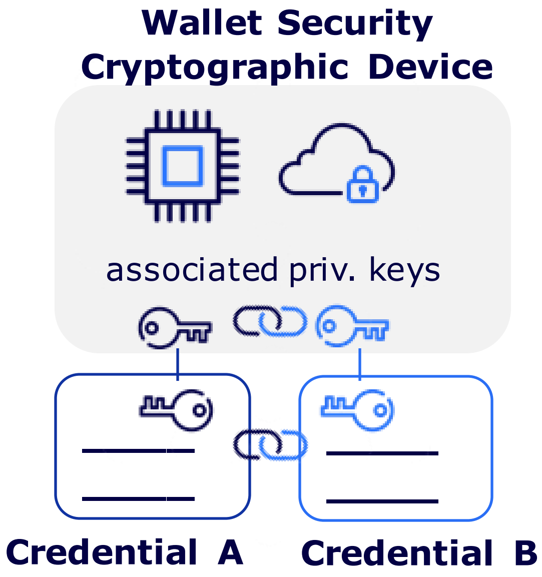
Cryptographic Binding with *proof-of-association*

Process

- The process works similar to proof-os-possession, additionally:
  - various credentials are bound to keys from the same WSCD
  - WSCD can create a proof during issuance and presentation that two or more keys belong to the same cryptograpic device (*proof-of-association*)
- Issuer of an Attestation Credentialproofs first the PID of the user and issues credential bound to key associated to the PID

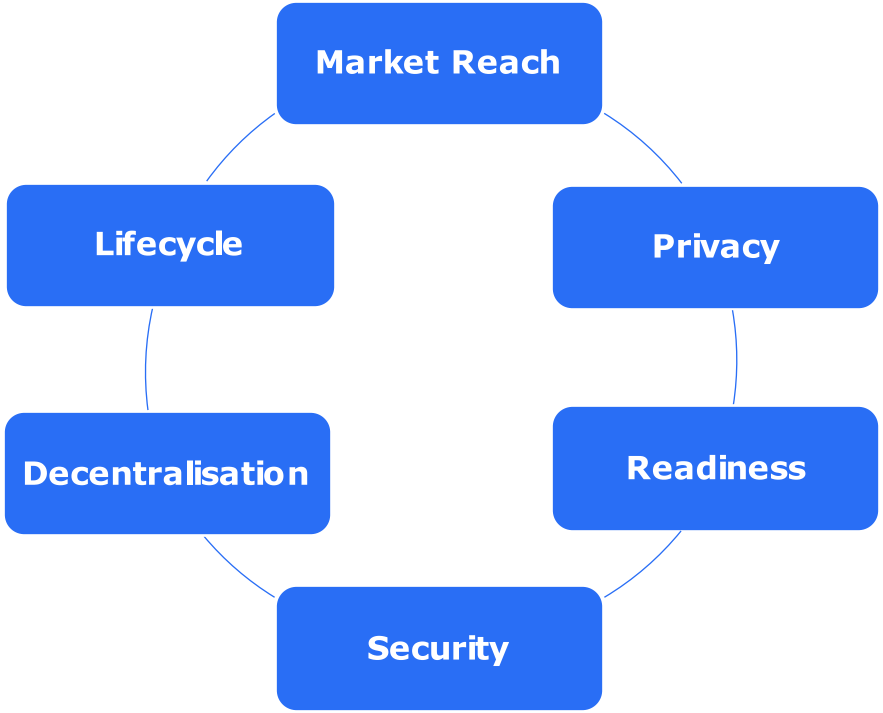
Challenges

- Even higher requirements to the WSCD
  - not compatible with native smartphone key stores (no association)
  - CloudHSM/JavaCard on Secure Element is possible
- requires governance strategy to make this an efficient user binding
  - high degree of implicit assumptions
- Backup & Recovery strategy may be difficult



Evaluation Criteria

Is the solution usable for most users?



What impacts does the solution have on the lifecycle or credentials?

Is the presentation of credentials privacy-preserving?

Are there dependencies to central service?

Is the solution based on technically matured mechanisms?

Is a strong user binding guaranteed?

Comparison

	+	-
Biometric Binding **Claim-based Binding**	• Easy, well-understood and established mechanism from the analogue world • no requirements on WSCD • no dependence to a particular Wallet Instance • easy backup & recovery	• Limited privacy as PII data needs to be disclosed • interoperability issues through missing standardization and incompatabiltity for biometric devices
Cryptographic Binding with *proof-of-possession* **Cryptographic Binding** with *proof-of-association*	• Established and standardized mechanism in the digital world • no disclosure of PII data for user binding required (privacy preserving)	• limited market reach of Secure Elements for WSCD • Cloud-HSM may force further centralization • strong binding to WSCD complicates backup & recovery • PoA may not be mature enough

Wallet Attestations

Motivation

- enable proof of authenticity of a Wallet and its WSCD
- concepts of Wallet Attestations were presented at TDI 2023 and are now adopted by ARF 1.3 (Wallet Instance Attestation)

Touchpoints with User Binding

- Proof of Possessions require Wallet Attestations, standardization work of "Attestation-Based Client Authentication"
- Proof of Association may use Wallet Attestations as well and may communciate assocation within or as part of PoP

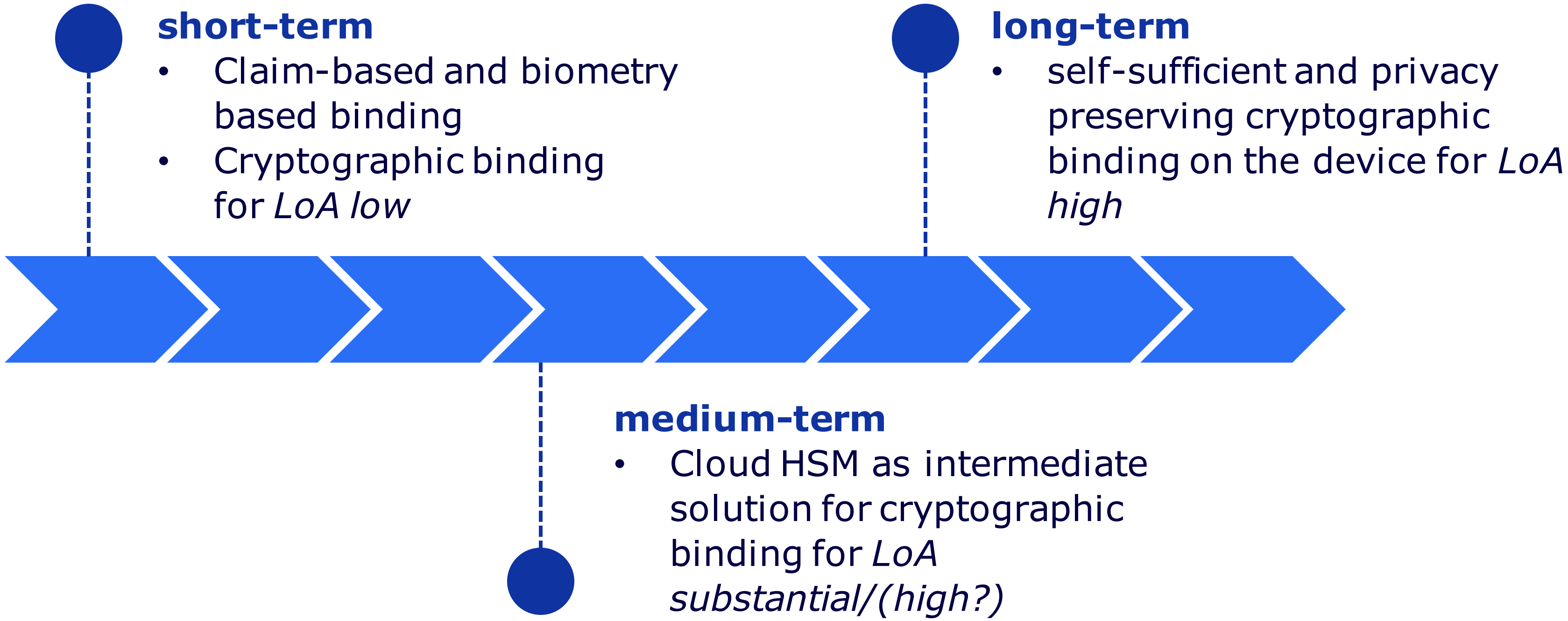
Challenges

- Wallet Attestation concept may be overloaded by too many burdens:
  - Authenticity of the Wallet/WSCD towards Issuer
  - Authenticity of the Wallet towards Relying Party
  - Revocation means for user-initated revocation
  - Revocation means for WSCD compromise

--> Wallet Attestations are mainly intended to support user binding, don't mix in too many other requirements

Conclusion and Outlook

User Binding is an essential building block for proofing user authenticity in the wallet and trust into the digital credentials das Vertrauen in digitale Nachweise



short-term

- Claim-based and biometry based binding
- Cryptographic binding for *LoA low*

long-term

- self-sufficient and privacy preserving cryptographic binding on the device for *LoA high*

medium-term

- Cloud HSM as intermediate solution for cryptographic binding for *LoA substantial/(high?)*

Next Steps

User Binding requires further research and standardization efforts to establish a successful ecosystem:

- consider the semantic gap for biometric/claim-based bindings (equivalent to RFC7800?)
- improve research on proof-of-assocation (PoA) and get feedback from communities/implementers
  - put emphasis on solving backup/recovery strategies
- research on privacy-enhancing claim-based binding with dedicated linking attributes
  - work initiated within IDunion research project
- research on privacy-enhancing Zero-Knowledge Cryptography for the long-term future
- develop understanding for coexistance of user binding mechanisms and migration strategies

Thank you.

Paul Bastian

Bundesdruckerei GmbH
Innovations
E-Mail: paul.bastian@bdr.de