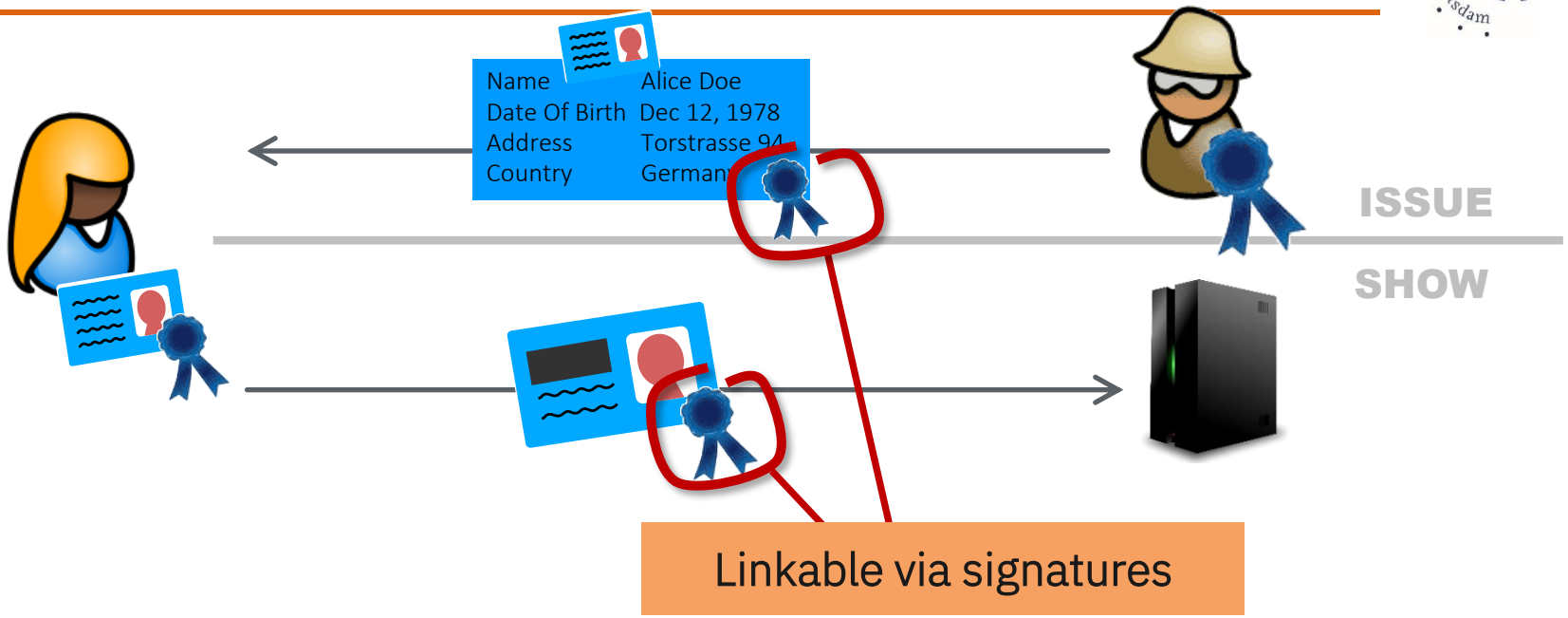
Innovation Highlights of EUDI Funke: Zero-Knowledge Proofs

Prof. Dr. Anja Lehmann

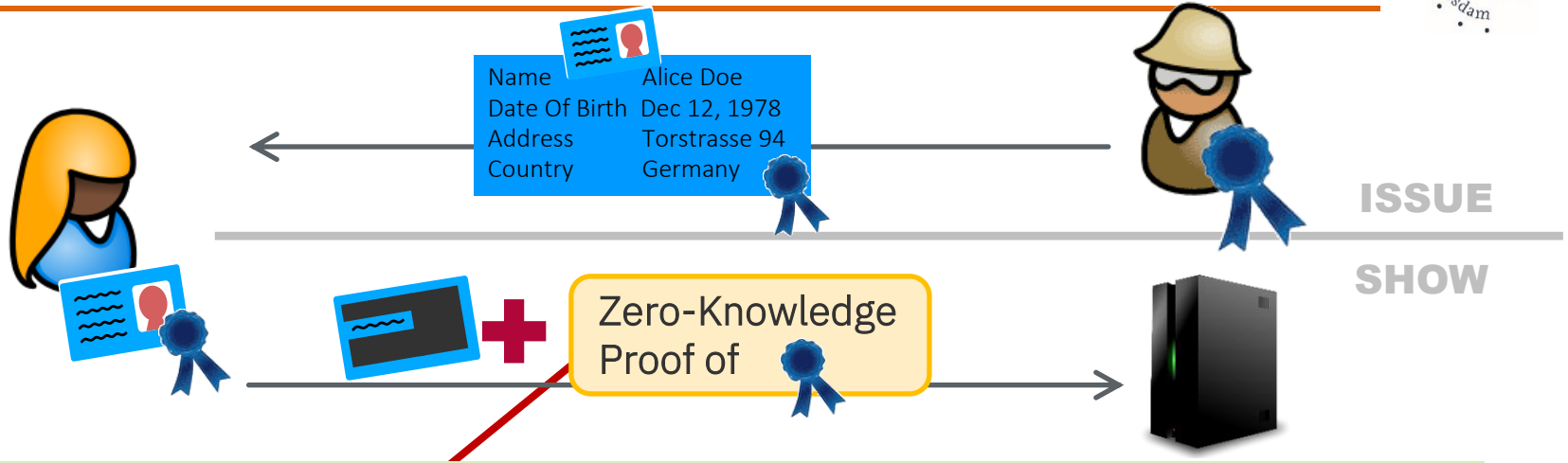
HPI Hasso Plattner Institut
Digital Engineering · Universität Potsdam

Digital Identity | Classic Credentials & Limitations



- Digital identity credentials based on cryptographic signatures
- Signatures are great for security, but bad for privacy → unique identifier

Digital Identity | Privacy through Zero-Knowledge Proofs

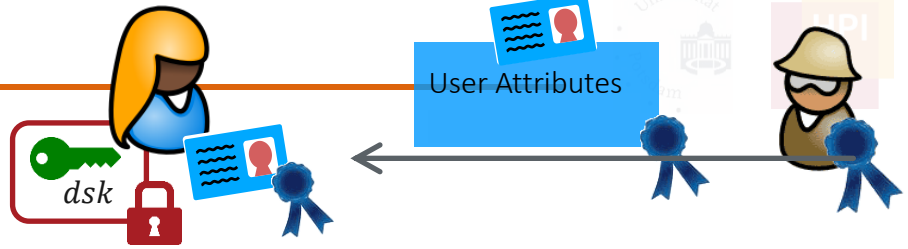


Zero-Knowledge Proof (ZKP)

Proof that reveals *nothing* beyond validity → perfect privacy & unlinkability!

- Practical ZKP-based solutions for privacy-preserving eID since 2001
- Not considered for EUDI because of lack for **device-binding**

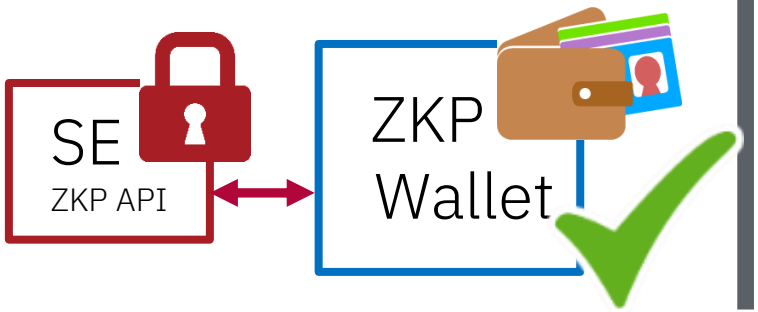
Security | Need for Device Binding



- Cloning of digital credentials is trivial
- Credential must be bound to key protected via Secure Element of phone
  Every showing needs to involve Secure Element (SE)
- Device-binding for ZKPs developed in 2010, SE API standardized in 2013

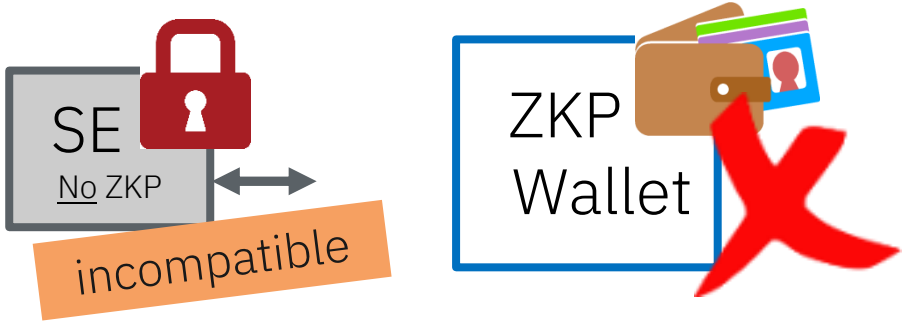
Theory

Problem solved!



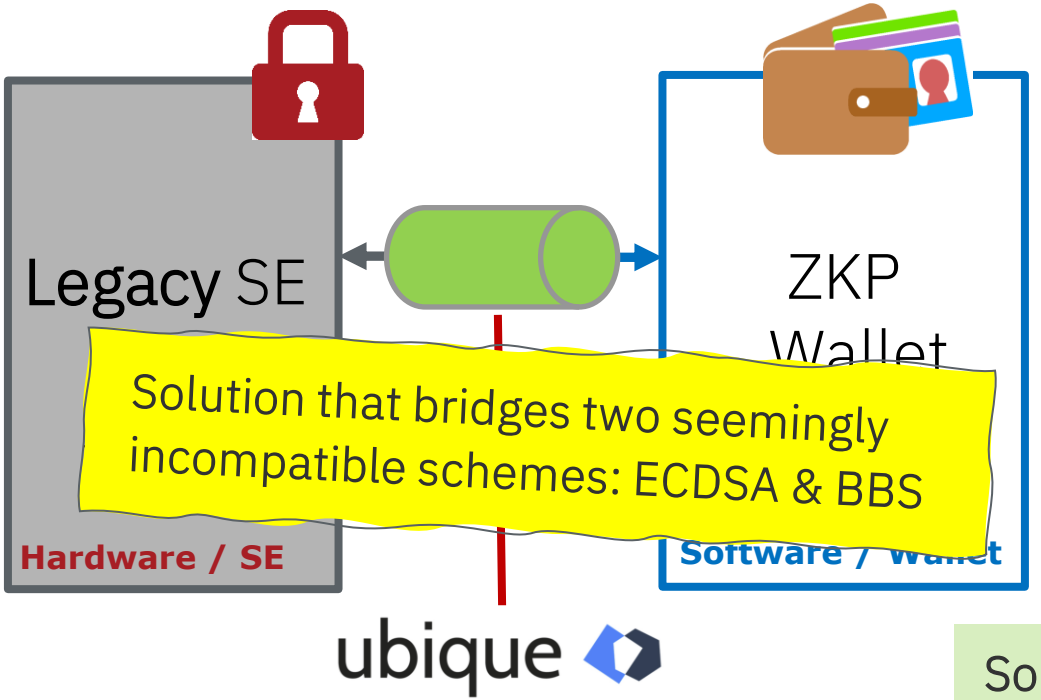
Practice

SE API not implemented, upgrade impossible
No device binding for ZKPs



ZKP + Legacy Device Binding | Ubique Innovation

- Ubique wanted to use ZKP + device binding now … and came up with a solution!



First deployment of ZKP wallet with device binding on legacy SE

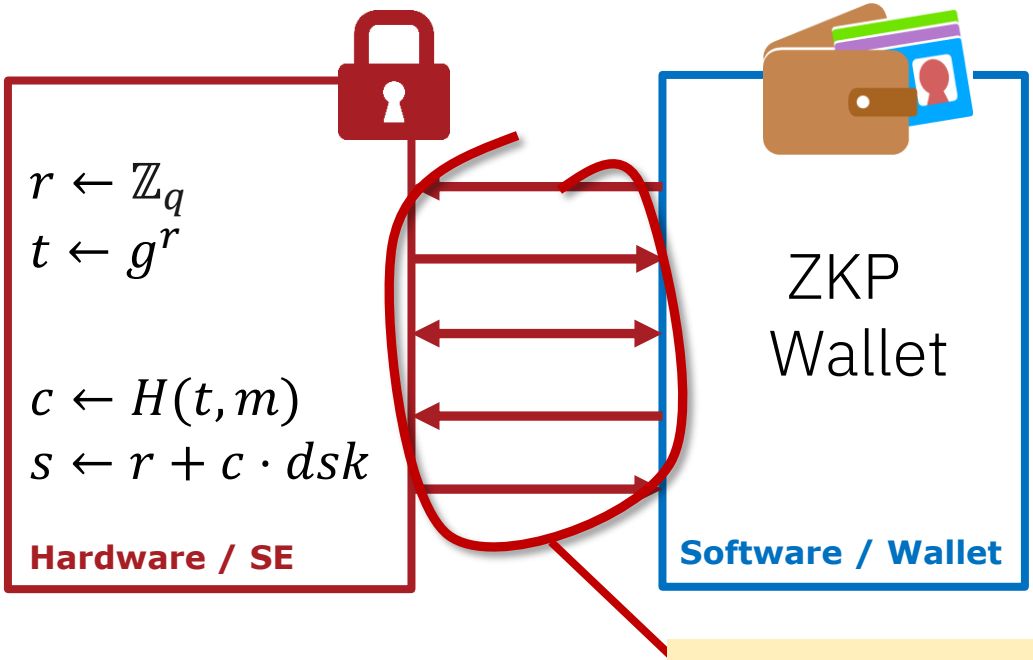
ZKP can be used on **existing phones**
(bridging: 800ms, 150kb)

Solution for short-term ZKP deployment

Ubique solution described here: *https://ia.cr/2025/1981*

ZKP + Native Device Binding | Funke Reality Check #2

- wwWallet/Yubico implemented ZKP with native device binding



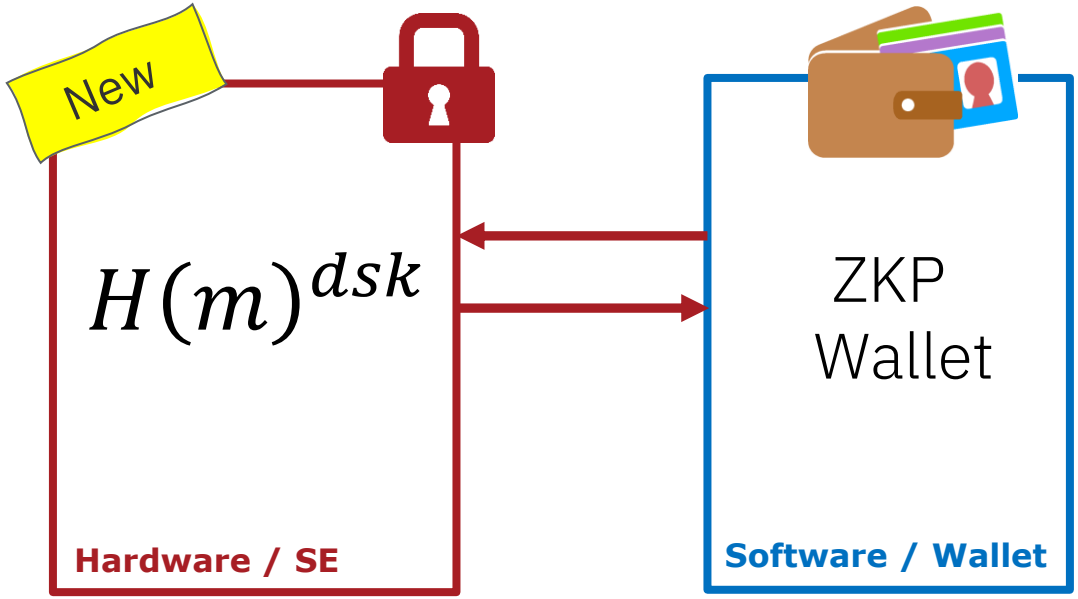
Native ZKP APIs:

Simple and lightweight
(~ Schnorr signature)

Yubico: Two API calls are annoying, why not one?

ZKP + Native Device Binding | Improved Protocol*

- Simpler device-binding, compatible with ZKP (BBS) credentials (inspired by BBS#)



Optimal efficiency & super simple

New: privacy w/o trust in hardware

*Device Bound Anonymous Credentials With(out) Trusted Hardware. https://ia.cr/2025/1995
Karla Friedrichs, Franklin Harding, Anja Lehmann, Anna Lysyanskaya.

ZKP Innovations by EUDI Funke

- Funke removed barrier towards ZKP deployment → lack of device binding

Short-term: Ubique solution works now, efficient enough for most use cases

Mid term: new native API (simpler design, optimal performance & privacy)

Thank you @ EUDI Funke!