TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

TeleTrusT-Informationstag "Elektronische Signatur und Vertrauensdienste"

Berlin, 12.11.2025

National EUDI Wallet Project Germany

Dr. Torsten Lodderstedt, Bundesagentur für Sprunginnovation (SPRIND)

Paul Bastian, Bundesdruckerei GmbH

Meet the Project Team

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Federal Ministry for Digital Transformation and Government Modernisation
SPRIN-D
Federal Office for Information Security
Fraunhofer AISEC
bdr. BUNDESDRUCKEREI
MEIRÉ
pwc

EUDI Wallet: Different Perspectives

Regulatory Obligation

Mandated by **EU regulations** for publishing verified digital credentials, ensuring **trusted and standardized** digital interactions.

Rigorous Certification

Ensures **high security, data protection, and interoperability, building trust** and preventing fragmentation.

Cornerstone for Digitalization

Empowers citizens with **data control, streamlines access to services, and fosters innovation** for a digital society.

Our Goal and Strategic Prerequisites

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Overall mission: Build a national EUDI Wallet that is embraced by society because of its positive impact on the digitalization of German society.

As prerequisites we need to know:

- Needs
- Concerns
- Conditions & prerequisites

The Path to the DE EUDI Wallet

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

1 Architecture & consultation

- **Sharing through screenshots** as default today
- **"over-identification"** concerns in civil society
- **High security & privacy requirements**
- **Adoption**
- **Interoperability**

2 Blueprint

- Based on ARF
- **Ecosystem architecture and governance**
- Cloud HSM architecture
- Digital sovereignty

3 Funke

- **Evaluation through prototypes:** e.g. PID, EAAs, QES, pseudonyms, batch processing, and Zero-Knowledge Proofs
- **Tests:** LSPs and beyond, evolve and refine blueprint, enhance German contributions to the ARF

Standards development

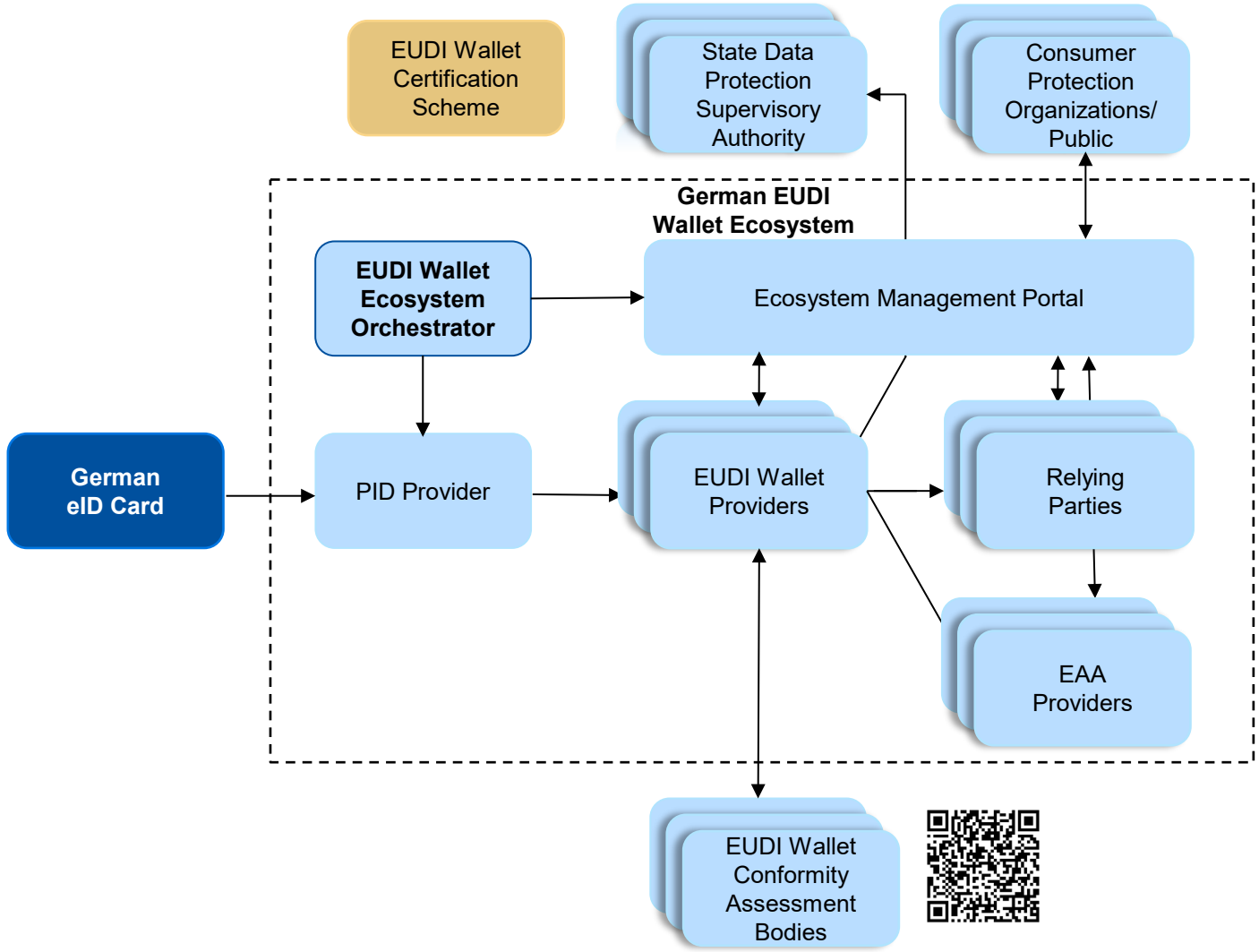
Project members contribute to several SDOs, e.g. OpenID Foundation, IETF, ETSi, ISO, CEN, W3C, CSC

Development state provided EUDI Wallet

Development EUDI Wallet ecosystem

The German EUDI Wallet Ecosystem

- **National wallet and alternative wallets:**
  Citizens can choose between certified state-issued wallet and alternative wallets.
- **Ecosystem managed by orchestrator:**
  An orchestrator coordinates all stakeholders and services within the German EUDI Wallet ecosystem.
- **Self-service onboarding to EUDI Wallet ecosystem through Ecosystem Management Portal:**
  Relying parties (RPs) and EAA Providers register via a single portal.

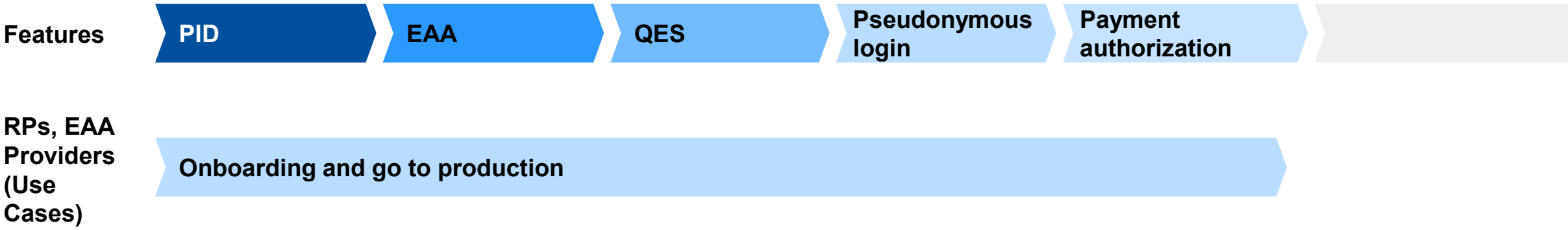


Incremental Rollout Strategy

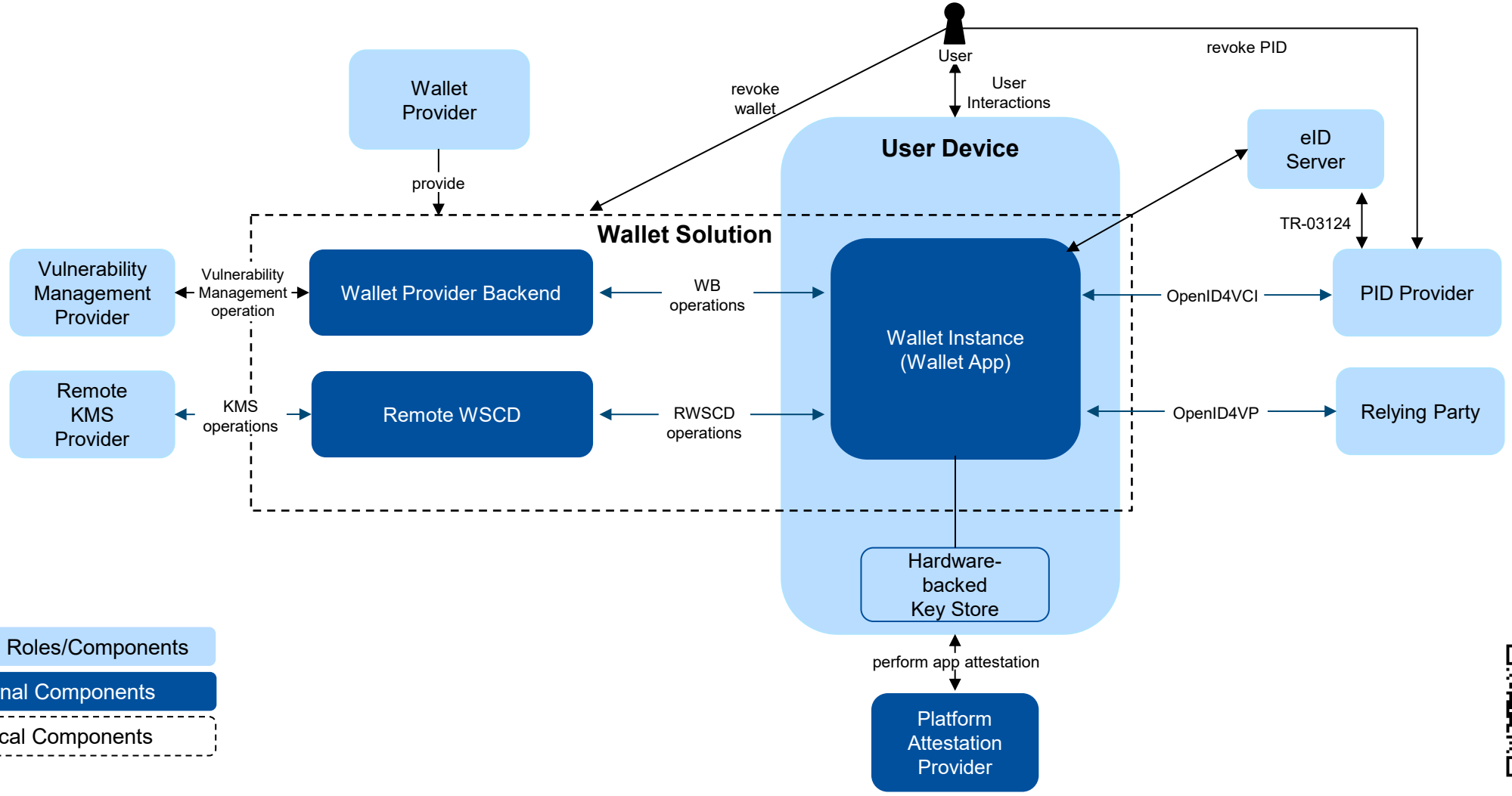
Bring value to the society as quickly as possible

Ensure there are use cases from day 1

Inspect and adapt



Architecture of the German national EUDI Wallet



Let‘s have a look – Demo

Start of Sandbox – Come On Board!

The EUDI Wallet Sandbox will launch at the end of the year

A testing environment where **companies and public authorities** can **try out the wallet in real-world use** for the first time. At the start, digital identity verification via **Person Identification Data (PID)** will be possible. The goal is **active participation** from business, academia, and public administration, as well as the development of **individual application scenarios.**

We are building a diverse ecosystem with real-world use cases to make the German national EUDI Wallet part of everyday life - **and we need your participation to make it happen.**

Future Topics

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

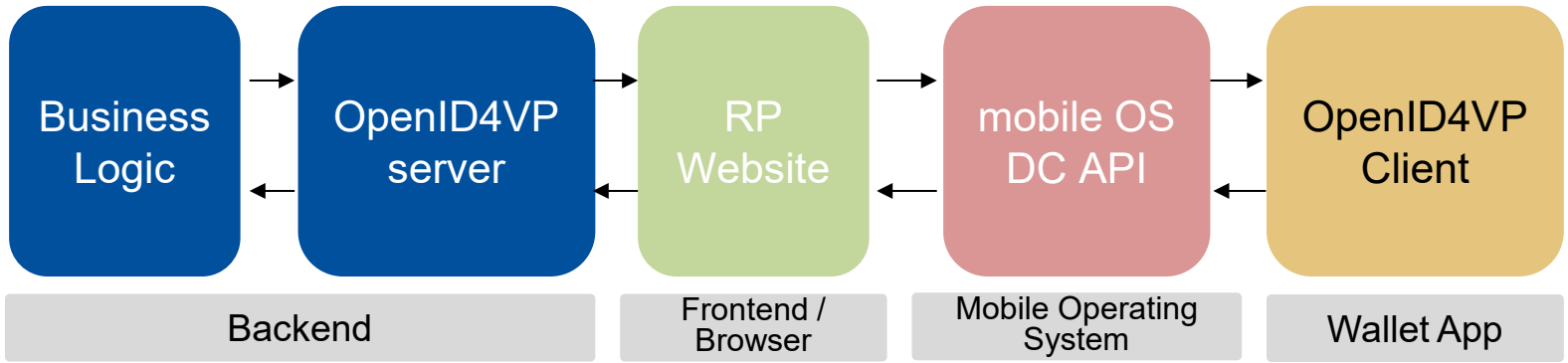
W3C Digital Credentials API

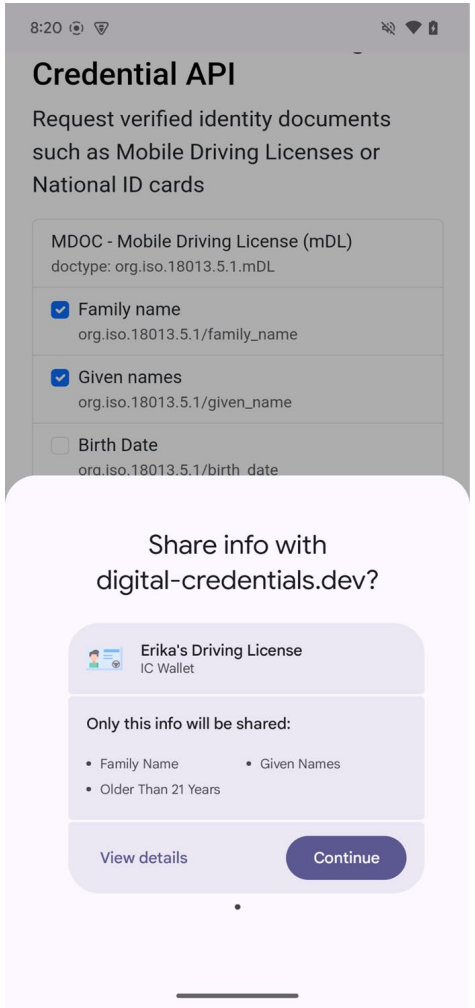
Secure Elements

Zero-Knowledge Proofs

W3C Digital Credentials API

- Improved UX for selecting correct wallet and returning to the same browser tab
- Phishing-resistant cross-device flows on protocol level as mobile OS uses BLE for proximity check
- Easier implementation flow as response is returned through the frontend





W3C Digital Credentials API

Digital Credentials API is a major step towards a user-friendly and secure wallet ecosystem.

But…

API implementations currently have varying support for messages and formats

Cross-device flow messages go through relay servers causing privacy concerns

Key Storage for National EUDI Wallet

Credentials in the national EUDI Wallet are secured by different means:

1. PID is secured by Remote WSCD using Cloud-HSM and remote 6-digit Wallet-PIN.

2. (Q)EAAs are secured by local, native key stores using platform authentication.

Remote WSCD

- National EUDI Wallet will launch with remote WSCD:
  - Most smartphones lack key storage and user authentication required to achieve LoA high
  - Remote WSCD allows us to reach the most users
  - New technologies to enable local WSCD are not production-ready
- Remote WSCD is currently the only feasible solution combining **security** with sufficient **user reach**
- However, we would like to move to local WSCD, as it allows:
  - Better scalability
  - Lower costs
  - Better privacy
  - Offline support
- We expect suitable, widespread Secure Elements to take another 5 years

Migration to Local WSCD

Local WSCD is the long-term solution with various possibilities:

1. Global Platform initiatives (SAM, WSCA API)
2. Android Strongbox
3. iOS SE Platform (since iOS 18.1)

Migration strategy

1. All devices initially use remote WSCD to reduce complexity and maximize user reach
2. Continuously investigate local WSCD implementation options
3. Gradually integrate device classes to from Remote to Local WSCD

Zero-Knowledge-Proofs (ZKP)

The initial setup for (PID) credentials will use batch issuance:

Provides unlinkability between Relying Parties

Increases complexity and costs

Linkability between Provider and Relying Party remains (due to the nature of digital signatures)

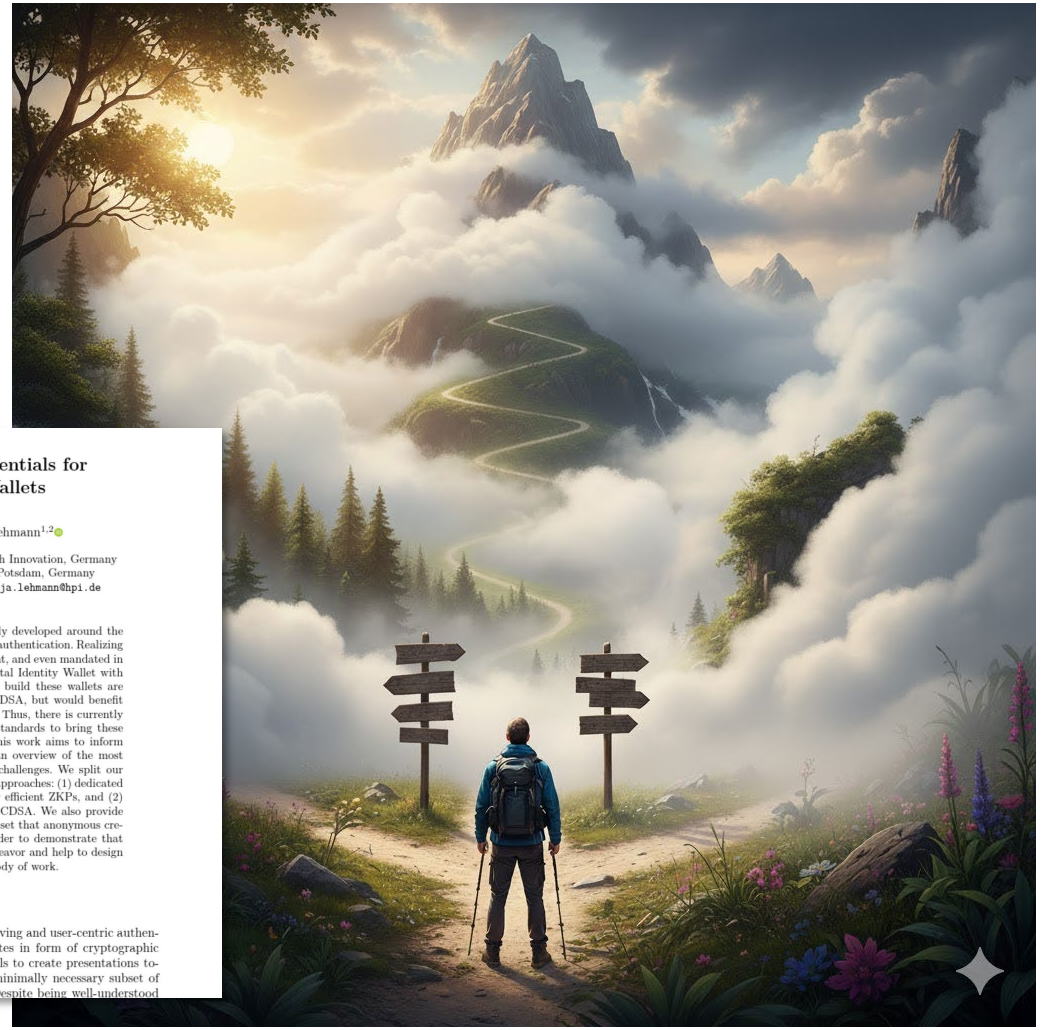
ZKP solve these issues and may offer additional features:

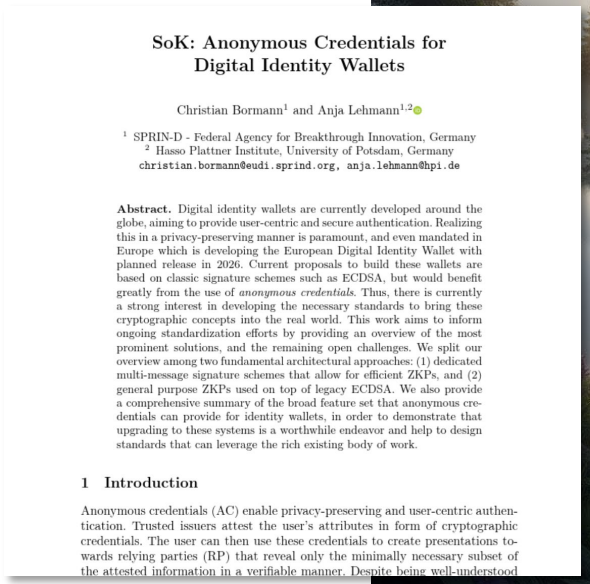
- Hiding issuers
- Pseudonyms
- Single key binding
- Range proofs
- …

Zero-Knowledge-Proofs (ZKP)

- “Cryptographers Feedback” in 2024 sparks discussion on ZKP for eIDAS
- Many possible solutions with no clear winner or favorite among cryptographers

We investigate the options!





SoK: Anonymous Credentials for Digital Identity Wallets

Christian Bormann[1] and Anja Lehmann[1,2]

[1] SPRIN-D - Federal Agency for Breakthrough Innovation, Germany
[2] Hasso Plattner Institute, University of Potsdam, Germany
christian.bormann@eudi.sprind.org, anja.lehmann@hpi.de

Abstract. Digital identity wallets are currently developed around the globe, aiming to provide user-centric and secure authentication. Realizing this in a privacy-preserving manner is paramount, and even mandated in Europe which is developing the European Digital Identity Wallet with planned release in 2026. Current proposals to build these wallets are based on classic signature schemes such as ECDSA, but would benefit greatly from the use of *anonymous credentials*. Thus, there is currently a strong interest in developing the necessary standards to bring these cryptographic concepts into the real world. This work aims to inform ongoing standardization efforts by providing an overview of the most prominent solutions, and the remaining open challenges. We split our overview among two fundamental architectural approaches: (1) dedicated multi-message signature schemes that allow for efficient ZKPs, and (2) general purpose ZKPs used on top of legacy ECDSA. We also provide a comprehensive summary of the broad feature set that anonymous credentials can provide for identity wallets, in order to demonstrate that upgrading to these systems is a worthwhile endeavor and help to design standards that can leverage the rich existing body of work.

1 Introduction

Anonymous credentials (AC) enable privacy-preserving and user-centric authentication. Trusted issuers attest the user's attributes in form of cryptographic credentials. The user can then use these credentials to create presentations towards relying parties (RP) that reveal only the minimally necessary subset of the attested information in a verifiable manner. Despite being well-understood

The Contenders

Option 1

BBS with legacy device binding

- Short-term solution suggested by Ubique in FUNKE challenge
- Solution uses BBS for issuer signatures & ECDSA for device binding
- Allows legacy Secure Elements within reasonable time (800 ms, 150 kB)

Option 2

BBS with native device binding

- Simple, efficient device binding w/o trust in hardware
- Requires support in hardware, tested by Yubico in FUNKE challenge
- Mature scheme with many possible extensions but no PQC

Option 3

Circuits-based ZKP

- General-purpose ZKP mechanisms, e.g. ZK-SNARKs, Google’s Longfellow
- Additional “ZKP layer”, allows use of legacy Secure Elements and existing infrastructure
- Very complex, more security reviews needed

Thank you for your attention!

Contact:

Dr. Torsten Lodderstedt

SPRIND – Federal Agency for Breakthrough Innovation

E-Mail:

Torsten.Lodderstedt@eudi.sprind.org

Contact:

Paul Bastian

Bundesdruckerei GmbH

E-Mail:

Paul.Bastian@bdr.de

Questions & Answers