

TeleTrust-Informationstag

"Elektronische Signatur und Vertrauensdienste"

Berlin, 19.11.2024

Auf dem Weg zum deutschen EUDI Wallet Ökosystem

Dr. Torsten Lodderstedt, Bundesagentur für Sprunginnovation
Paul Bastian, Bundesdruckerei

THE GERMAN EUDIW PROJECT



Germany is developing the concept for a digital ecosystem for **secure, privacy-friendly and user-friendly EUDI Wallet(s)** in an **open architecture and consultation process**.



The associated project is being carried out by the Federal Agency for Disruptive Innovations (SPRIND GmbH) on behalf of the Federal Ministry of the Interior and Community with the Federal Office for Information Security and supported by Bundesdruckerei GmbH, Fraunhofer Institute for Applied and Integrated Security (Fraunhofer AISEC) and PricewaterhouseCoopers.



SPRIN-D



OBJECTIVES OF THE PROJECT

QUESTIONS WE AIM TO ANSWER



What are the **needs** in the context of digital wallets, what are the **benefits** and **risks** ?



How can we ensure that **society embraces the concept** and the wallet ecosystem going forward?



What should be **provided by government** and what can be **left to the market**?

CONTEXT AND STARTING CONDITIONS OF OUR PROJECT



Ecosystem Design

- Meeting the German needs and specialties
 - no persistent, global person identifier
 - decentralized eID system
 - federalistic structure of our nation (>11000 municipalities, 16 states, federal government)



Interoperability

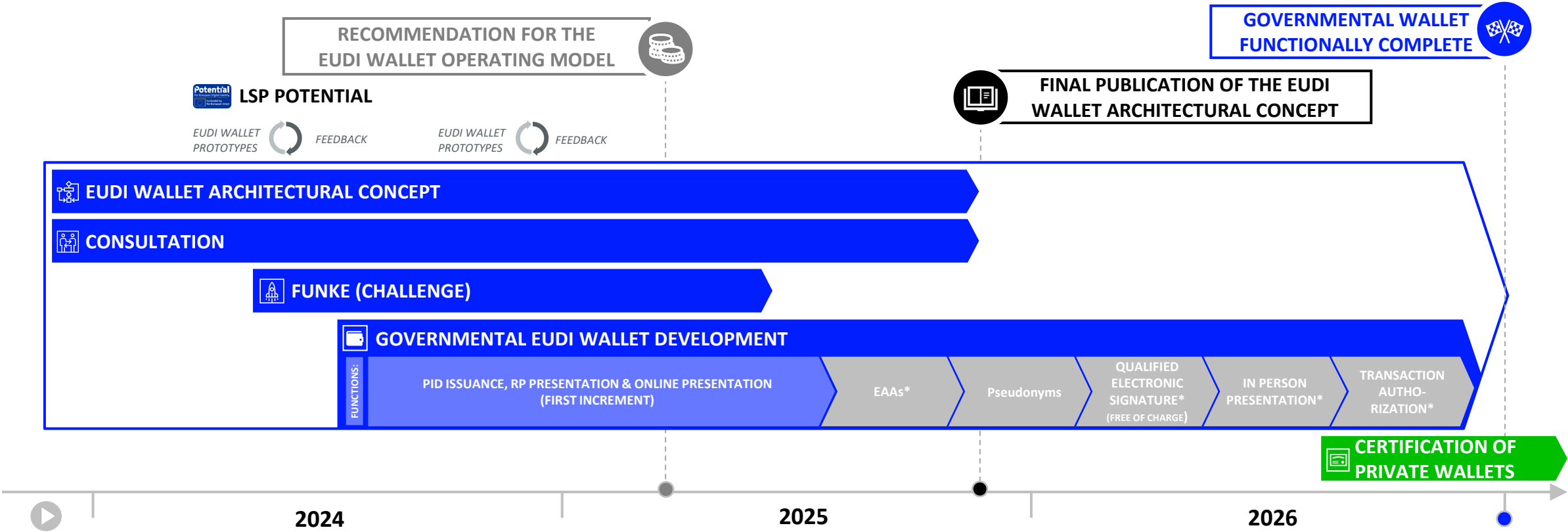
- Ensure interoperability with RPs, Providers and Wallets across the EU and beyond



Feasibility

- Best combination of security, privacy, usability, and user reach
- What is feasible today and tomorrow?
- Evaluation through prototypes and tests

PROJECT OVERVIEW

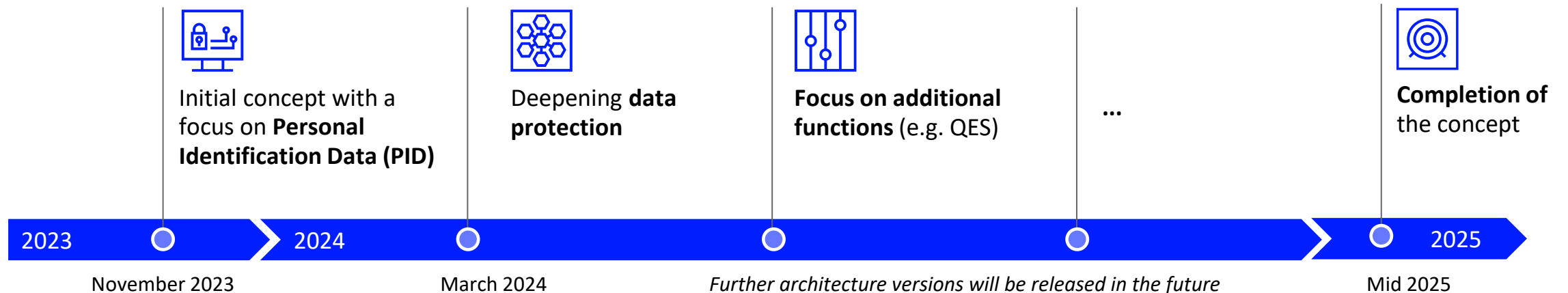


IN THE ARCHITECTURE PROCESS, EXPERTS REGULARLY PUBLISH ITERATIONS WITH A DIFFERENT FOCUS

The **concept** for a **digital wallet ecosystem** is being developed by experts with the **ongoing involvement of the public**. The aim of this constant exchange is to ensure a **high level of user-friendliness and acceptance** of the wallet.



Roadmap of the architecture versions



THE CONSULTATION PROCESS ENSURES THE COMPREHENSIVE INVOLVEMENT OF RELEVANT STAKEHOLDERS AND THE PUBLIC

Consultation formats to accompany the architecture process



Workshops

- **Development** of **results** and feedback with stakeholders
- Workshops are offered **on new architecture versions**



Open Online Consultations

- **Low-threshold offer** for open questions on specific topics
- Consultation hours are held on **operating models**, for example



Interviews

- Determining the **needs of relevant stakeholder groups**
- Participation of **groups with special needs**



Would you like to participate in the consultation process?



All open consultation formats are announced and documented on **OpenCoDE**



Comments and feedback on the architectural concept and the consultation process can be submitted there



Open CoDE
Software



THE “EUDI WALLET PROTOTYPES” FUNKE - TESTS OF THE ARCHITECTURE CONCEPT AND NEW IDEAS FOR HARD CHALLENGES

Innovation competition Funke



6 teams took part in the **funded track**,
5 teams in the **non-funded track**



Jury comprised of **technical experts** and
representatives from **politics and civil society**



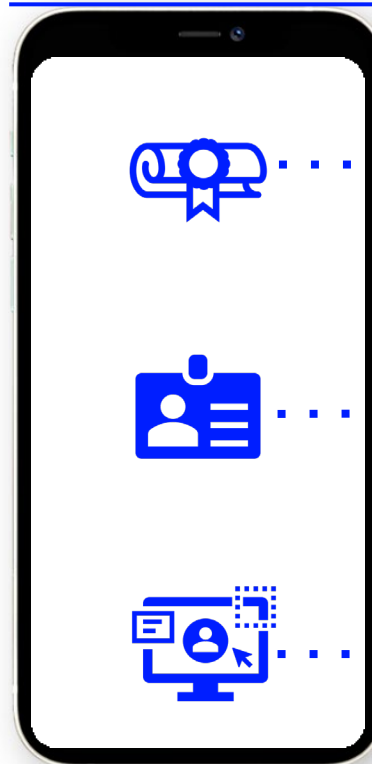
All PID implementation approaches of the
architecture concept are tested



Once stage 1 is complete, the prototypes will be
made available to the **pilot project POTENTIAL***
for **testing in six use cases**.

*Within the framework of Potential, a consortium of 19 countries & 140 public and private partners is working to ensure the interoperability of EUDI wallets in six use cases.

Core functions of the EUDI wallet prototype



Level 1

Issuing & presentation of **personal identification data (PID)**

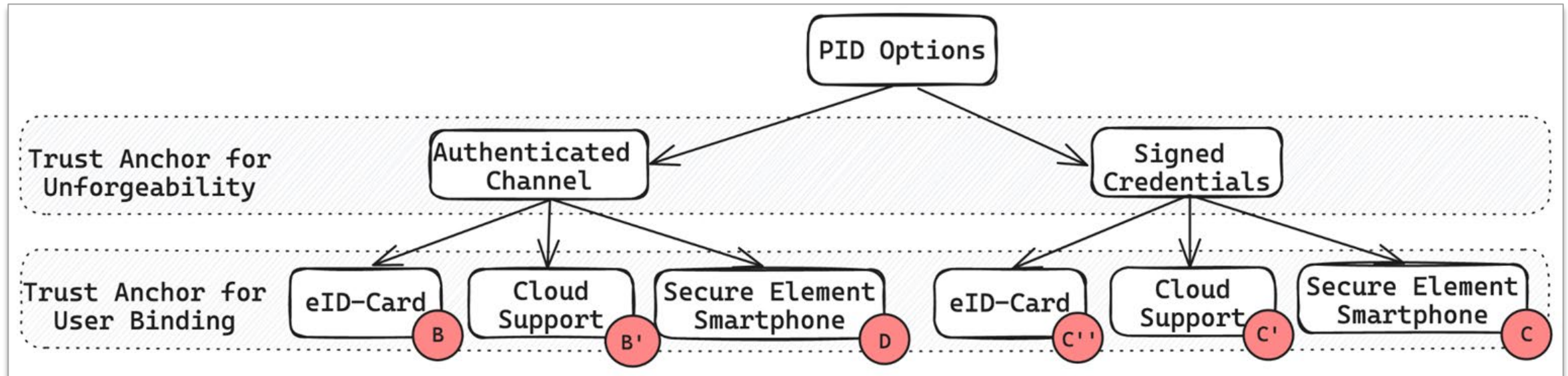
Level 2

Issuing & presentation of **electronic certificates (EAs)**

Level 3

Pseudonymous login, qualified electronic signature (QES) & payment

6 OPTIONS TO EVALUATE FOR PID HANDLING



Options differ in regard to **(Non-)repudiation, cryptographic key storage and architecture design**

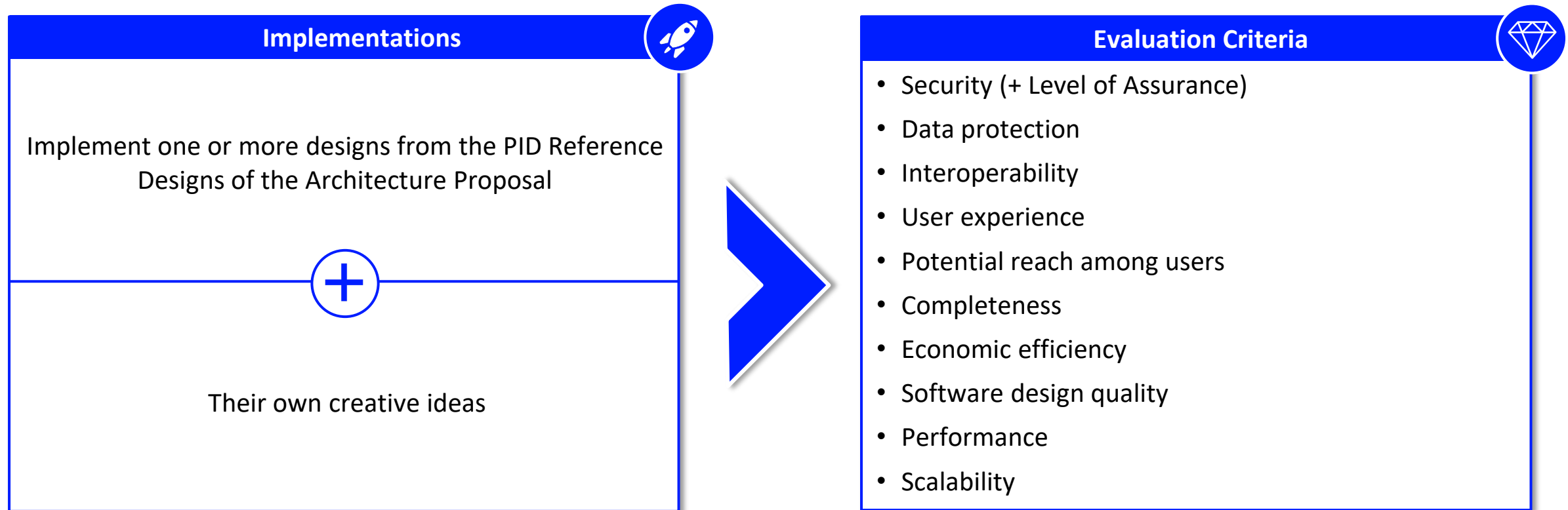


All PID design options will be **implemented and tested** in the FUNKE Challenge

IMPLEMENTATION OF THE TEAMS

	Authenticated Channel			Signed Data		
	E-ID Card B	Cloud Support B'	Secure Element D	E-ID Card C''	Cloud Support C'	Secure Element C
Animo		✓				✓
Authada	✓*		✓	✓		✓
Governikus	✓	✓				
Sphereon				✓*		✓
TICE GmbH						✓
Ubique Innovation AG					✓	✓
Google					✓	✓
Kaprion						✓*
Lissi				✓		✓
Samsung						✓*
wwWallet						✓

THE GOAL IS A SECURE AND INTEROPERABLE WALLET THAT CAN ACHIEVE A HIGH LEVEL OF USER REACH AND ACCEPTANCE



THE FUNKE TEAMS

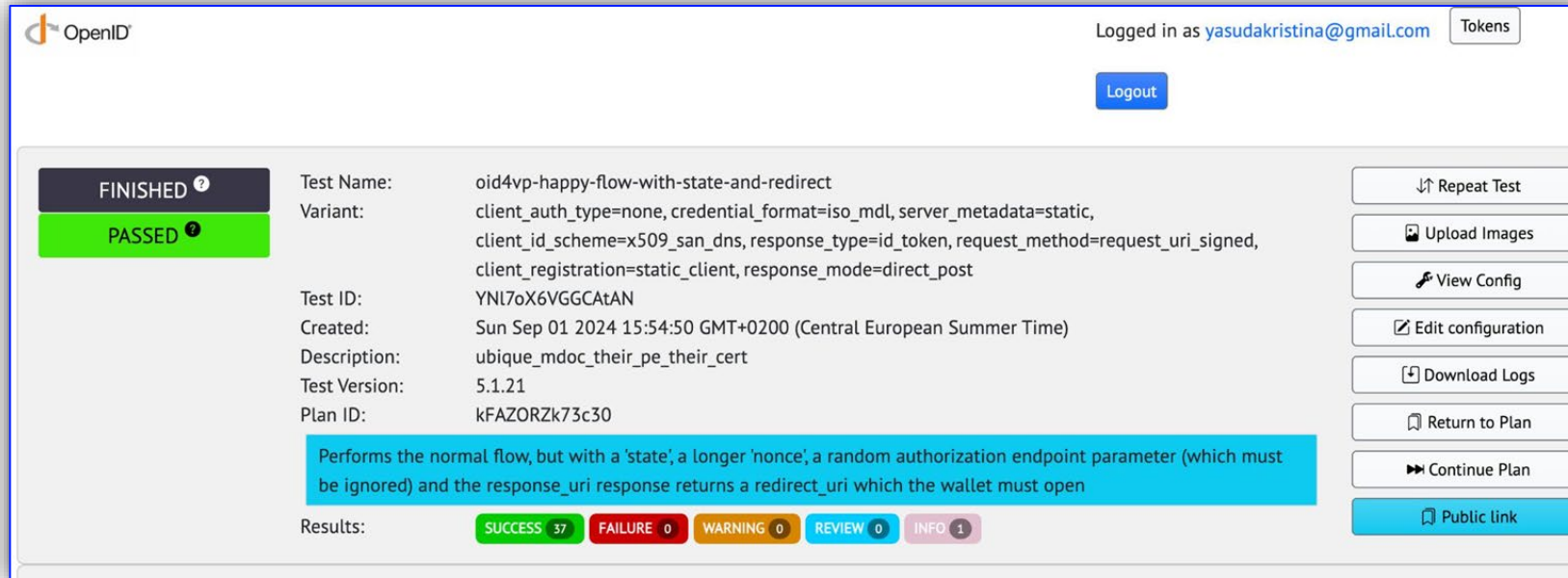
SELECTED TEAMS: FUNDED TRACK

 AUTHADA GmbH	 TICE GmbH	 ubique Innovation AG
 GOVERNIKUS Governikus	 ANIMO Animo Solutions	 sphereon Sphereon

SELECTED TEAMS: NON-FUNDED TRACK

 LISSI Lissi	 KAPRION Technologies	 SUNET, GUNET, YUBICO
 Android	SAMSUNG Samsung Electronics	

OPENID CONFORMANCE TESTS FOR OPENID4VP



The screenshot shows the OpenID Connect test results page. At the top, it says 'OpenID' and 'Logged in as yasudakristina@gmail.com' with a 'Logout' button. The test status is 'FINISHED' and 'PASSED'. The test name is 'oid4vp-happy-flow-with-state-and-redirect'. The variant is 'client_auth_type=none, credential_format=iso_mdl, server_metadata=static, client_id_scheme=x509_san_dns, response_type=id_token, request_method=request_uri_signed, client_registration=static_client, response_mode=direct_post'. The test ID is 'YNI7oX6VGGCAAtAN'. The created date is 'Sun Sep 01 2024 15:54:50 GMT+0200 (Central European Summer Time)'. The description is 'ubique_mdoc_their_pe_their_cert'. The test version is '5.1.21'. The plan ID is 'kFAZORZk73c30'. A blue box contains the description: 'Performs the normal flow, but with a 'state', a longer 'nonce', a random authorization endpoint parameter (which must be ignored) and the response_uri response returns a redirect_uri which the wallet must open'. The results show 'SUCCESS 37', 'FAILURE 0', 'WARNING 0', 'REVIEW 0', and 'INFO 1'. On the right, there are buttons for 'Repeat Test', 'Upload Images', 'View Config', 'Edit configuration', 'Download Logs', 'Return to Plan', 'Continue Plan', and 'Public link'.



**PASSED at
submission:**

ubique 



LISSI



ANIMO

LSP POTENTIAL TESTING

LSP POTENTIAL Use-Case	Funke Team	
Use Case 1: eGov Services	wwWalet	
Use Case 2: Bank Account Opening	Lissi	Animo
Use Case 3: SIM Card Registration	Samsung	Authada
Use Case 4: Mobile Driving License	Google	Animo
Use Case 5: Qualified eSignature	Sphereon	Authada
Use Case 6: ePrescription	Ubique	

THE SCOPE OF THE SECOND STAGE

Goals

- The Goal of the level is to implement generic support for various EAAs in combination with the possibility of non-traceability and very good UX.
- Issuance and Presentation of EAAs
 - **mdoc** and **SD-JWT VC** for Credential format
 - **OpenID4VP** for online presentation
 - **OpenID4VCI** for issuance
 - **ISO 18013-5** for in-person presentation of mdoc-based EAAs
 - Proposals for the presentation of SD-JWT VC in in-person scenarios are welcome



STAGE 2 ends on the 10th of december, Jury decision will be announced during Funke Conference the day after.

EUDIW Ecosystem Rollout

GERMAN GOVERNMENT RECENTLY DECIDED IN FAVOR OF A HYBRID MODEL FOR WALLET PROVIDERS

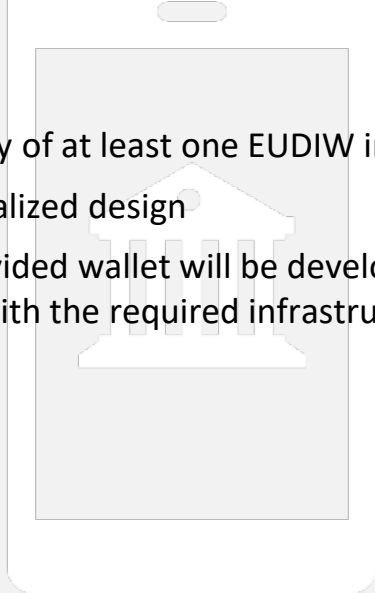
DE will build a Government-provided EUDIW

Ensures Sovereignty

Guarantees availability of at least one EUDIW in DE

Aims for fully decentralized design

The Government-provided wallet will be developed and rolled out incrementally along with the required infrastructure

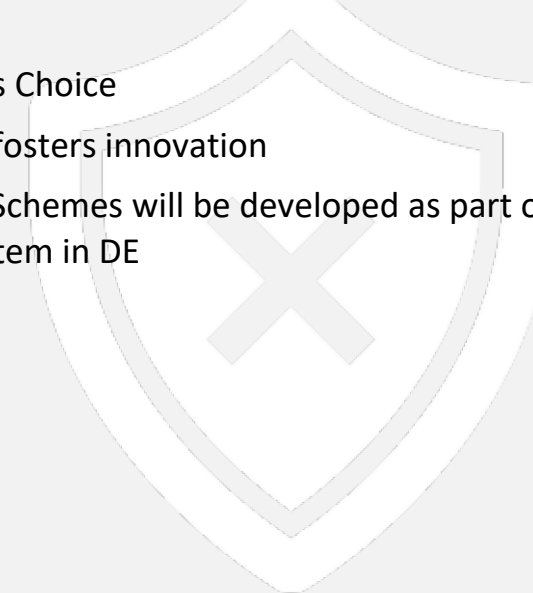


DE will be open to alternative Wallet Providers

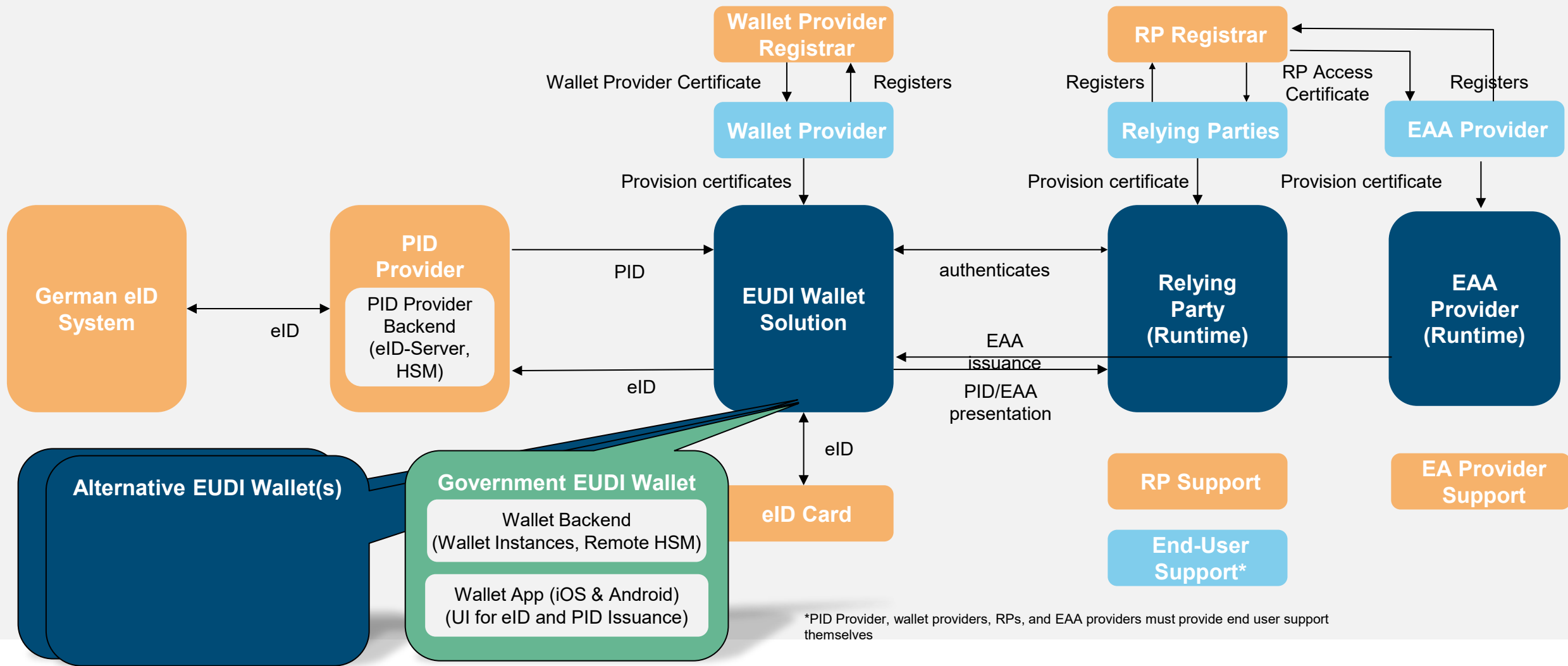
Trust requires Choice

Competition fosters innovation

Certification Schemes will be developed as part of the establishment of the ecosystem in DE



German EUDIW Ecosystem architecture (Draft)



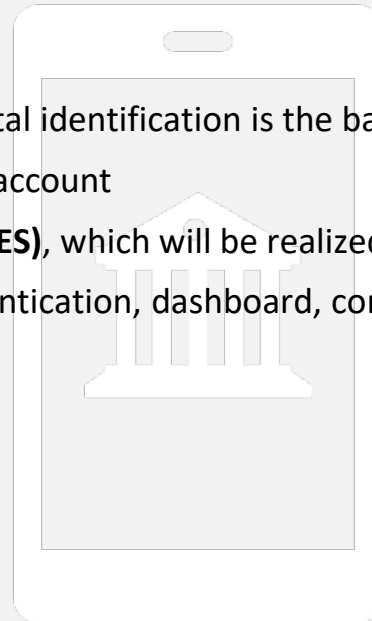
THE FIRST ITERATION OF THE GOVERNMENT-PROVIDED EUDIW

Functions of the first iteration of the EUDI Wallet

Focus on Identification (PID) on LoA High as secure and digital identification is the basic function of the EUDIW

- **Identification with Relying Parties**, e.g. opening of a bank account
- **Building block for further functions of the wallet (EAAs, QES)**, which will be realized in subsequent iterations.

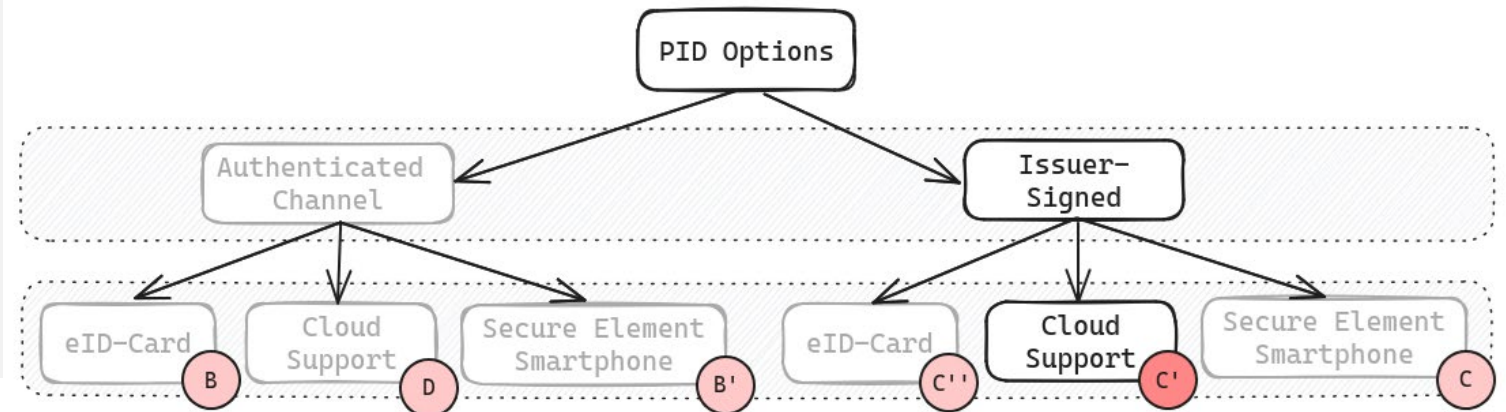
Empowerment of Users is a further core objective (RP authentication, dashboard, complaints)



THE FIRST ITERATION OF THE GOVERNMENT-PROVIDED EUDIW

Technical Design of the first iteration of the EUDI Wallet

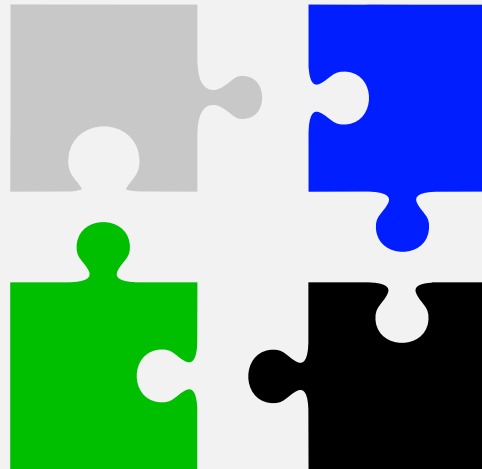
- PID data is stored encrypted on the phone
- PID device/confirmation keys are managed in **Cloud HSM**
- PID is using **Signed Data** for best interoperability



WHY CLOUD HSM ?

Most phones these days **lack a security module** with the **required security level** we could utilize (either don't have it at all, or the user authentication is not sufficient or we cannot access it), using a Cloud HSM allows us to reach the most users

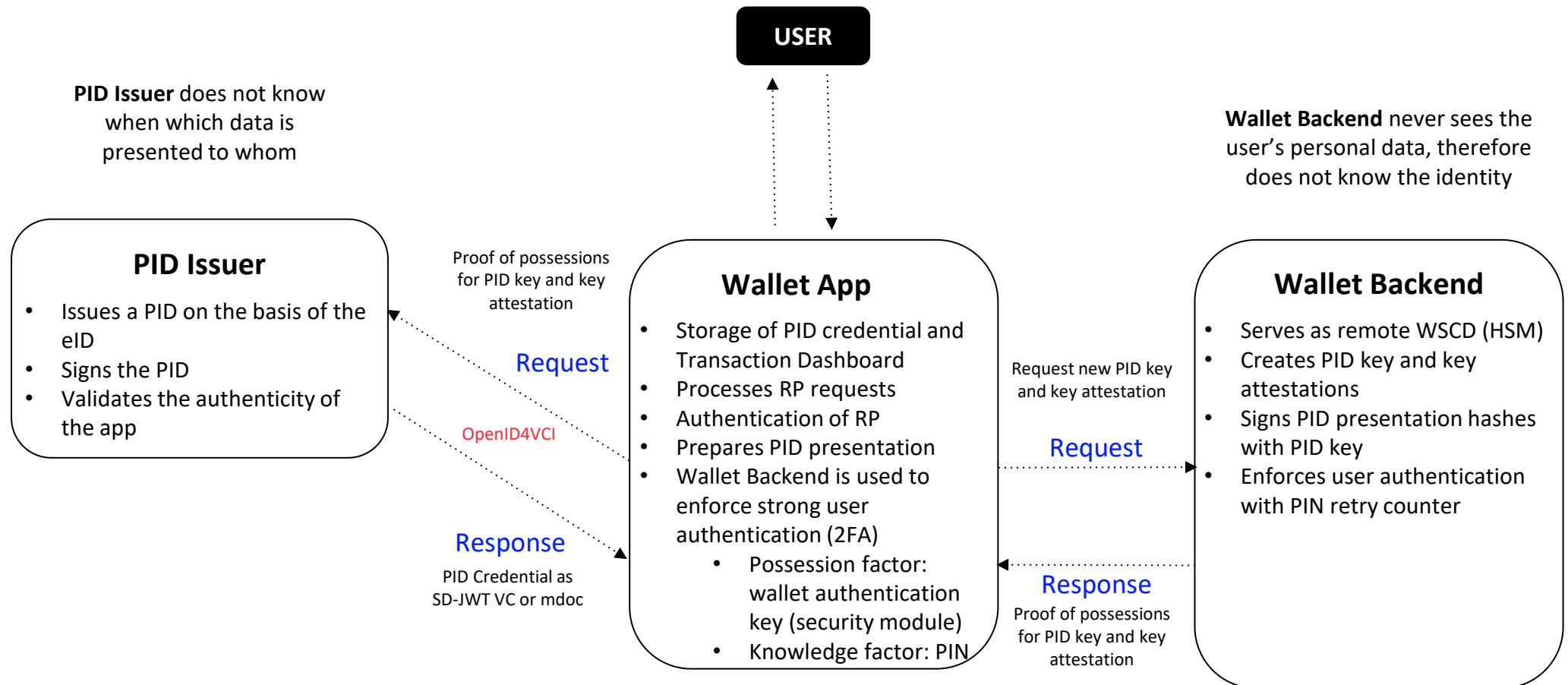
Interfaces of the wallet are **ARF compliant** and can be kept for the **subsequent increments**



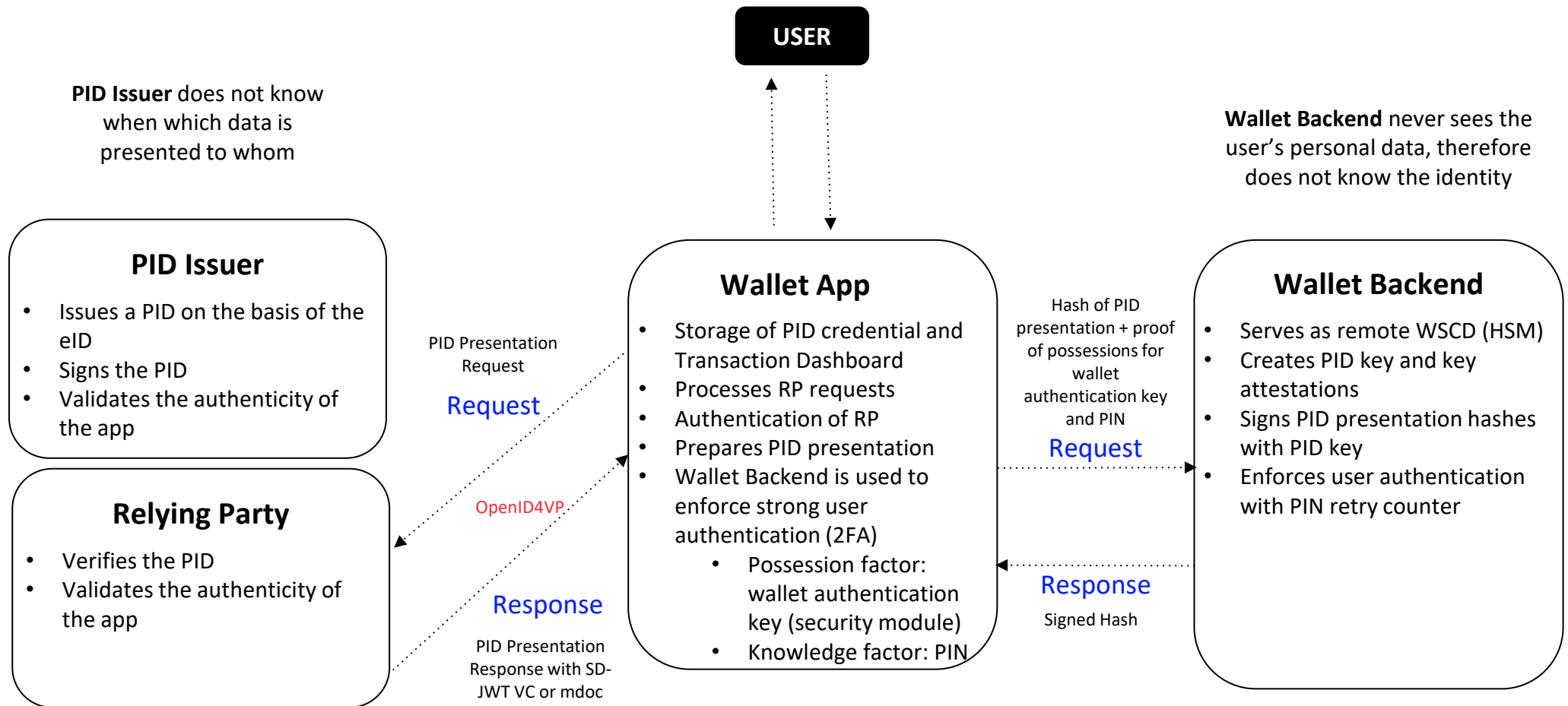
Prototypical experience with **eUICCs** indicate this approach **needs more work to become a viable solution** for large scale deployments

Design allows for **incremental migration to decentralized key management** (as suitable solutions become available and/or for lower assurance levels)

UNDER THE HOOD (FOCUS ON ISSUANCE)



UNDER THE HOOD (FOCUS ON PRESENTATION)



RELYING PARTY MANAGEMENT

Requirements from the eIDAS legal text

Relying Parties must register with Member State at a **Relying Party Registrar**:

- name
- register number
- **Intended use**
- indication of the **data to be requested** from users

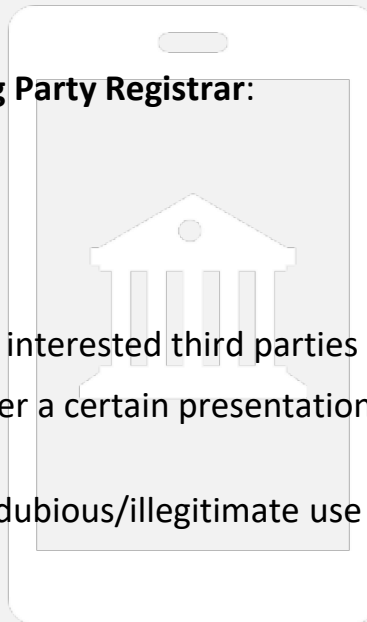
Member state publishes RP data, which allows inspection by interested third parties

RP must authenticate with EUDIW, wallet must check whether a certain presentation request matches the registered “indication of the data to be requested by the relying party from users”

Objective: this creates transparency and allows to check for dubious/illegitimate use cases

Further requirements from the ARF

PID/EAA Providers may use **embedded disclosure policy** to govern authorization of Relying Parties



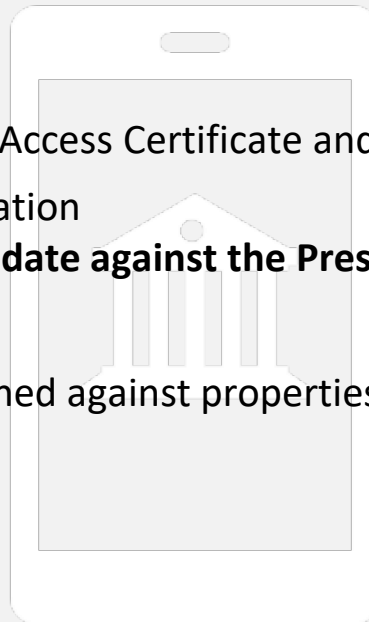
RELYING PARTY MANAGEMENT

Technical Design Proposals (under discussion)

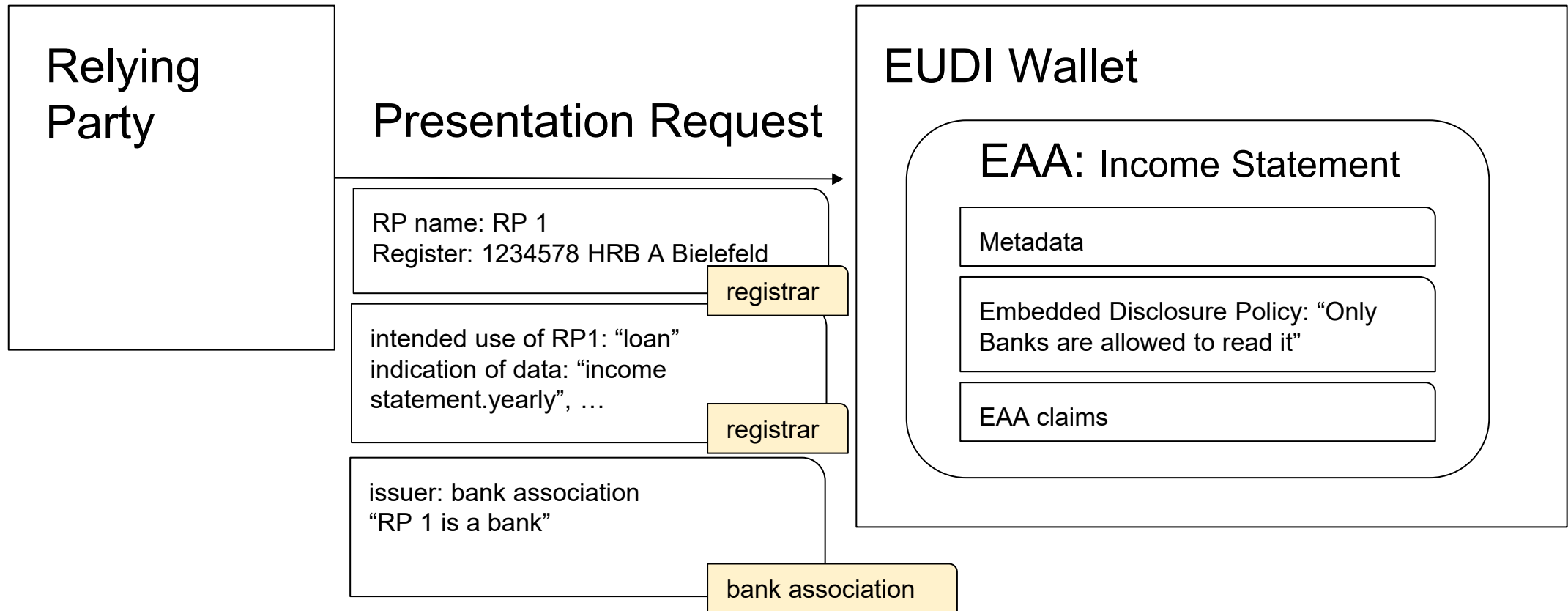
Relying Party Registrar puts relevant RP data into RP Access Certificate and additional attestations

- EUDI Wallet must display RP data for authentication
- EUDI Wallet must display **intended use** and **validate against the Presentation Request**

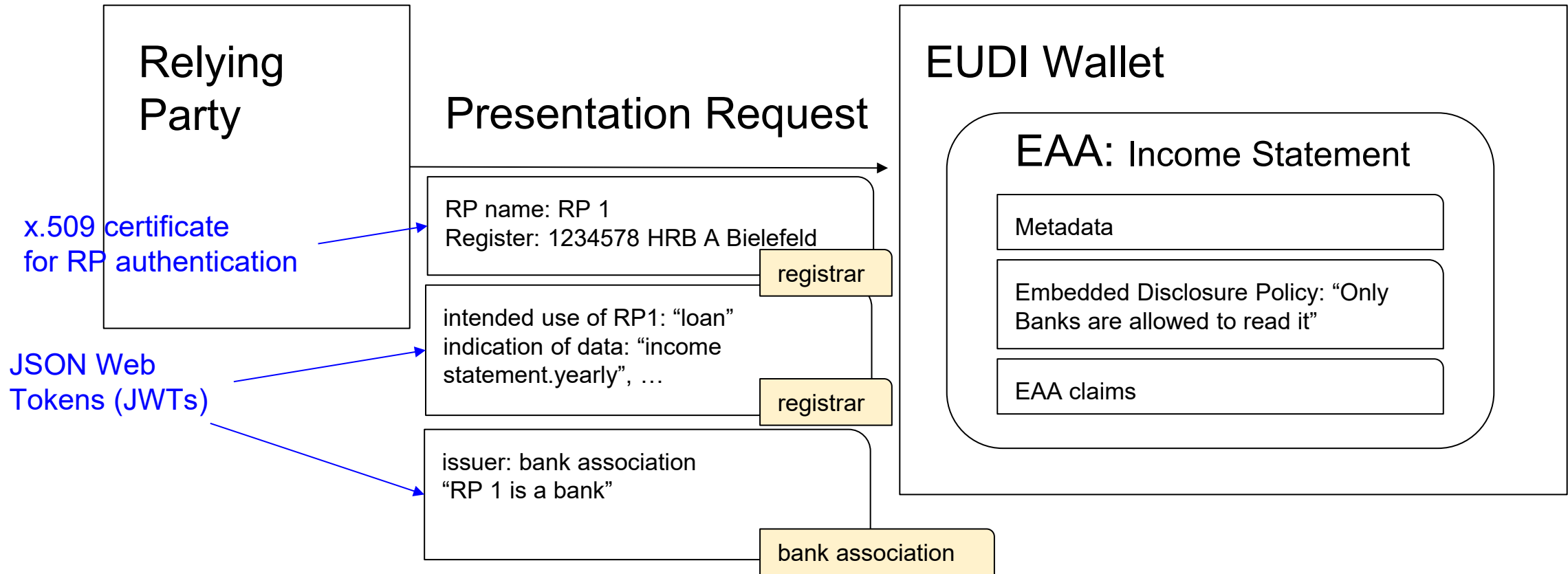
EAA provider specific disclosure policies will be matched against properties of the RP asserted (typically be domain specific authorities) in additional attestations



RELYING PARTY MANAGEMENT



RELYING PARTY MANAGEMENT



FUTURE TOPIC: DECENTRALIZED KEY STORAGE

Cloud HSM

- The current technology of key storage in mobile devices and its market fragmentation make decentralized key storage complicated or unavailable
- Cloud HSM is an intermediate solution



Decentralized Key Storage on User's Device

- The long-term goal of BMI is to have key storage in the Secure Element of the User's device
- Best option in terms of privacy, versatility and costs
- Mid-term: Use Native/Local WSCDs for lower assurance levels

FUTURE TOPIC: ZERO KNOWLEDGE PROOFS

EUDIW shall be privacy preserving

- Unlinkability across RPs is hard to implement with traditional cryptography
- Requires ephemeral credentials and batch credential issuance
- Feasible but the issuance process is more complex and requires a secure, active „connection“ between wallet and issuer to fetch fresh credentials
- The federalistic organization of Germany would require to support this for 100k+ EAA providers (municipalities, schools, enterprises, ...)



Zero Knowledge Proofs could be an alternative

- Unlinkability can be implemented with single, long living credential
- Requires standardization, recognition, implementation, and support in Secure Elements

We have started to look into this topic as long term option

In case of questions, please contact us:

Via Open CoDE:

