# Der Weg zur deutschen EUDI-Wallet

21.01.25
Berlin
Paul Bastian (Bundesdruckerei GmbH)
Andreas Wand (D-Trust GmbH)

# Was bisher geschah: 2020 – Forderung Digitale Identität für alle

*„Jedes Mal, wenn eine Website uns auffordert, eine neue digitale Identität zu erstellen oder uns bequem über eine große Plattform anzumelden, haben wir in Wirklichkeit* ***keine Ahnung, was mit unseren Daten geschieht****. Aus diesem Grund wird die Kommission demnächst eine* ***sichere europäische digitale Identität*** *vorschlagen. Eine, der wir vertrauen, und die Bürgerinnen und Bürger überall in Europa nutzen können, um alles zu tun, vom Steuern zahlen bis hin zum Fahrrad mieten. Eine Technologie, bei der wir* ***selbst kontrollieren*** *können, welche Daten wie verwendet werden.“*

Ursula von der Leyen, Präsidentin der Europäischen Kommission, 16. September 2020

https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_de

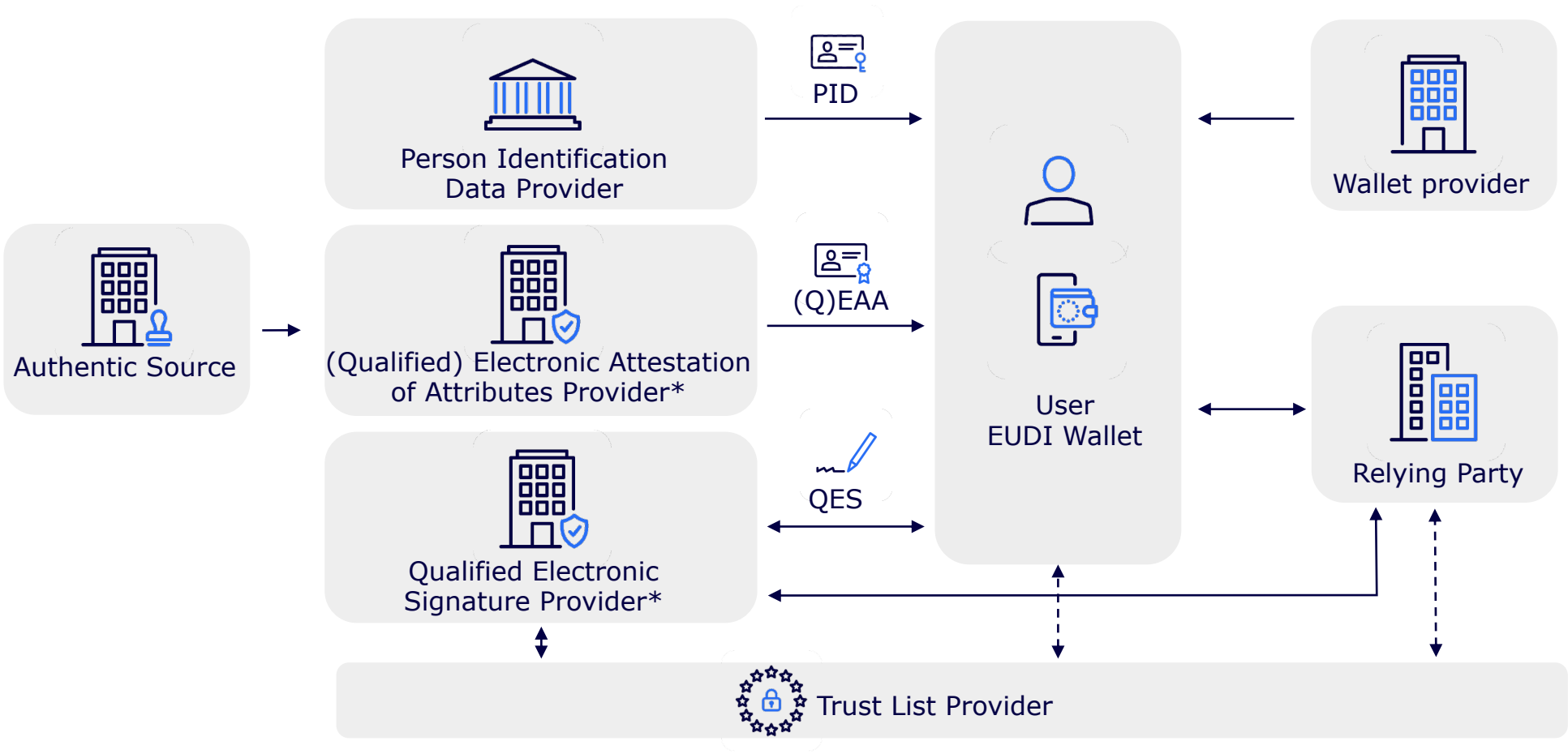
# Europaweit sicher identifizieren, Nachweise erbringen und unterschreiben


Hauptfunktionen der EUDI-Wallet

- Identifizierungsmittel
- Nachweise
- Signatur / Siegel
- „Bezahlung“

https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/EU+Digital+Identity+Wallet+Home

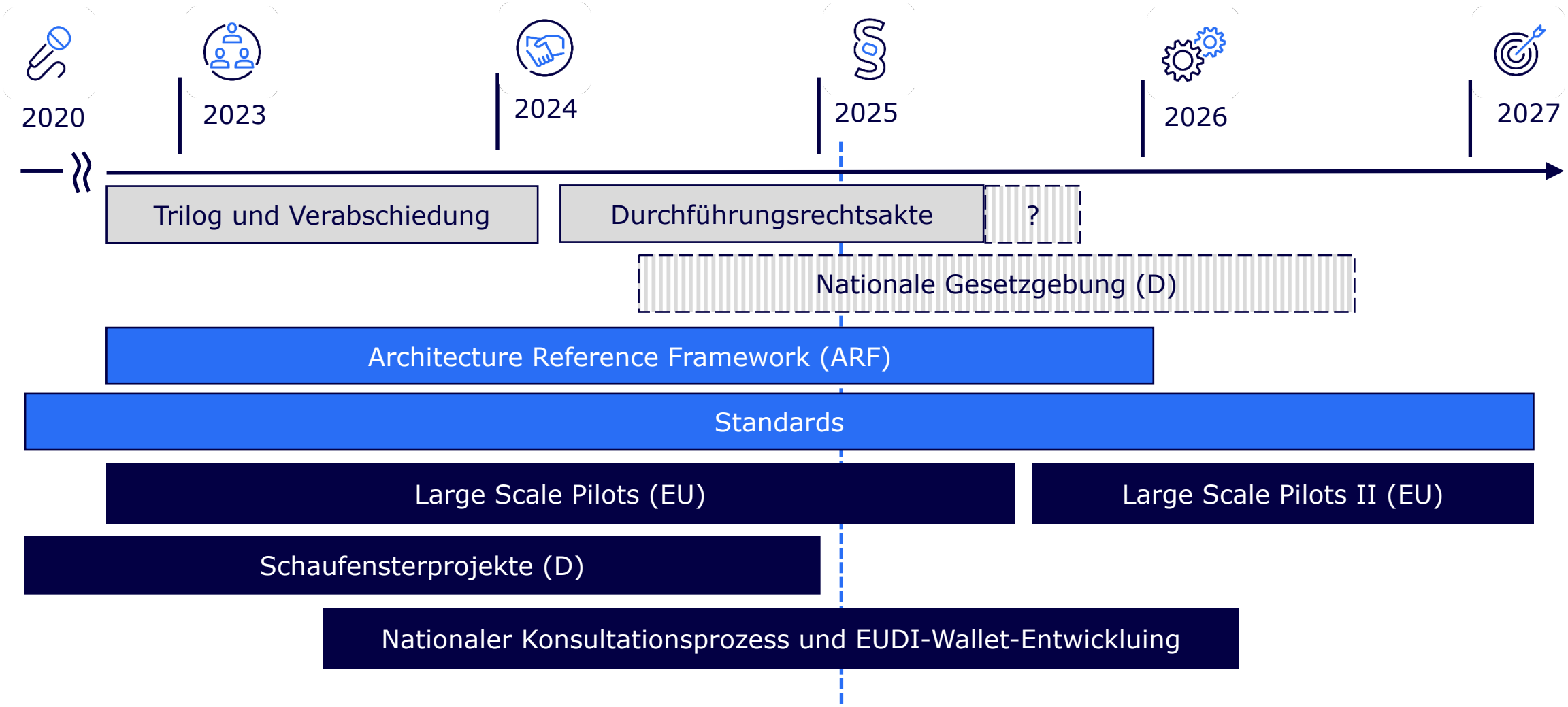
# Rollenmodell entsprechend eIDAS 2.0 Architecture Reference Framework (ARF) ermöglicht dezentrales Identitätsökosystem



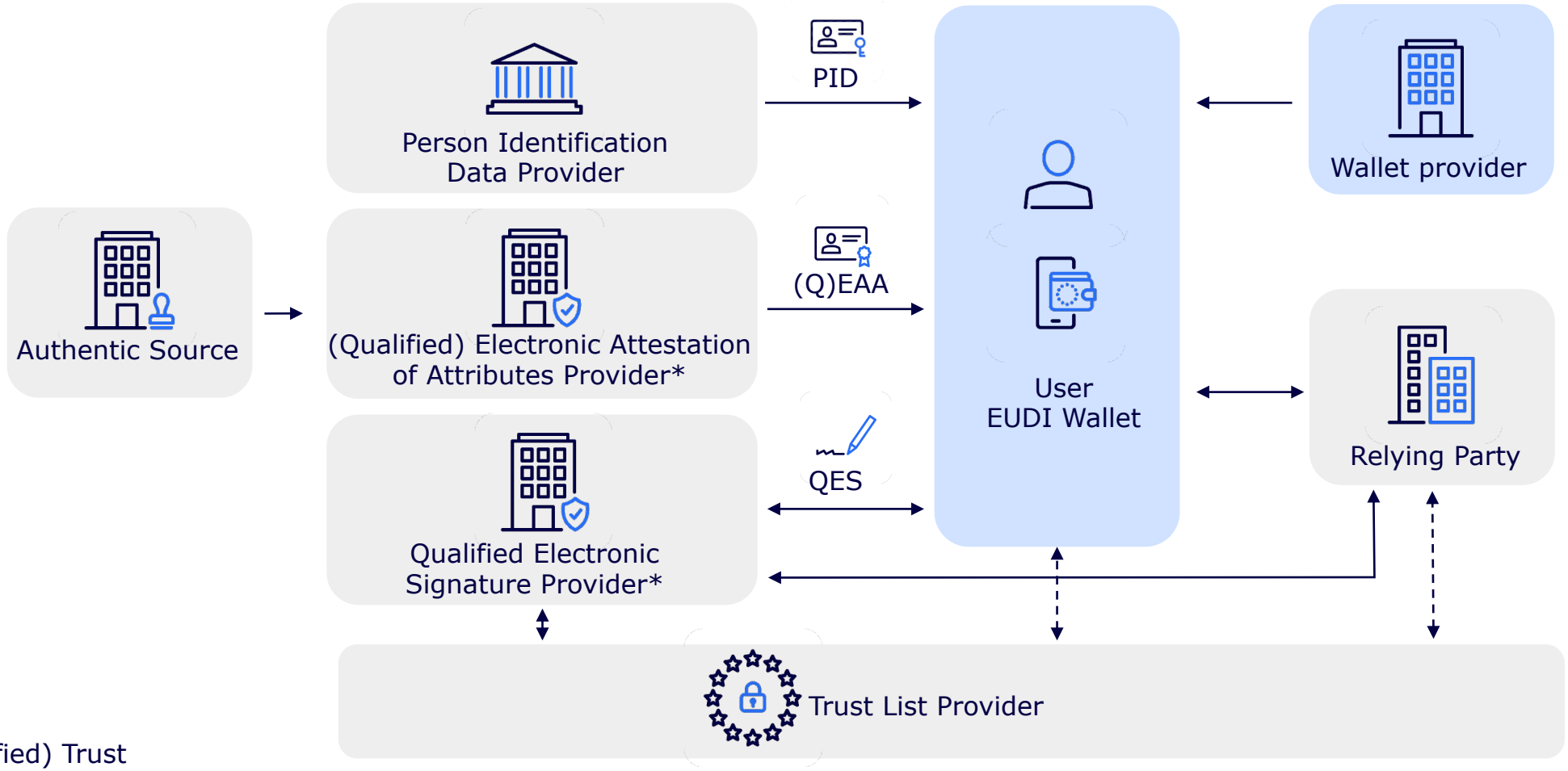

*(Qualified) Trust Service Provider

https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/arf.md

# Zeitplan eIDAS 2.0 - über die Hälfte des Weges geschafft



# Das Rollenmodell entsprechend eIDAS 2.0 Architecture Reference Framework (ARF) ermöglicht dezentrales Identitätsökosystem




*(Qualified) Trust Service Provider

https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/arf.md

# 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.

Federal Ministry of the Interior and Community

SPRIN-D

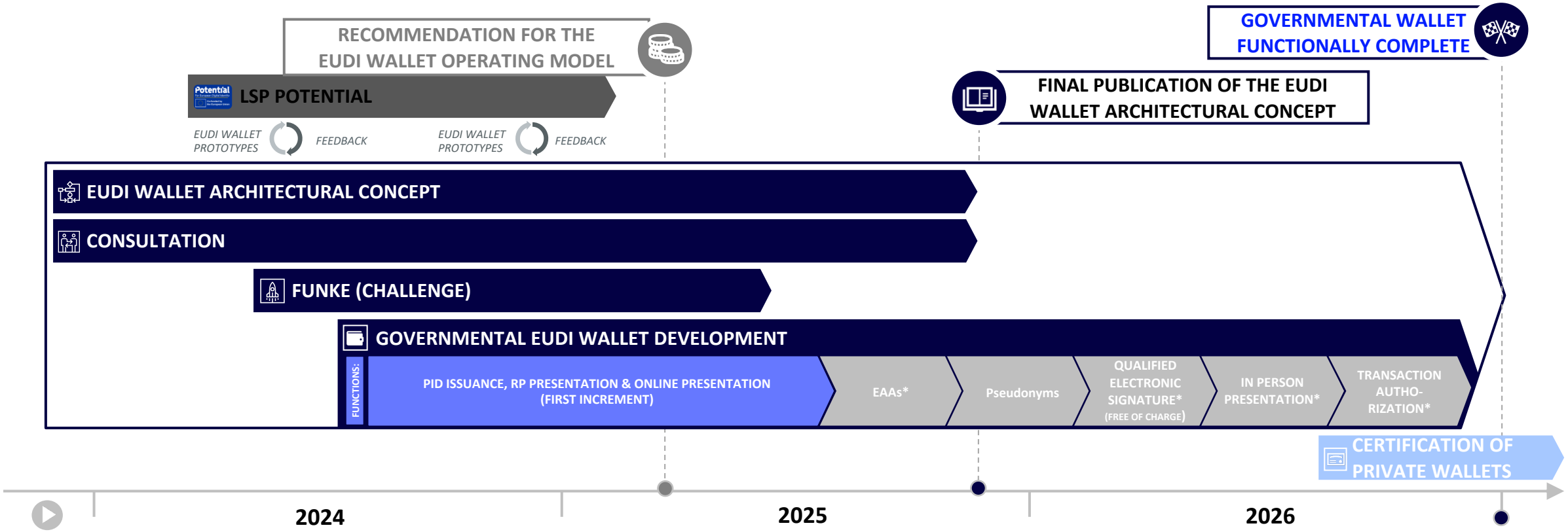
Bundesamt für Sicherheit in der Informationstechnik

Fraunhofer AISEC

BUNDESDRUCKEREI

pwc

# PROJECT OVERVIEW



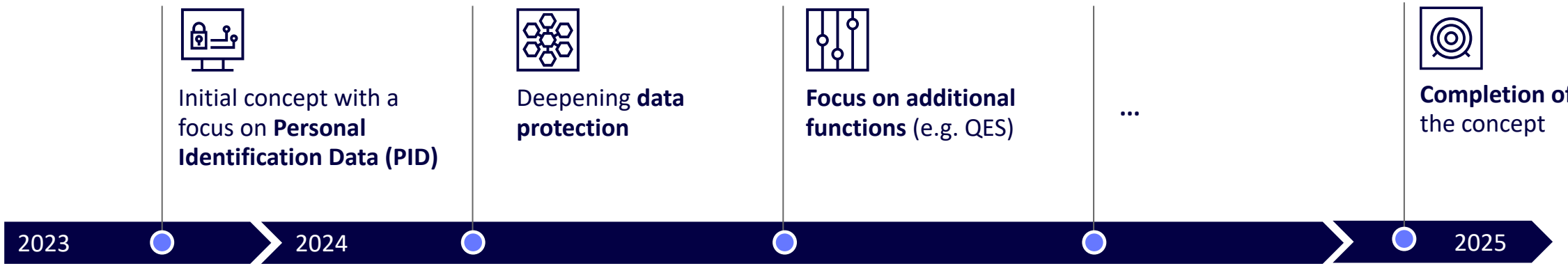

START: JULY 2023

*The exact development iteration have not yet been defined

# 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 COMPREHENSICE 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

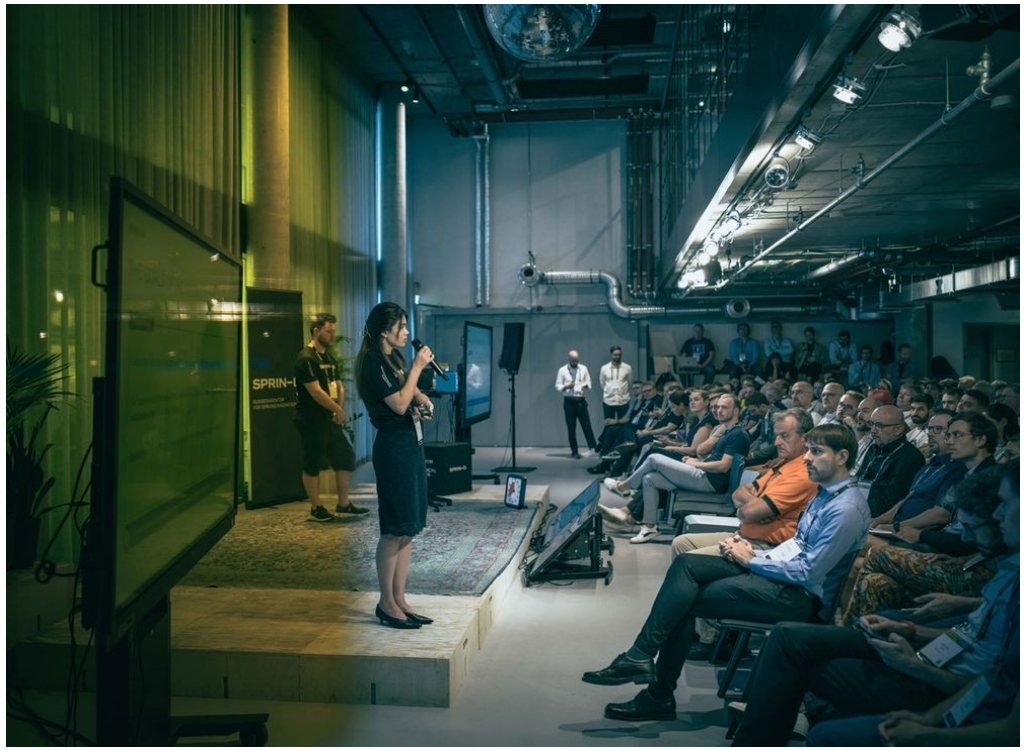
6 teams took part in the **funded track**,
5 teams in the **non-funded track**

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

**All PID implementation approaches** of the architecture concept are tested

FUNKE gives useful insight for the first iteration of the German Government-provided Wallet, furthermore the FUNKE Wallets are used in LSP POTENITAL.

## FUNKE Conferences



# 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

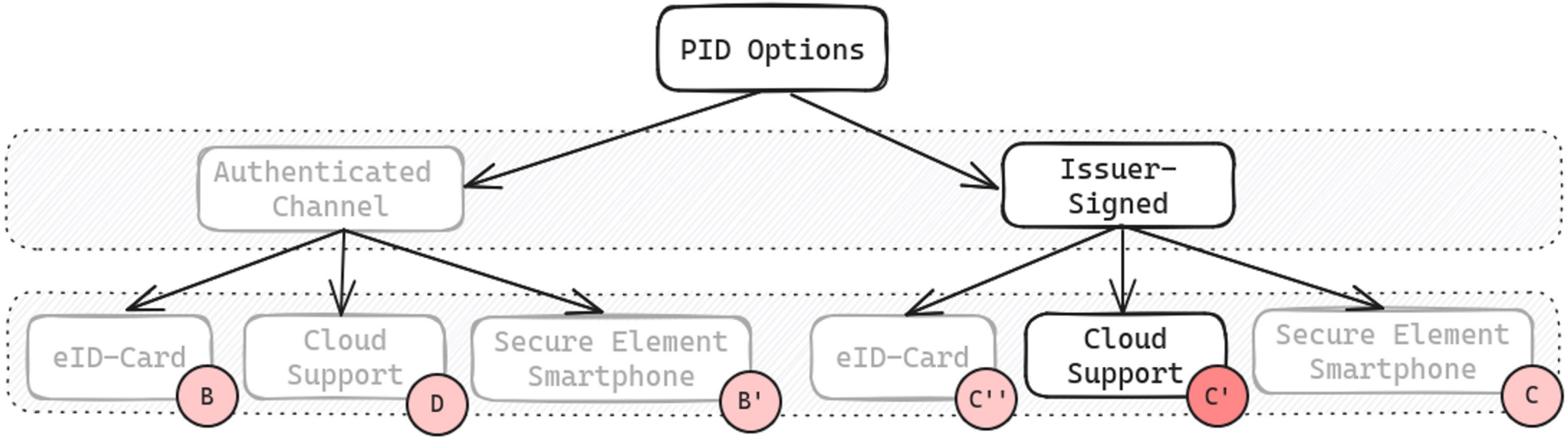
Competition fosters innovation

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

# THE FIRST ITERATION OF THE GOVERNMENT-PROVIDED EUDIW

**Decision for PID Option C' from Architecture Proposal**

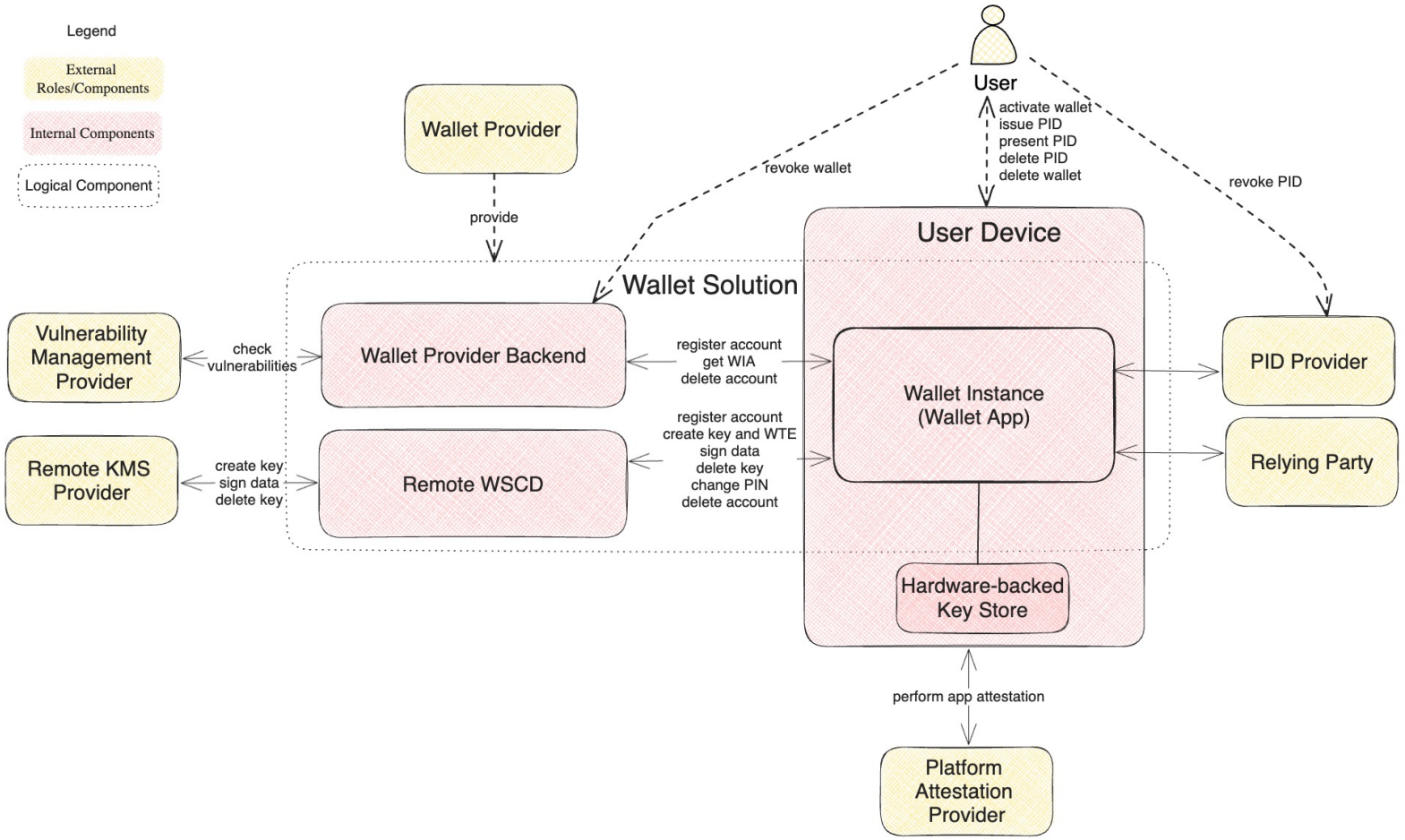
- PID data is stored encrypted on the phone
- PID device/confirmation keys are managed in Cloud HSM
- PID is using Signed Data for best interoperability



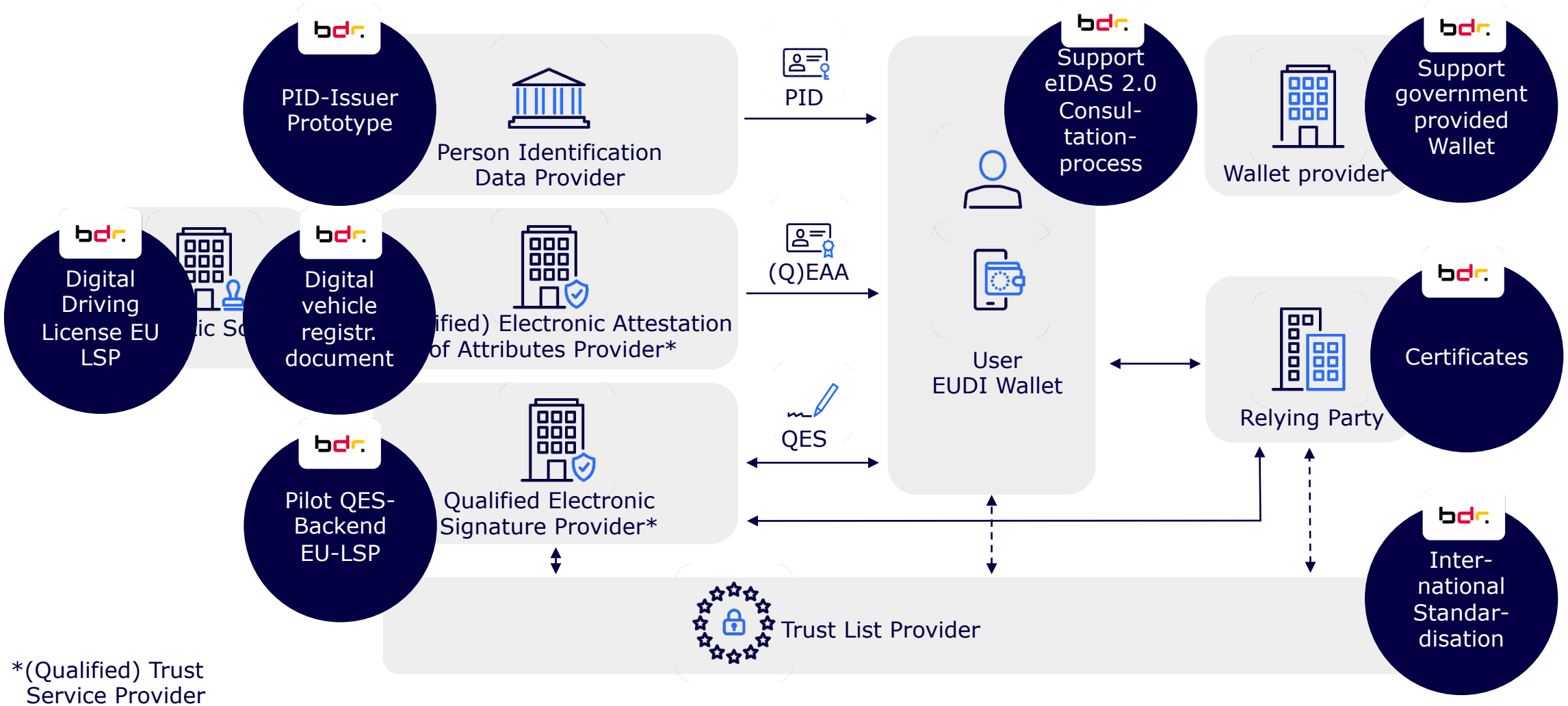
# THE FIRST ITERATION OF THE GOVERNMENT-PROVIDED EUDIW

**Technical Design of the first iteration of the EUDI Wallet**

- using EU Reference Implementation
- Backend divided into Wallet Provider Backend and Remote WSCD
- leveraging Key Management Solution with HSM as-a-service
- design for secure lifecycles for PID Attestations, Wallet Attestations and Key Attestations



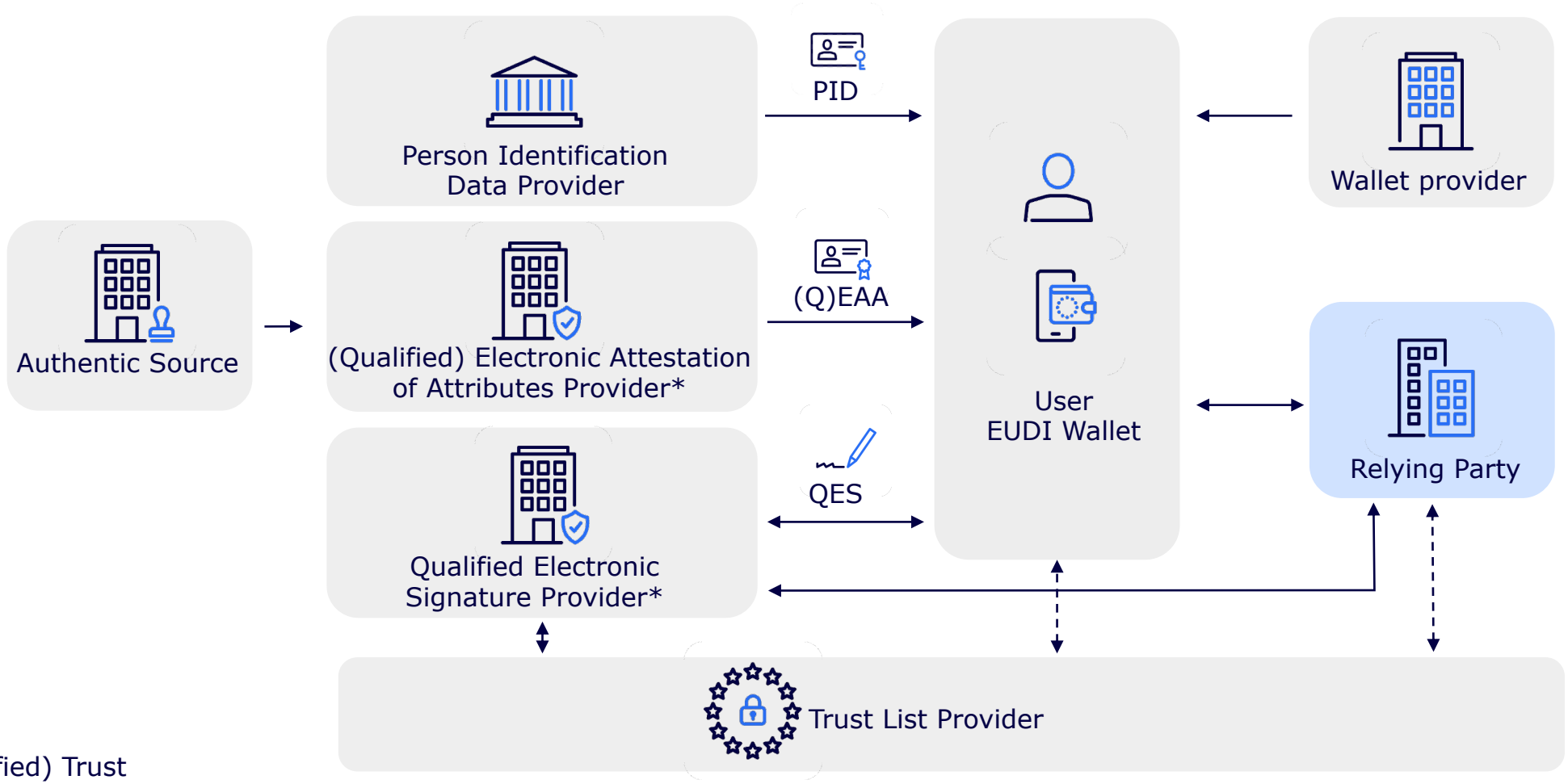
# Das Rollenmodell entsprechend eIDAS 2.0 Architecture Reference Framework (ARF) ermöglicht dezentrales Identitätsökosystem




*(Qualified) Trust Service Provider

https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/arf.md

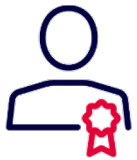
# Das Rollenmodell entsprechend eIDAS 2.0 Architecture Reference Framework (ARF) ermöglicht dezentrales Identitätsökosystem




*(Qualified) Trust Service Provider

https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/arf.md

# Was steht in der **eIDAS** hierzu?



Art 5b Abs. 1-11 eIDAS:

- Registrierung der vertrauenden Parteien („kosteneffizient und risikoangemessen“)
  - Öffentliche automatisierte, signierte Liste mit Mindestinhalt (Land der Niederlassung, Name der vertrauenden Partei und eindeutiger Kenner, sowie beabsichtigte)
  - Basierend auf dieser Liste Bereitstellung einer Identifizierungs- und Authentisierungslösung

- Verantwortlichkeit der vertrauenden Parteien; Pseudonyme dürfen nicht grds. abgelehnt werden
- Möglichkeit von Vermittlern/Sammelschnittstellen, dürfen keine Daten aus der Transaktion speichern
- Konkretisierung durch Durchführungsrechtsakt

➢ Ziel: Zugriff nur auf Daten, die die vertrauende Parteien benötigen bzw. verarbeiten dürfen.

# Was steht im **Durchführungsrechtsakt** hierzu? 1/2

**Entwurf** aus November 2024 (Kommentierung nicht mehr möglich):

- Genauere Anforderungen für öffentliche Registrierungspolicies (Vor allem: Welche Nachweise sind erforderlich und welche Pflichten hat die vertrauende Partei?)
- Genauere Anforderungen an den Registrierungsprozess
  - Registrierung innerhalb von 5 Werktagen
  - zu erfassende Daten (insbesondere auch Kontaktdaten und Daten zur beabsichtigten Nutzung und abzurufende Attribute, Festlegung der Identifier)
  - Überprüfung der Identität und Angaben **-> Konfliktpotential zur Vorgabe "kosteneffizient", da Doppelprüfung**)
  - Aufbewahrung 10 Jahre
- Nur rudimentäre Rollendefinition und keine Definition von Attributsgruppen

- ➢ Ziel: Zugriff nur auf Daten, die die vertrauende Parteien benötigen bzw. verarbeiten dürfen.
- ➢ Nur eine Registrierung notwendig. Aber wahrscheinlich mehrere Zugriffszertifikate

# Was steht im **Durchführungsrechtsakt** hierzu? 2/2

**Entwurf** aus November 2024 (Kommentierung nicht mehr möglich):

- Genauere Schnittstellenanforderung, insbesondere REST API, JSON unterstützend in OpenAPI V3
- Anbindung an die Wallet mittels Zugriffszertifikaten
  - Ausgestaltung national
  - Erstellung einer Zertifikatspolicy und CPS (Certificate Practice Statement)
  - Definition grundlegender Anforderungen an diese Zertifikate (X.509 Zertifikate mit CT-Logging (Certificate Transparency), Pflicht zum Aufbau einer Revozierungsliste)
  - Identifizierung der vertrauenden Partei und Überprüfung des Registers
  - Pflichten zum Widerruf der Zertifikate bei relevanten Umständen und Änderungen
- Außerdem **Möglichkeit** der Einführung von Registrierungszertifikaten

- ➢ Ziel: Zugriff nur auf Daten, die die vertrauende Parteien benötigen bzw. verarbeiten dürfen.
- ➢ Zugriff nur durch Zertifikate, nicht durch Schnittstellen (P): Interoperabilität

# Welche Möglichkeiten gibt es für Zugriffszertifikate?

## Nationale Ausgestaltung der Zugriffszertifikate

1

**Modifizierte Berechtigungszertifikate**

Weiterentwicklung und Verbesserung der eID-Berechtigungsgzertifikate bzw. Neuaufbau eines nationalen Zertifikatsschemas

2

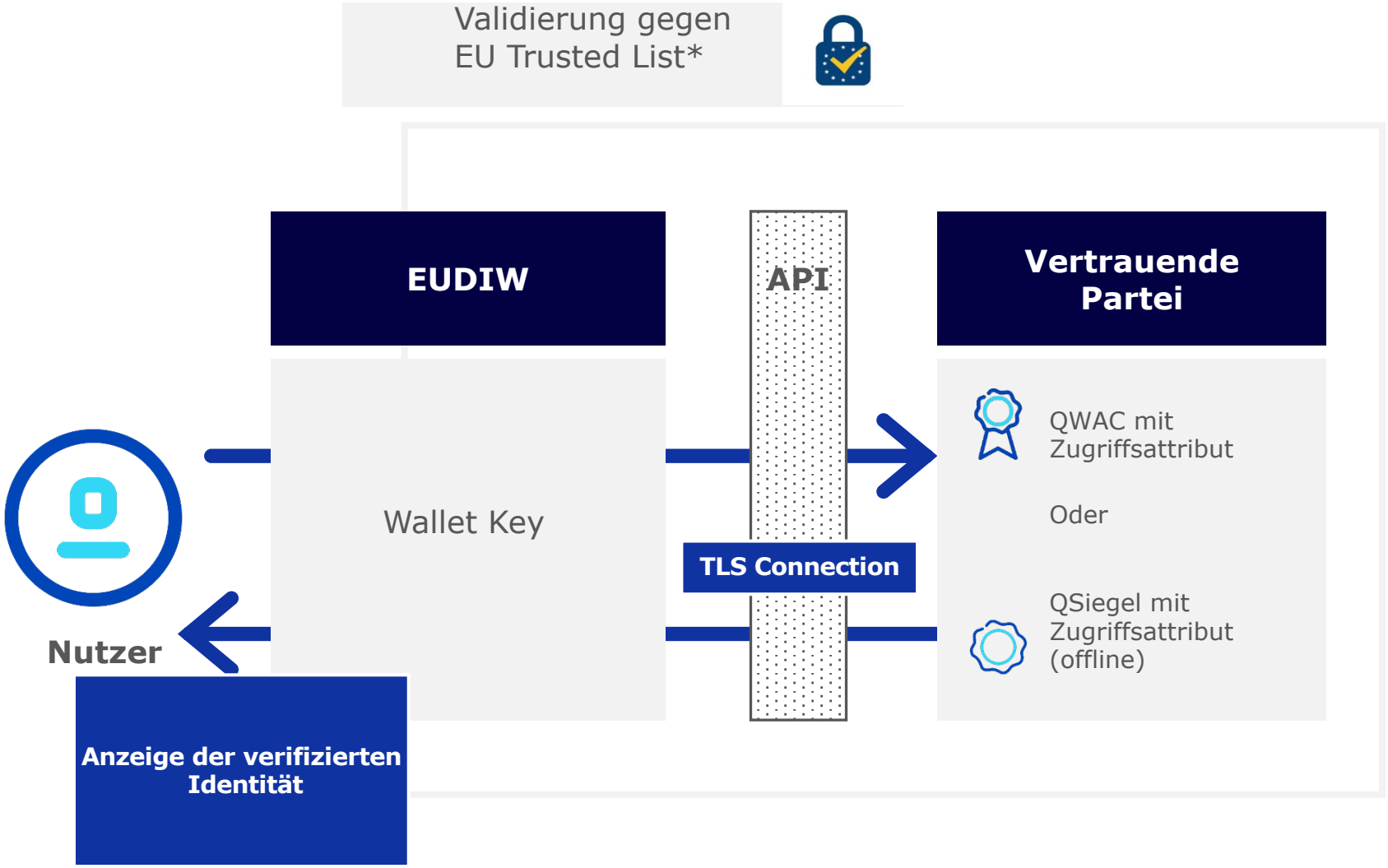
**PSD2 Lösung**

Nutzung etablierter eIDAS-Mittel (QWAC und QSiegel) mit verifizierter Identität und Zugriffsattributen

# PSD2 Modell für die EUDIW

## Vorteile:

- Interoperabilität
- Wenig Aufwand für Mitgliedsstaaten
- Bekannt und Bewährt
- CA bereits ausreichend vorhanden
- Hohe Verfügbarkeit und schnelle Antwortzeiten
- Einheitliche Validierbarkeit




*European Trust Service List according to Implementing Decision (EU) 2015/1505 (https://webgate.ec.europa.eu/tl-browser)

# Für die Anbindung von vertrauenden Parteien an die EUDIW sind noch folgende Dinge in Deutschland zu schaffen bis 18.12.2026:

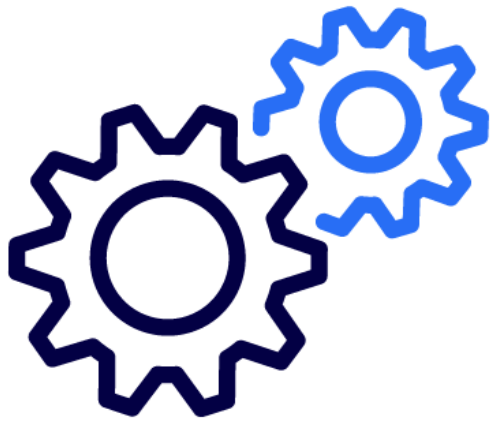
- Schaffung Registrierungsverfahren, Festlegung der zuständigen Stelle des Registrars, Erstellung Registrierungspolicy
- Schaffung der öffentlichen Registrierungsliste samt Schnittstellen
- Festlegung der Anforderungen an Zugriffszertifikate samt Zertifikatspolicy
- Ggf. Schaffung von Registrierungszertifikaten samt Zertifikatspolicy und Vermittlern

**Noch zu klären:**

- Wie wird die Interoperabilität der Zugriffszertifikate sichergestellt?
- Wie wird umgegangen, wenn einzelne Mitgliedsstaaten keine Registrierungszertifikate ausgeben?

# Wie sich Organisationen heute vorbereiten?

- Leichte Onboarding-Prozesse mit Personalausweis (eID)
- Relying Party Authentifizierung und Zertifikatsvertrauensinfrastruktur
- Interoperabilität, inbesondere bei Vertrauensmechanismen
- Anbindung Authentic Sources an QTSPs
- Digitale Organisationsidentitäten und Organisations-Wallets
- Zero-Knowledge-Proofs (ZKP) und Postquanten-Kryptographie (PQC)
- Gerätewechsel und Backup
- Wissensvermittlung und Aufklärung der Gesellschaft



# Wie sich Organisationen heute vorbereiten?

- Beteiligung am Konsultationsprozess
- Kommentierung der Implementing Acts
- Erprobung der Technologie
- Prototypisierung von auszugebenden Credentials und deren Schemata
- Prüfung von Prozessen und Workflows

# Vielen Dank.

**Paul Bastian(paul.bastian@bdr.de)**

**Andreas Wand (andreas.wand@d-trust.de)**