

German/US Expert Meeting

IT Security Association Germany (TeleTrust) in cooperation with FIDO Alliance

San Francisco, 08.05.2024

Trusted Identity: The new EUDI Wallet ecosystem

Dr. Kim Nguyen, SVP Innovations
Bundesdruckerei GmbH, Berlin, Germany

eIDAS 2.0 – Establishing a Framework for a European Digital Identity



eIDAS 1.0
2014

- Public
- Federated ID model
- Notification of member states eID schemes
- Population coverage in Europe:

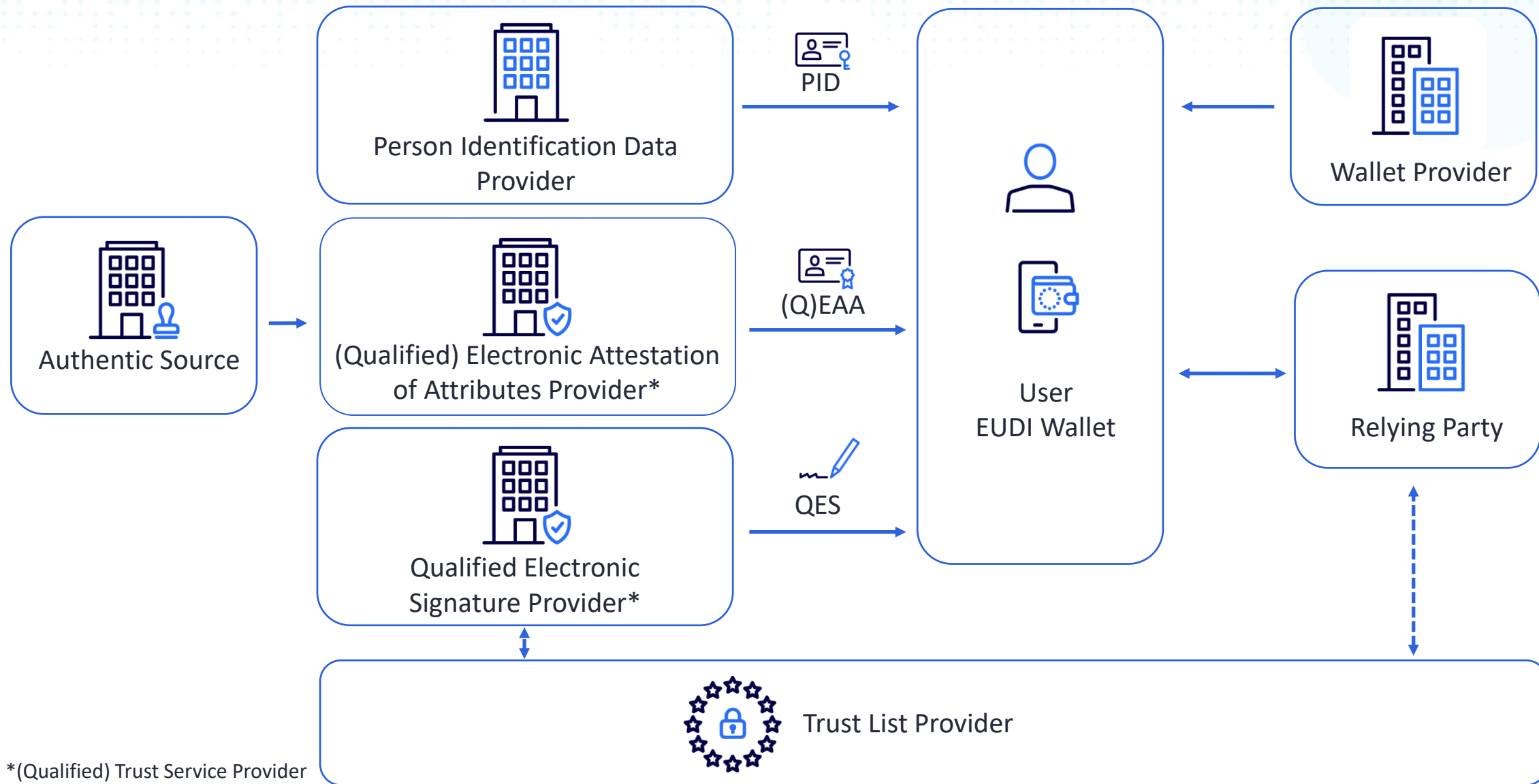
59%



eIDAS 2.0
2024

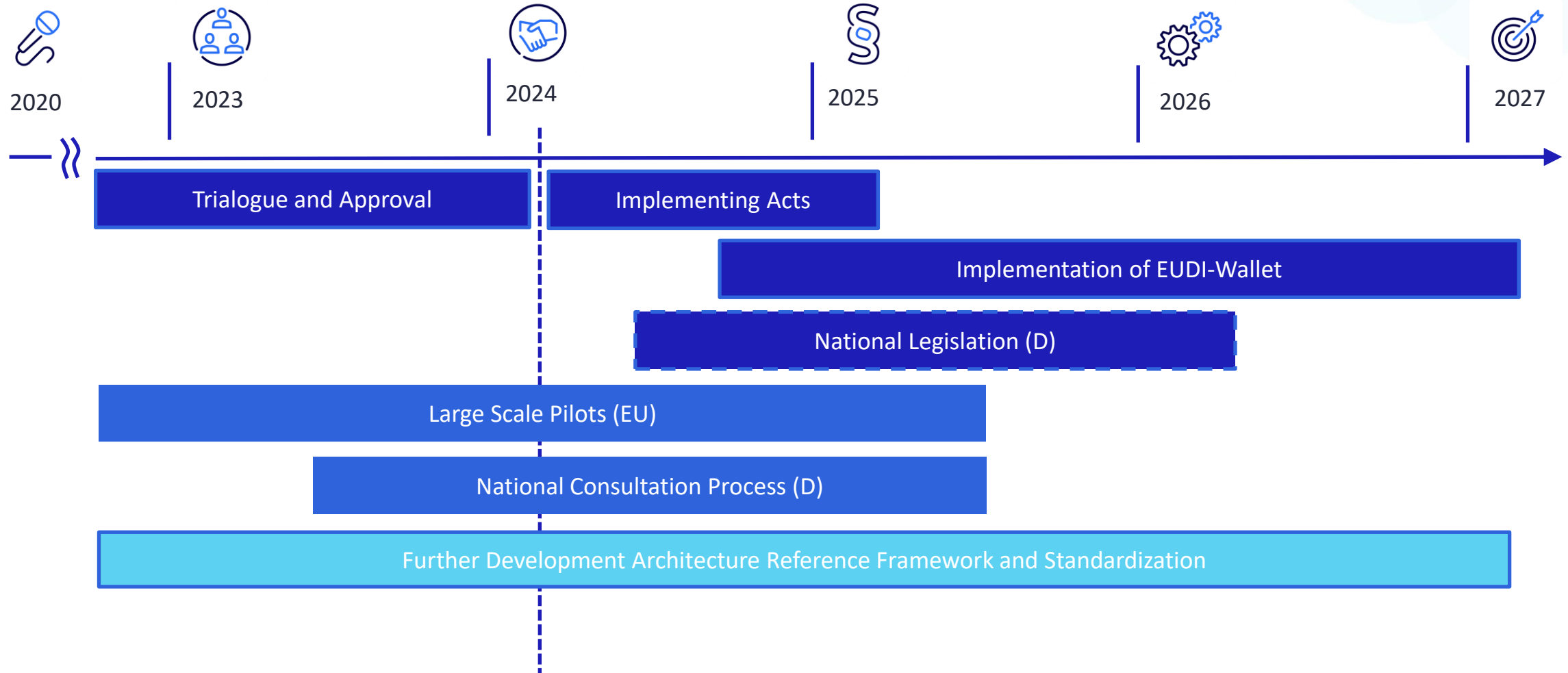
- Public and private sector
- Decentralized ID model
- Notification of eID/wallets
- Qualified electronic Attestation of Attributes
- Qualified electronic ledgers, Archiving
- Population coverage in Europe 2030:

> 80%



*(Qualified) Trust Service Provider

eIDAS 2.0 – Estimated Schedule



eIDAS 2.0 – German National Consultation Process



Involvement of the public, civil society and private organizations



Realization of extensive workshops on operating models and applications



Wallet Challenge with funded tracks to test designs and create open source code



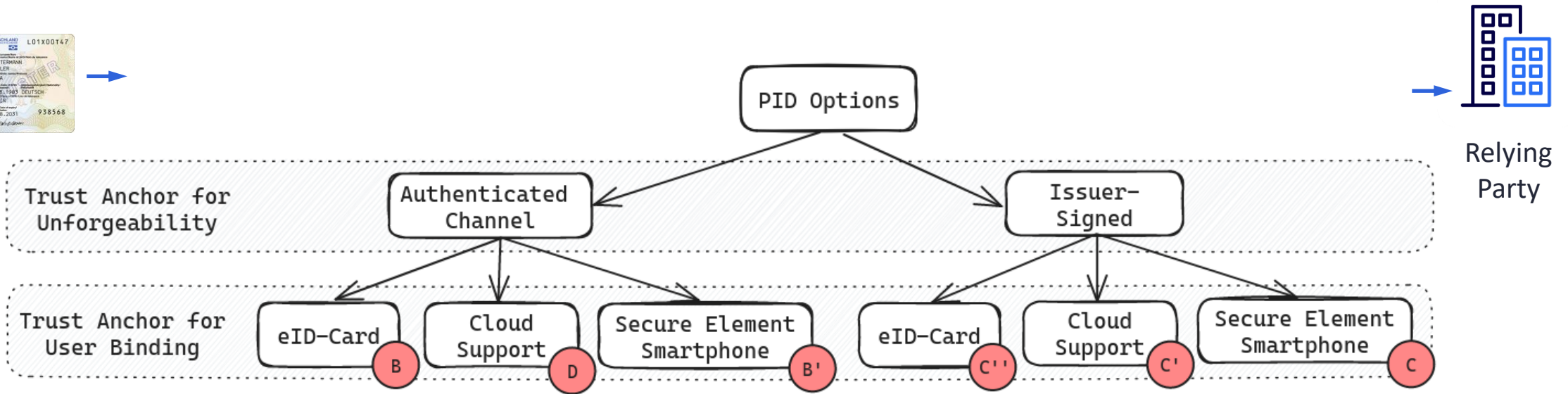
Continuous development and publication of the Wallet architectural concept

Transparent and participatory architecture and consultation process to provide a validated, interoperable, widely accepted and sustainably financeable concept for eIDAS implementation in Germany



Federal Ministry
of the Interior
and Community

Architecture options for PID Issuance based on the German eID System



Relying
Party

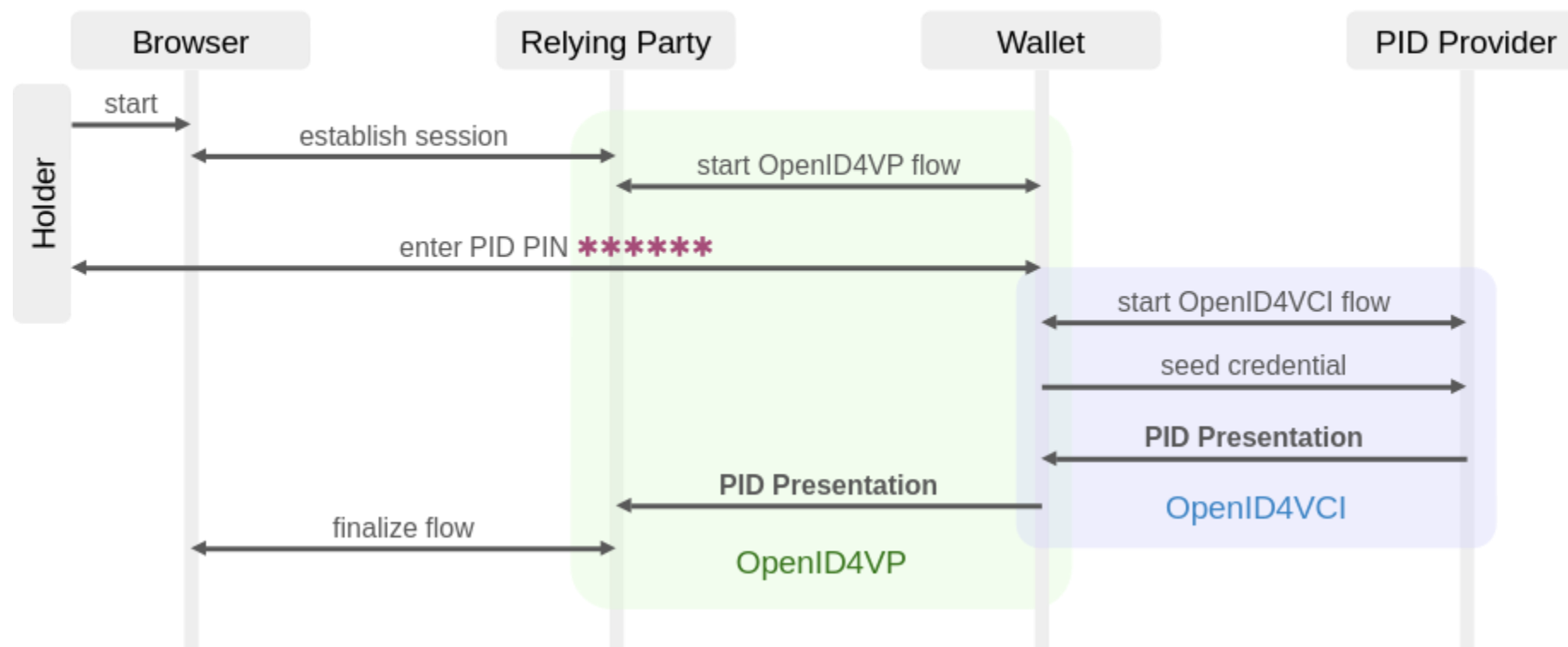
- exploration and evaluation of various options to realize the PID
 - different cryptographic designs
 - different wallet architectures

Wallet Security Cryptographic Device

- Wallet Security Cryptographic Device (WSCD) as the trust anchor in the Wallet
 - External (existing eID, Smartcards)
 - Internal (TEE, Secure Elements, eSIM, ...)
 - Cloud (HSM)
- choice of WSCD impacts the Wallet architecture

PID Presentation

B': PID Presentation



- The Architecture Reference Framework (ARF) gives guidance for technical direction
- Credential Formats support selective disclosure in a hash-and-saltbased approach
 - ISO mdoc for CBOR encoding
 - IETF SD-JWT for JSON encoding
- Exchange Protocols based on OAuth2
 - OpenID for Verifiable Credential Issuance
 - OpenID for Verifiable Presentations
- To be determined:
 - Trust Management
 - Relying Party Authentication and Authorization
 - Pseudonyms
 - Revocation

Important Issues to be clarified in detail

- User-friendly onboarding processes with eID Card
- Wallet Secure Cryptographic Device (WSCD) - cloud-based solutions
- Linking and combined presentation of PID and (Q)EAA
- Relying Party authentication and certificate trust infrastructure
- Digital identification means for legal entities - Legal person, legal corporate wallet