Bundesnetzagentur

EUDI-Wallet: Signatur und Governance

Konstantin Götze, Leiter Elektronische Vertrauensdienste

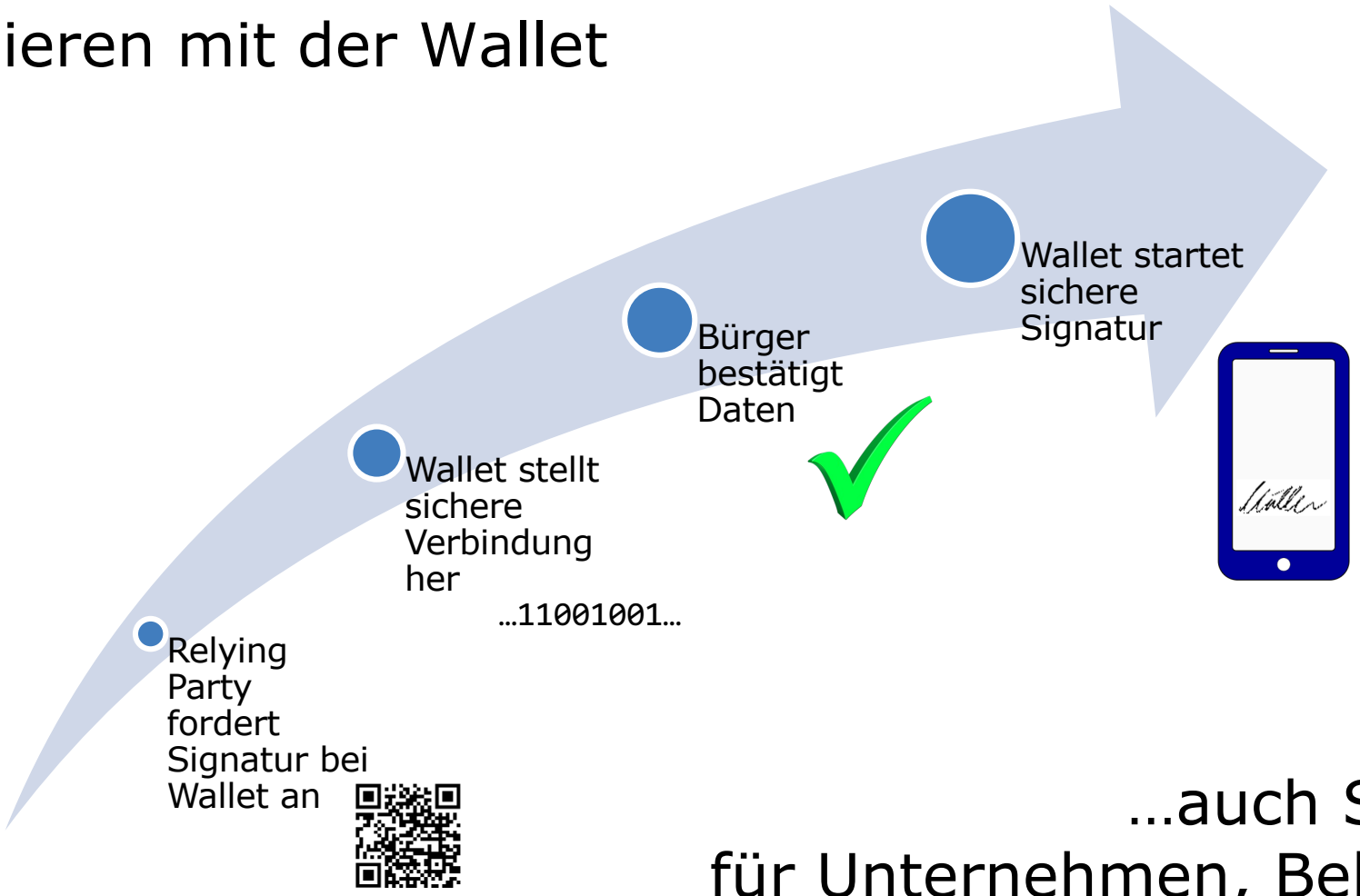
OMNISECURE 2023

Berlin, 22.05.2023

EUDI-Wallet: Signieren und Siegeln

EUDI-Wallet: Signieren und Siegeln

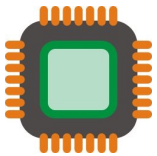
Signieren mit der Wallet



…auch Siegeln
für Unternehmen, Behörden

EUDI-Wallet: Signieren und Siegeln

Wo ist der Schlüsselspeicher?



im Smartphone
→ Sicherer Chip nötig (Secure Element)

am Smartphone
→ Signatur-/Siegelkarte anhalten (NFC)

beim Vertrauensdiensteanbieter
→ Vertrauenswürdige Anbindung

EUDI-Wallet: Signieren und Siegeln

Online/Offline use cases

- online/remote: Vertrauensdiensteanbieter erzeugt Signatur/Siegel, Wallet steuert
- offline/local: Wallet/Karte erzeugt Signatur/Siegel

Offene Frage:

- Falls Wallet Signatur/Siegel erzeugt
  → Zertifizierung als „QSCD“

EUDI-Wallet: Governance

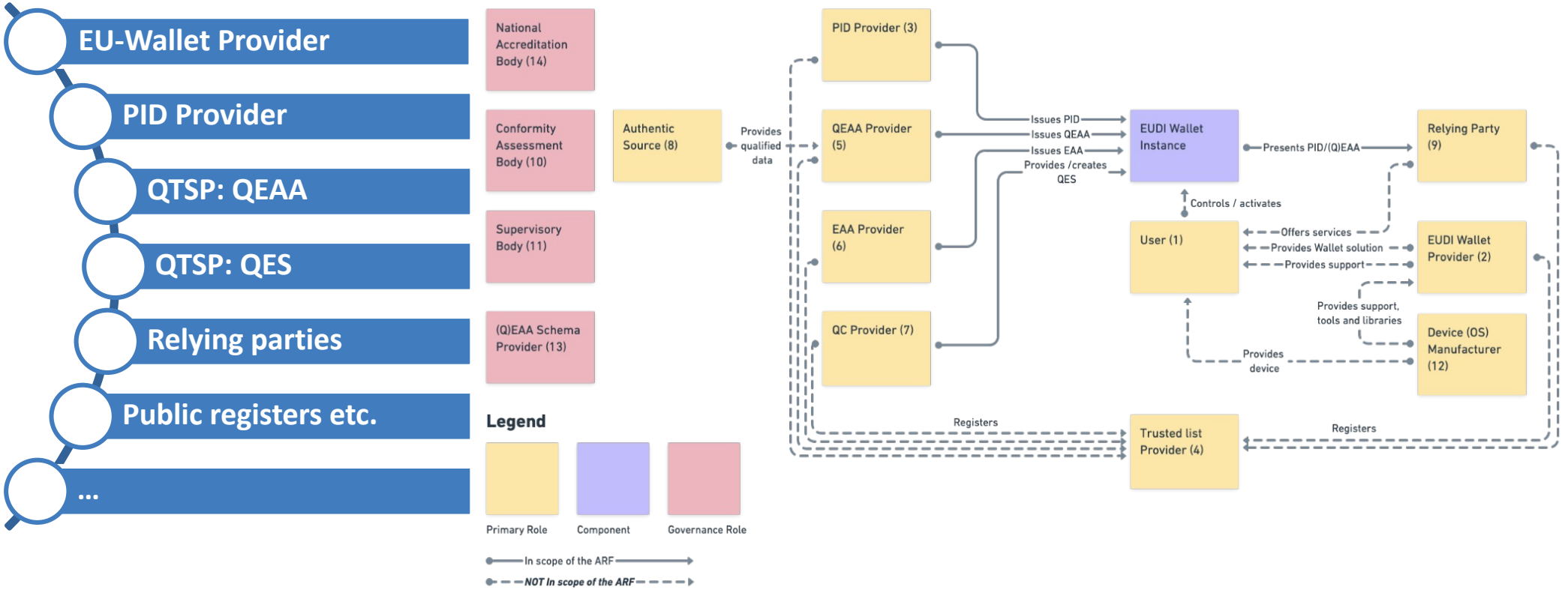
EUDI-Wallet: Governance

Governance: Bereitstellen einer verlässlichen Infrastruktur, verlässlicher Daten und datenschutzkonformer Nutzung

- Wallet als „Vertrauensraum" erfordert **Prüfung, Zulassung und Beaufsichtigung** der ganzen Wallet-Infrastruktur
- Eine Wallet verpflichtend, entweder vom **Staat** selbst, staatlich veranlasst oder staatlich zugelassen
- Wallet für natürliche und juristische Personen **zulassen und beaufsichtigen**
- **Zulassungsverfahren** basierend auf Konformitätsbewertung und Zertifizierung (Prüfung)
- Aufsicht bei Schadfällen mit der Möglichkeit der **Sperrung** einer ganzen Wallet-Infrastruktur

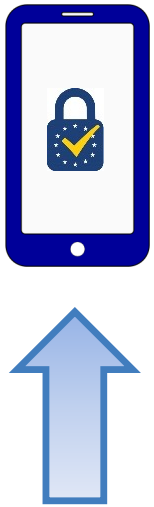
EUDI-Wallet: Governance

Vertrauensinfrastruktur: Rollen im Ökosystem



EUDI-Wallet: Governance

Upstream



Befüllen des Vertrauensraums Wallet mit verlässlichen Daten

Prüfbare Verlässlichkeit: Sicheres „Onboarding“ und sichere Quellen (z.B. staatliche Register)

Werden einzelne Wallets kompromittiert, zusätzlich Möglichkeit der Sperrung einzelner Wallets

EUDI-Wallet: Governance

Downstream

Datenschutz bei Bereitstellung von Daten aus der Wallet

Kontrolle des Nutzers über Herausgabe seiner Daten (Souveränität)

Wer fragt die Daten an?
→ Registrierung/Authentisierung von Relying Parties, Aufbewahren von Anmeldedaten von Relying Parties, Registrierung automatisiert, ggf. mit Nutzung vorhandener Register

Welche Daten werden abgefragt?
→ Einordnung abgefragter Daten in sensibel und nicht sensibel (special categories/high risk)

Auswahl abgefragter Daten
selective disclosure, Beschwerdemechanismus bei „*disproportionate amount of data*"

Bundesnetzagentur

Fragen gerne jederzeit an

eIDAS@BNetzA.de

Bundesnetzagentur

Konstantin Götze
Leiter Elektronische Vertrauensdienste

06131 18 3849
eIDAS@BNetzA.de