Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

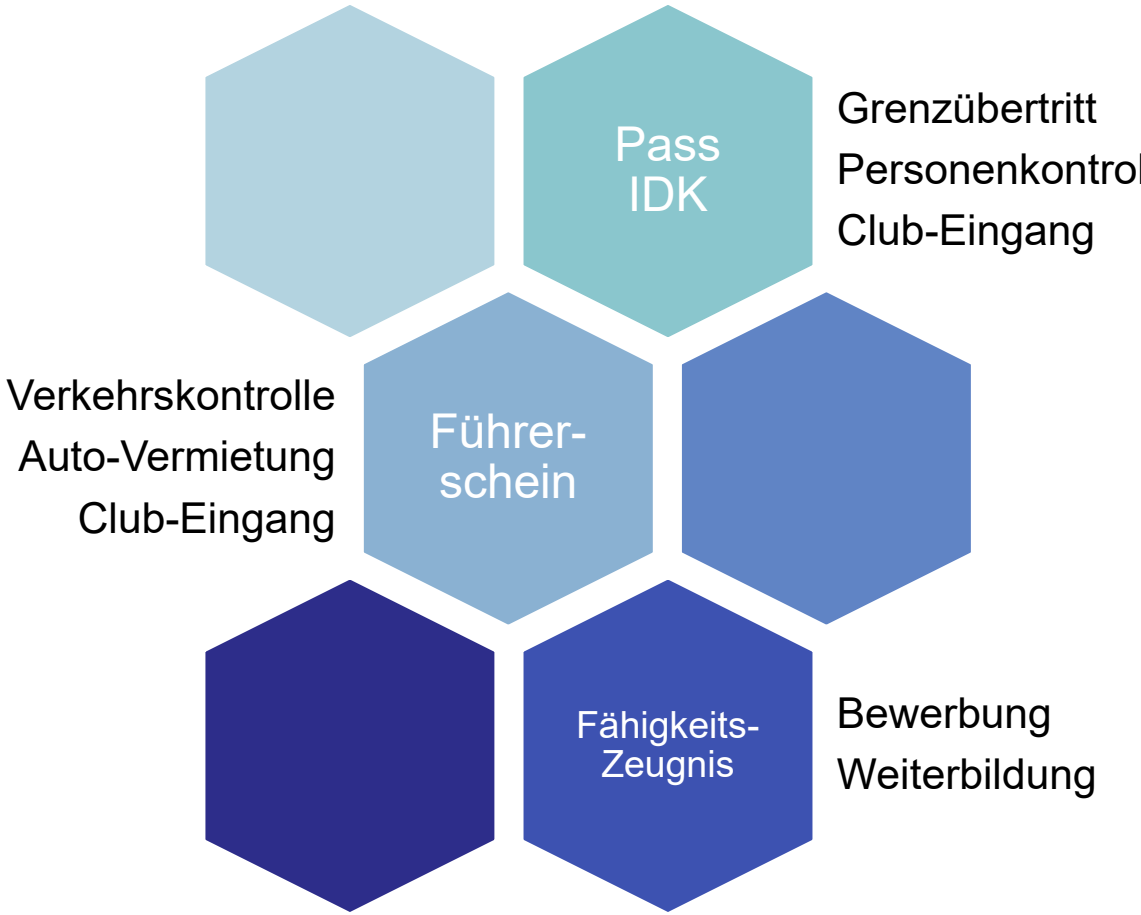
Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Justiz BJ

SSI for Dummies

Möglichkeiten von Self-Sovereign Identity für eine staatliche E-ID

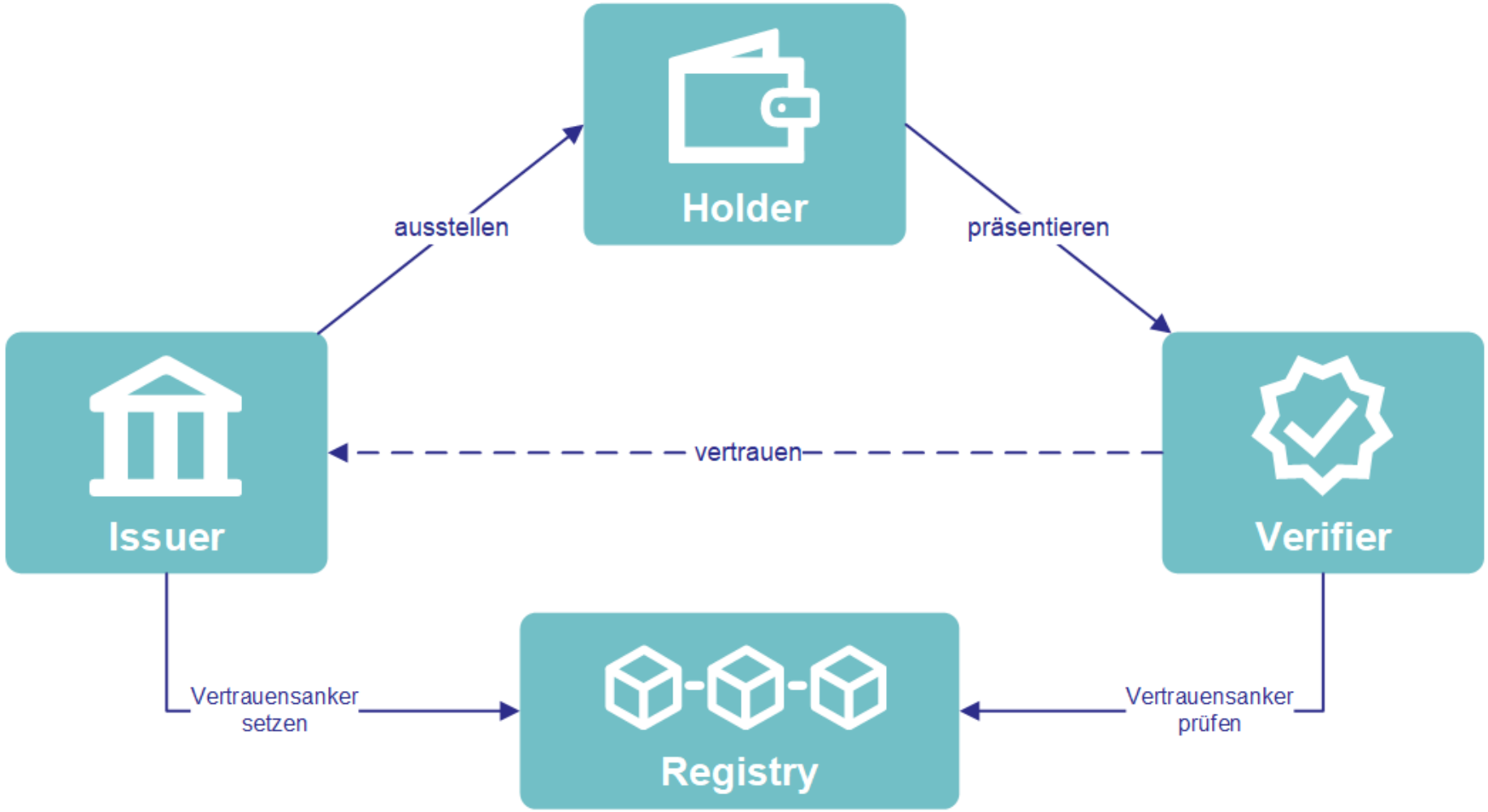
28. März 2022

Beweisdokumente, Bescheinigungen, Belege

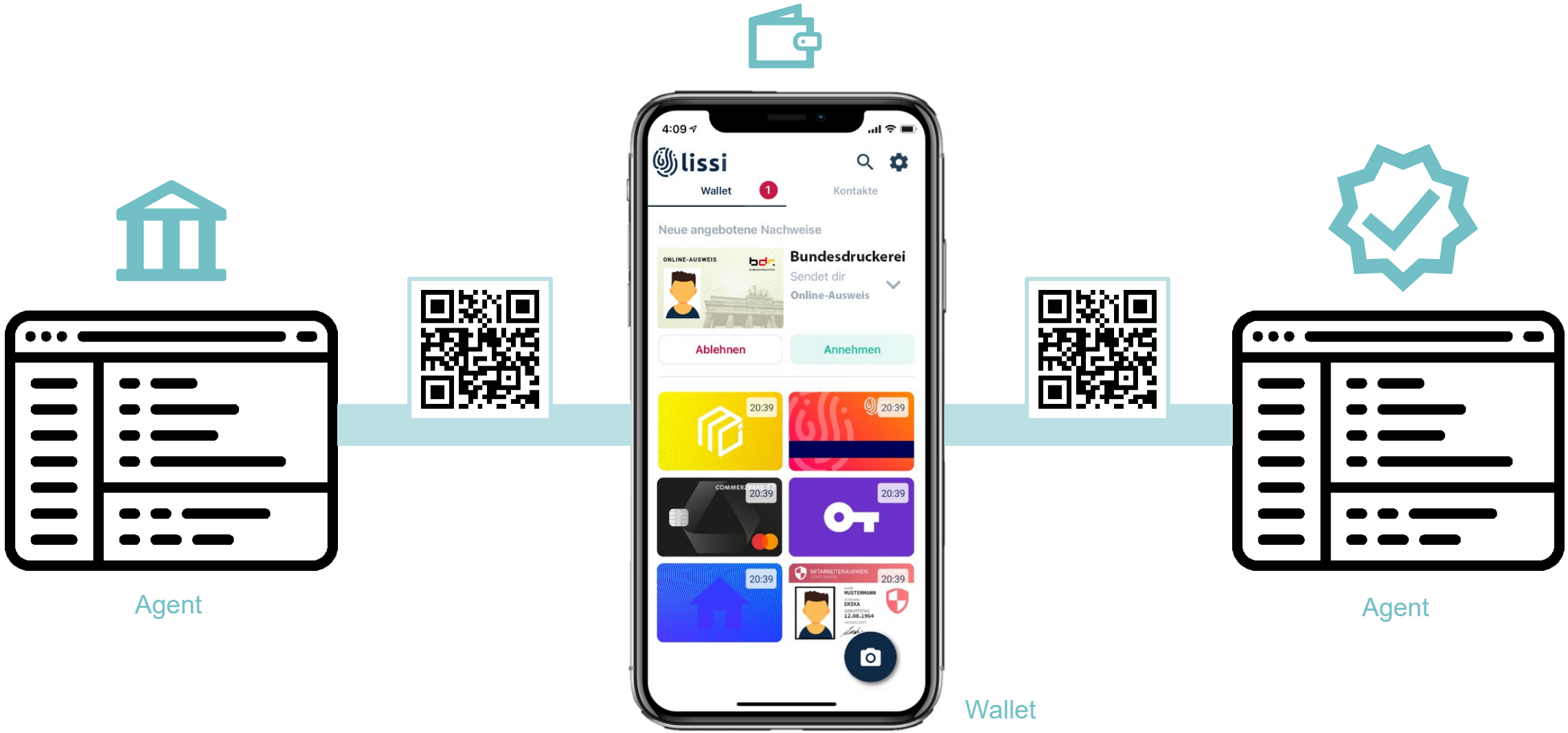


Verified Credentials

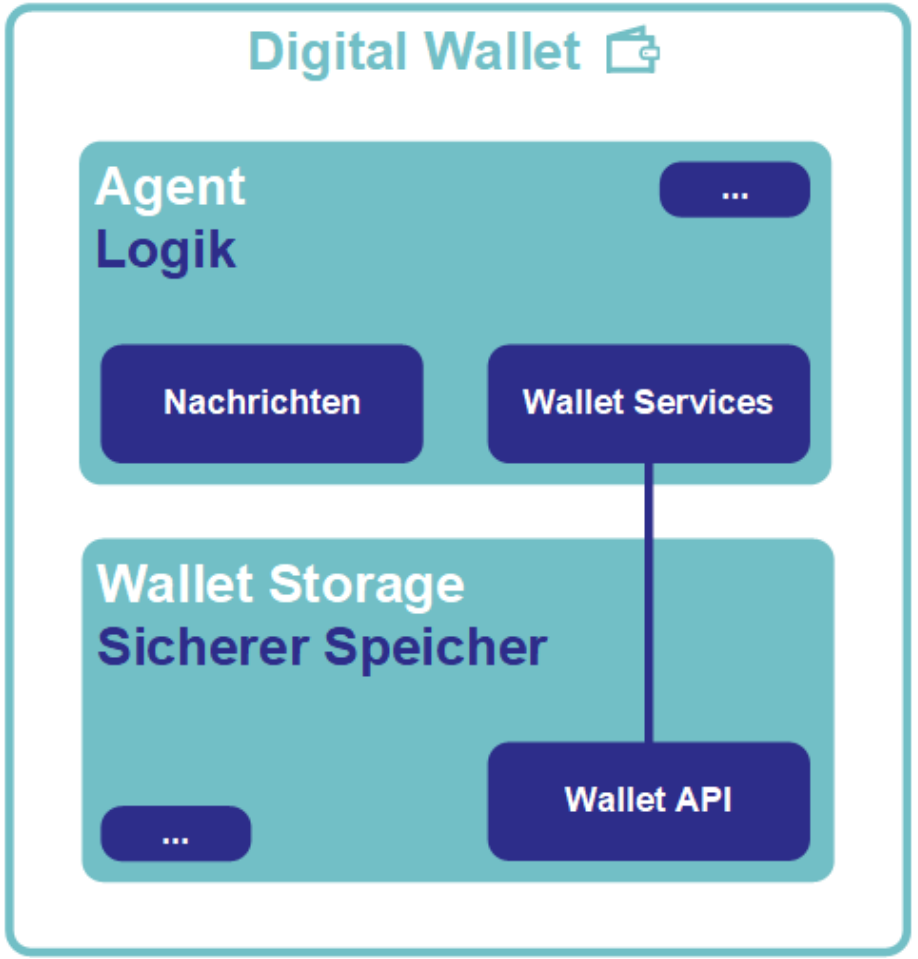
Self-Sovereign Identity Grundkonzept



Self-Sovereign Identity Anwendung



Wallets und Agents



- ***Wallet: Haupt-Element für die Benutzerinnen und Benutzer***
- ***Agent-Teil*** dient zur Benutzerführung und Funktionalität, z.B. Übermittlung, Backup, Aktualisierung Credentials
- ***Sicherer Speicher*** sorgt für die sichere Ablage von privaten kryptografischen Schlüsseln und Verifiable Credentials
- ***Agents der Issuer und Verifier sind ähnlich***
- ***Nachrichten senden: Peer-to-Peer***
  Vergleich zu E-Mail (Openness) und Threema (End-to-End)

Use-Cases – alle erdenklichen










Vorteile des SSI-Ansatzes

Nahe an der physischen Realität

- Verständlich für alle, verringert Komplexität von Systemen, E-Mail-Like Anwendung
- Authentisierung und Autorisierung ohne dogmatische Trennung

Infrastruktur-Gedanke

- Erschaffung Grundlage für viele Anwendungen
- Folgt dem API-Gedanken für Serviceanbieterinnen (Issuer und Verifier)
- Es ist kein Login
- Europäische Stossrichtung

Huhn-Ei-Problem lösbar

- Einzug in den Alltag, stets gleicher Ablauf
- Ökosystem entstehen lassen: Viele Anwendungen für E-Government und Privatwirtschaft dank gemeinsamer «Plattform»

Nachteile und Herausforderungen des SSI-Ansatzes

Maturität und Standardisierung

- Basis-Frameworks sind noch endgültig stabilisiert
- Standards in Entwicklung, Durchsetzung der «Besten» steht noch aus

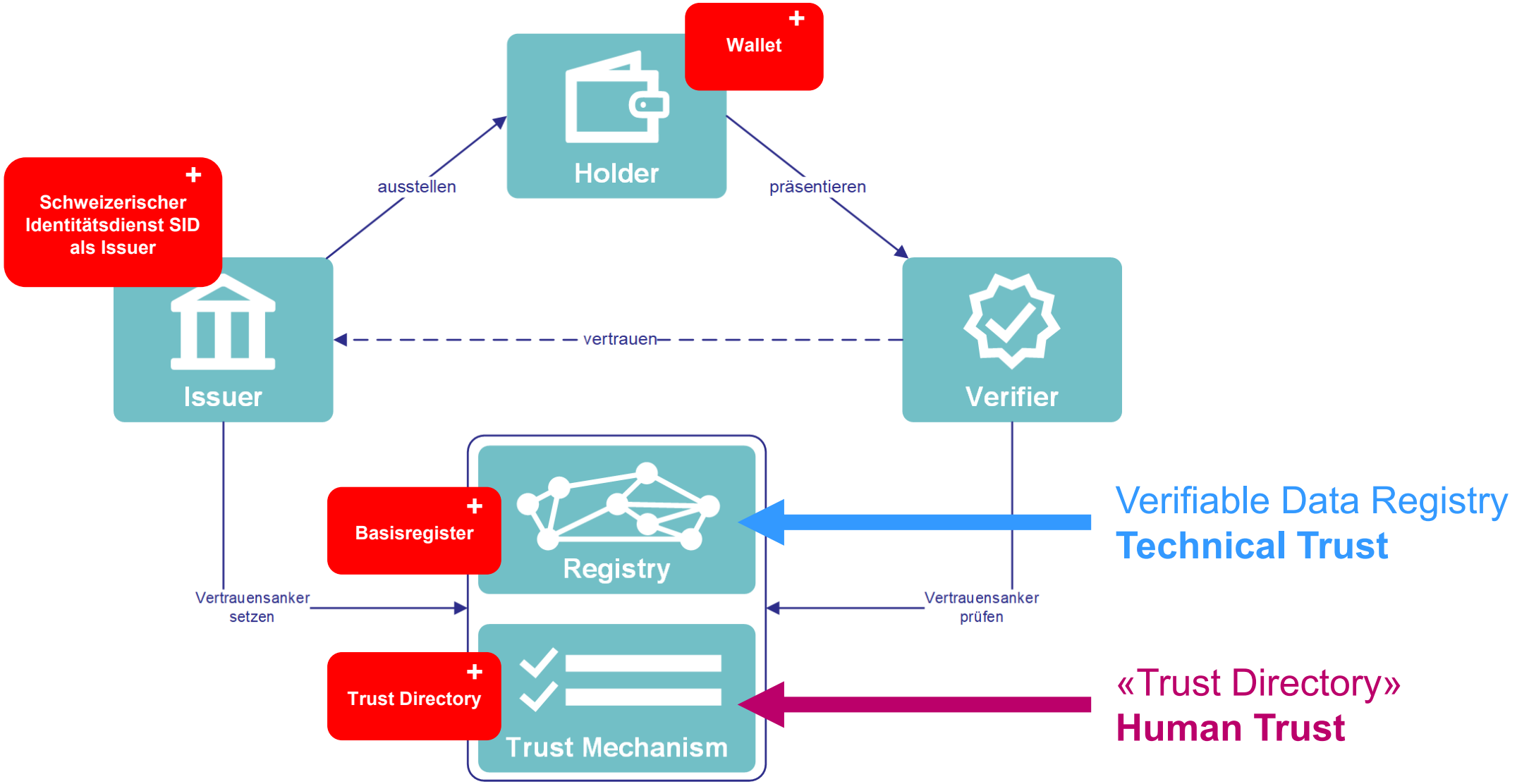
Hohe Eigenverantwortung bei Nutzerinnen und Nutzern

- Digitale Mündigkeit fördern!
- Sehr benutzerfreundliche und sichere Soft/Hardware benötigt: Wallet und Agents

Paradigmenwechsel schaffen

- SSI ist für viele Neuland, Leute müssen abgeholt werden
- «Fixierung auf E-ID» lösen – «Ökosystem digitaler Nachweise» denken

Staatliche digitale Vertrauensinfrastruktur



Basisregister und Bestätigungsmechanismus

- Inhalt des **Basisregisters** ist kryptografisch abgesichert
  (Verifiable Data Registry for Technical Trust)
  - Identifikatoren von Ausstellerinnen und Verifikatorinnen
  - Öffentliche Schlüssel von Ausstellerinnen und Verifikatorinnen
  - Informationen zu Revokationen von Verifiable Credentials
  - Technisch notwendig, 1 Plattform würde genügen

- **Bestätigungsmechanismus** ist durch eine Autorität sichergestellt
  (Trust Mechanism for Human Trust)
  - Überprüft und bestätigt die Zugehörigkeit der Identifikatoren an eine bestimmte Ausstellerin und Verifikatorin
  - Beliebige Autoritäten können eigene «Trust Directories» betreiben und damit beliebige Ausstellerinnen und Verifikatorinnen bestätigen