A-SIT

Stand EUDI Wallet und Large Scale Pilot

Arne Tauber, Herbert Leitold

Inhalte

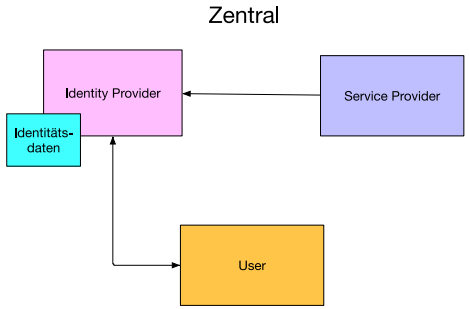
- Grundlagen Situation in Österreich
- Toolbox-Prozess und Architektur-Referenzrahmen
- Large Scale Pilot POTENTIAL
- Zusammenfassung

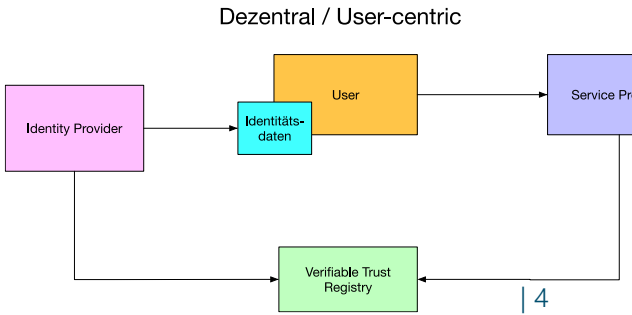
Hintergrund Ausweisplattform

- ID Austria (Online eID) bedeutet…
  - Identitätsdaten zentral bei Identitätsprovider (Behörde), jedes mal neu bestätigt
- Physischer Ausweis bedeutet…
  - Ausweis(-daten) an User ausgehändigt
  - Grundsätzlich dezentral, keine Beobachtbarkeit

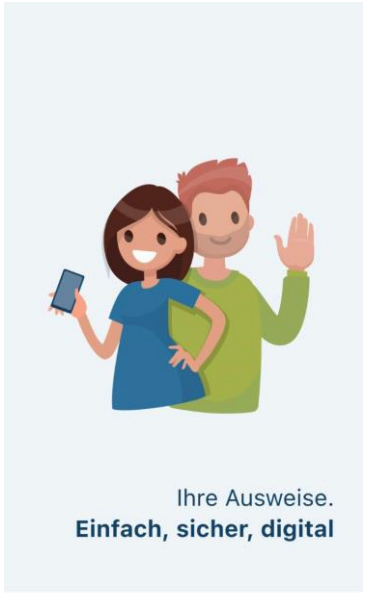
Dezentrale Identität

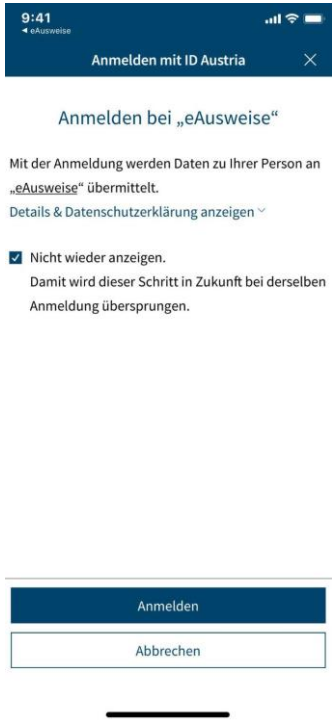
- Entkoppelung von Identity Provider und Service Provider/Prüfer
  - User als Intermediär (wie bei physischem Ausweis)
  - User-zentriert
    - Identitätsdaten/Attribute beim User
- Herausforderungen
  - Selective Disclosure / ZKP
  - Widerruf (Technisch / Fachlich)



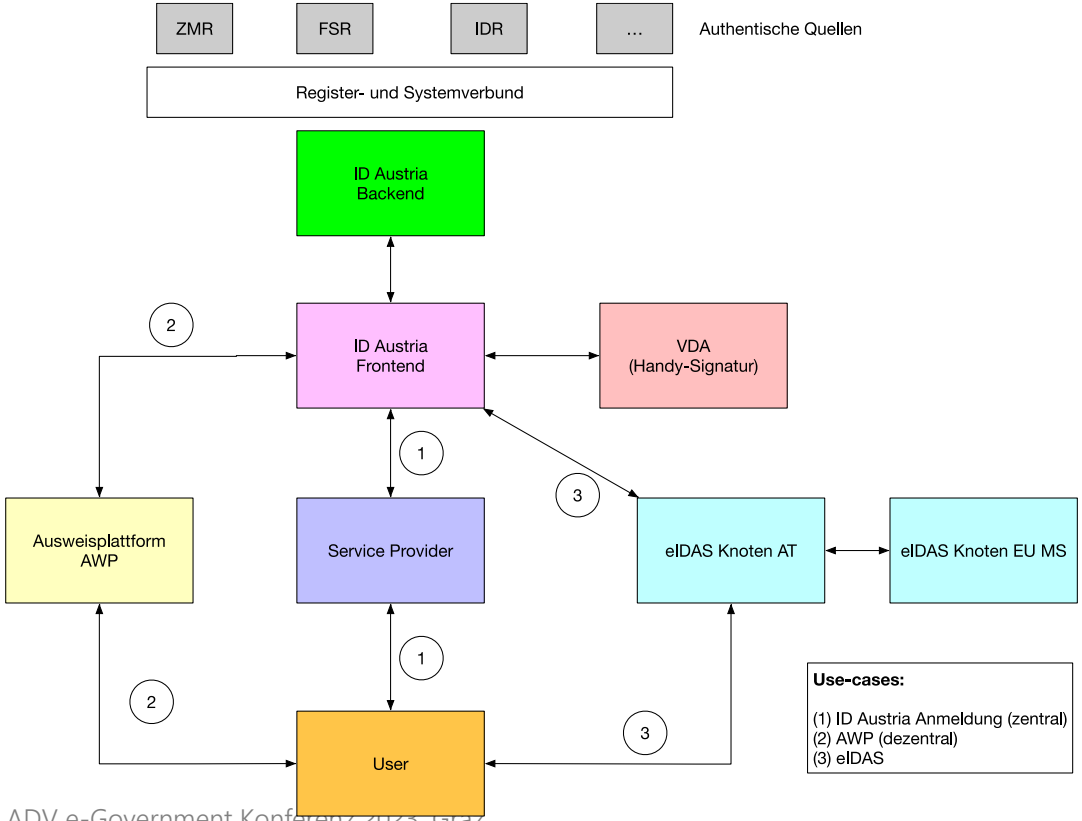


eAusweise App





Gesamtarchitektur eID in Österreich



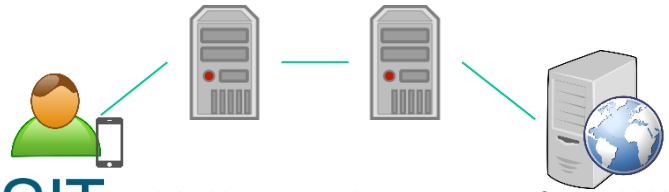
Inhalte

- Grundlagen Situation in Österreich
- **Toolbox-Prozess und Architektur-Referenzrahmen**
- Large Scale Pilot POTENTIAL
- Zusammenfassung

Zeitlinie eIDAS Revision bisher

Unterschiede eIDAS alt und neu

- eIDAS bisher (bzw. weiterhin)
  - nationale Knoten (eIDAS Nodes) entkoppeln MS-Situation
  - sowohl Relying Party-seitig als auch eID-seitig
  - Attribute als Teil des SAML-AuthN Requests aus Quell-MS-Infrastr.



- EUDI Wallet (neu)
  - Schnittstelle Wallet ⇔ Anwendung
    - MS-Umsetzung kann aus Wallet auch synchron abfragen, zB bPK berechnen
  - Attribute entweder
    - Person Identification Data
    - EAA im Wallet oder in „Cloud“
  - Attribute über qualifizierten VDA oder aus authentischer Quelle

Eckpunkte aus ARF v1.0 und ff.

- Formfaktor mobil (aktueller Fokus), aber auch weitere
- Bei Smartphone aus Vorgabe „LoA hoch“ samt Zertifizierung
  - eigenständig mit SE/TEE (wenn gegen hohes Angriffspotential sicher)
  - zusätzliche externe Vertrauensanker (smartcard über NFC)
  - unterstützt über Backend-Systeme (vgl. ID Austria aus LoA hoch)

v.a. im 1. Bullet abzuwarten, ob/was Markt aufzugreifen bereit ist

Im ARF festgelegte Protokolle

- Definiert vier User Flows
  - Remote cross-device und same-device
  - Proximity supervised und unsupervised (beide offline oder online)
- Remote flows über OpenID4VP
  - OpenID SIOPv2 für pseudonyme Authentifizierung
- Proximity flows über ISO/IEC 18013-5:2021
- PID muss sowohl als ISO/IEC 18013-5 als auch W3C VC folgen
- (Q)EAA entweder ISO/IEC 18013-5 oder W3C VC

Wallet Configurations

- Vorerst zwei „Configurations“
  - Type 1: PID LoA hoch (oder QEAA)
  - Type 2: (Q)EAA Präsentation
- Hintergrund ist, Profile zu definieren, sofern Vorgaben nicht zu allen Sektoren passen

Component	Requirement	Type 1	Type 2
Cryptographic keys management system - 1	EUDI Wallet Solution [...] rely on one of the following components to store and manage cryptographic keys: • Embedded Secure Element or Trusted Execution Environment (for mobile devices), • reliance on an external device (Secure Elements / Smart Cards), and • a backend (remote Hardware Security Module).	MUST	SHOULD
Attestation exchange Protocol - 2	The EUDI Wallet Solution [...] support the protocol detailed in the standard ISO/IEC 18013-5:2021 for **proximity flows**.	MUST	MAY
Attestation exchange Protocol - 3	The EUDI Wallet Solution [...] perform checks to enforce session binding (i.e., attribute request for PID).	SHOULD	MAY
Attestation exchange	EUDI Wallet Solution [...] support	MAY	MAY

Inhalte

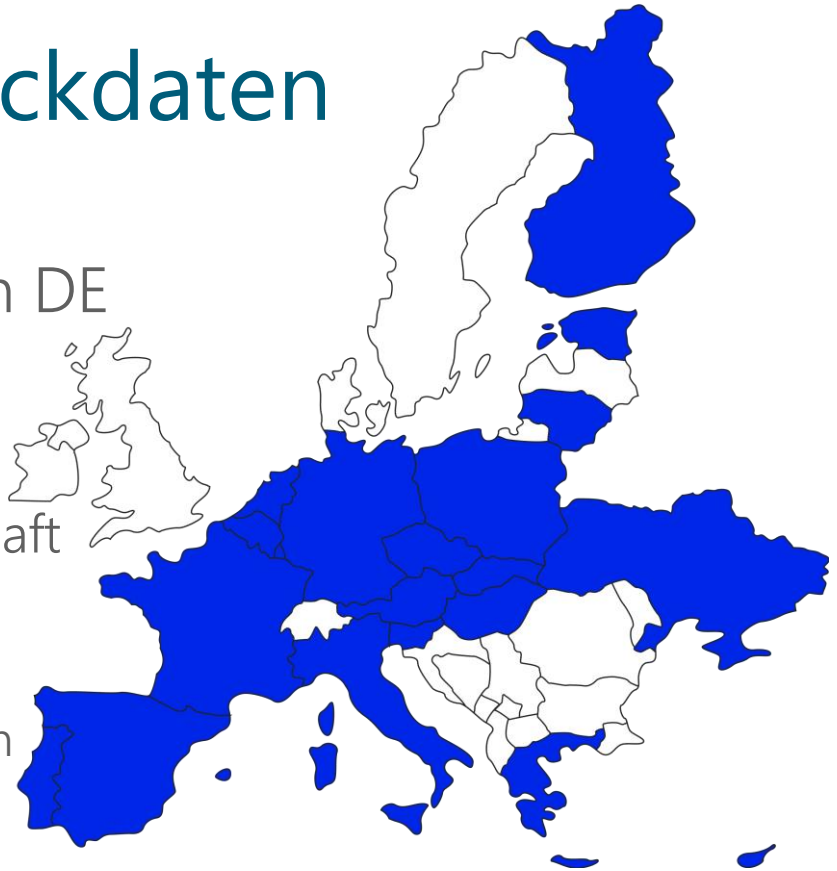
- Grundlagen Situation in Österreich
- Toolbox-Prozess und Architektur-Referenzrahmen
- **Large Scale Pilot POTENTIAL**
- Zusammenfassung

Hintergrund

- EK fördert seit einiger Zeit Large Scale Pilots in wesentlichen Politikbereichen
- Ebenso zum EUDI Wallet
  - 4 LSPs werden gefördert:
    - DC4EU https://dc4eu.eu/
    - EWC https://eudiwalletconsortium.org/
    - NOBID https://www.nobidconsortium.com/
    - POTENTIAL (Folgefolien) https://www.digital-identity-wallet.eu/

POTENTIAL Eckdaten

- Gesamtkoordination FR, technisch DE
  - 19 MS plus Ukraine
  - ca. 140 Organisationen
  - In Österreich über Arbeitsgemeinschaft mit 13 Partnern
    - Zu Wallet BMF federführend
    - Zu Use Cases entsprechend Sektoren
- Start 1. April 2023, Dauer 26 Monate



Technische Inhalte

- Umsetzung ARF und Integration in 6 Use Cases
  - In Ö. verantw. Ressort oder Aufsicht regulatorischer Lead
  1. Identifikation im E-Government (BMF, A-SIT, TUG-EGIZ)
  2. Kontoeröffnung (OeNB, OenPAY, Bitpanda, Erste, Hypo Vbg., RLBOOe)
  3. Digitaler Führerschein (BMF, A-SIT, TUG)
  4. SIM Registrierung (RTR, Magenta, Spusu)
  5. Qualifizierte Signatur (A-SIT, RTR, TUG)
  6. eMedikation (BMGSPK, A-SIT, TUG)

Inhalte

- Grundlagen Situation in Österreich
- Toolbox-Prozess und Architektur-Referenzrahmen
- Large Scale Pilot POTENTIAL
- **Zusammenfassung**

Zusammenfassung

- eIDAS Revision gibt eine Reihe von Neuerungen
  - Vor allen EUDI Wallet als Schritt in mobile Welt
- Technische Vorarbeit parallel zur Gesetzgebung
  - Toolbox und ARF
  - Referenzumsetzung als Angebot an MS
  - Large Scale Pilots zu Aufbau und Erprobung
- Österreich nimmt aktiv und gestaltend teil

Quellen eIDAS Revision

- Zeitlinie mit Links zu Institutionen bzw. Stellungnahmen
  - https://eur-lex.europa.eu/procedure/EN/2021_136
- Urspr. EK Vorschlag
  - eIDAS: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0281
  - Toolbox https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021H0946
- Allgemeine Ausrichtung Rat
  - https://data.consilium.europa.eu/doc/document/ST-15706-2022-INIT/de/pdf
- Europäisches Parlament
  - https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2021/0136(COD)&l=en
    - Weiter zu „Document Gateway" v,a, Committee Report 7/11/2022 bzw. jener 1st reading
- Architekturreferenzrahmen „ARF"
  - Outline: https://futurium.ec.europa.eu/en/digital-identity/toolbox (Registrierung Futurium notwendig)
  - ARF v1: https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework

a-sit.at/

Herbert.Leitold@a-sit.at