A-SIT

EUDI Wallet Status und Pläne

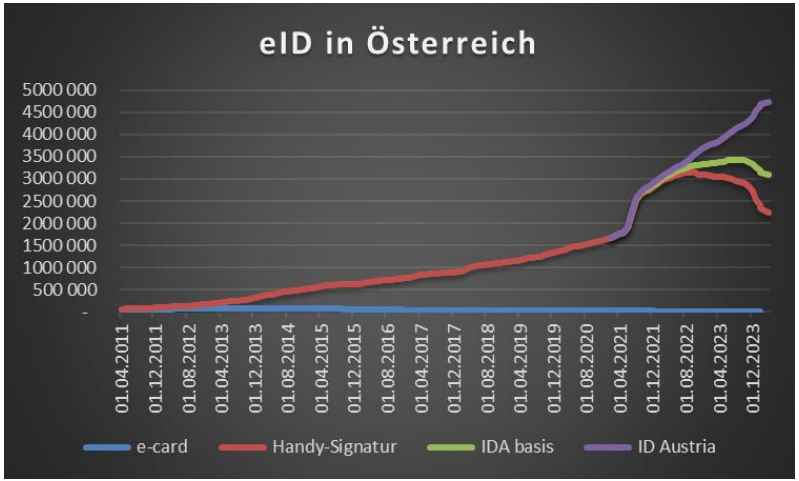
Herbert Leitold

Inhalte

- eID in Österreich
- Toolbox-Prozess und Architektur-Referenzrahmen
- Large Scale Pilot POTENTIAL
- Zusammenfassung und Umsetzungspläne

Situation eID in Österreich

- Seit 2005 für Online-Verfahren mit
  - sektor-spezifischer Identifikation (bPK)
  - qualifizierter elektronischer Signatur
  - elektronischer Vertretung
- Technologie-neutral
  - Nur mobil wirklich erfolgreich
- Seit 2022 auf LoA hoch notifiziert
- Seit 2022 mit „Ausweisplattform“ auch Präsenz-Situation
  - 600 k digitale Führerscheine, 400 k Zulassungsscheine, 250 k Altersnachweise
  - Identitätsnachweis seit Mitte Juni

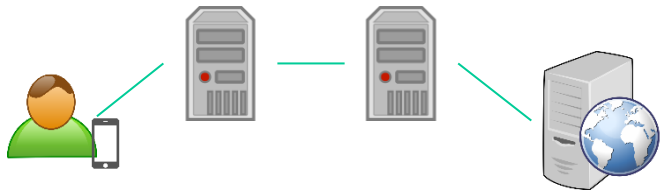


Inhalte

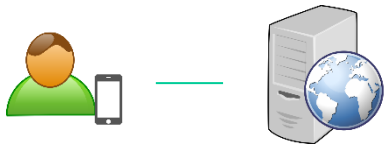
- eID in Österreich
- **Toolbox-Prozess und Architektur-Referenzrahmen**
- Large Scale Pilot POTENTIAL
- Zusammenfassung und Umsetzungspläne

Wesentlicher technischer Unterschied

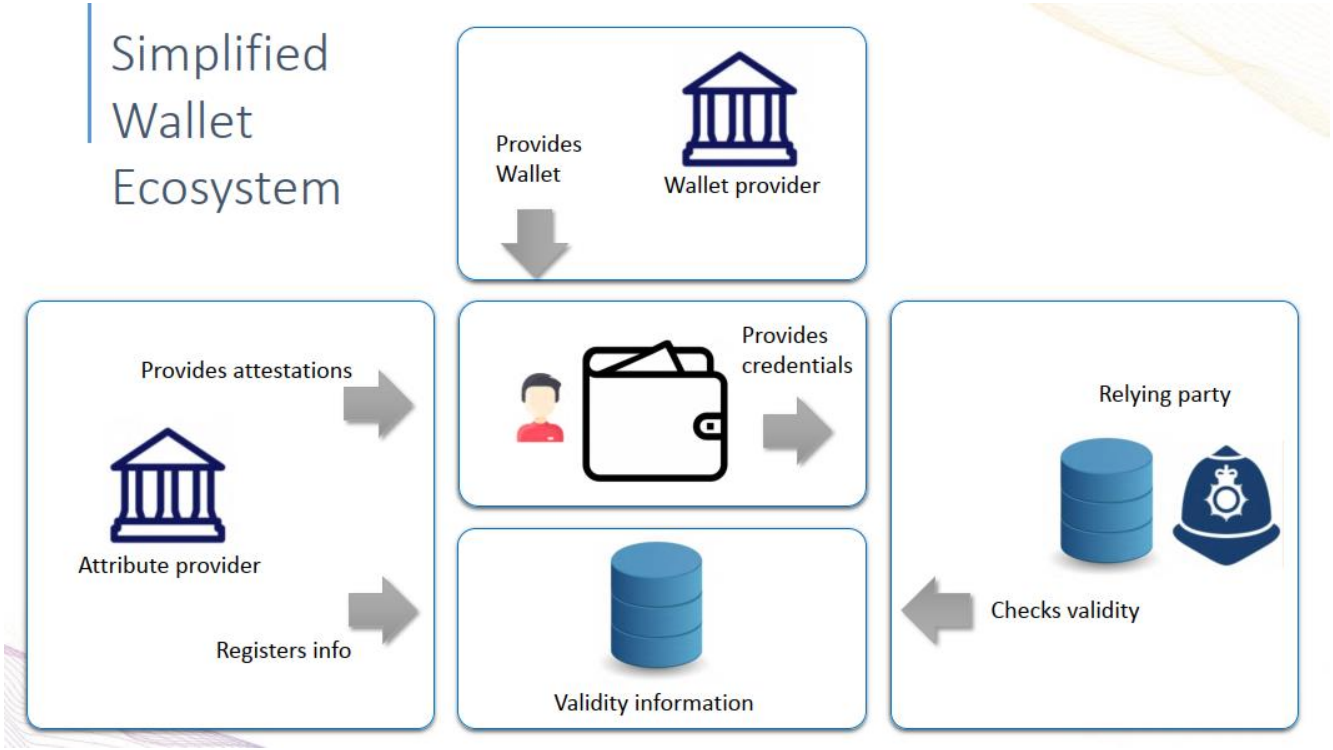
- eIDAS bisher (bzw. weiterhin)
  - nationale Knoten (eIDAS Nodes) entkoppeln MS-Situation
  - sowohl Relying Party-seitig als auch eID-seitig
  - Attribute als Teil des SAML-AuthN Requests aus Quell-MS-Infrastr.



- EUDI Wallet (neu)
  - Schnittstelle Wallet ⇔ Anwendung
    - Jedoch Identity Matching durch MS
  - Attribute entweder
    - Person Identification Data
    - EAA im Wallet oder in „Cloud“
  - Attribute über qualifizierten VDA oder aus authentischer Quelle



Ursprüngliche High-Level Sicht der EK



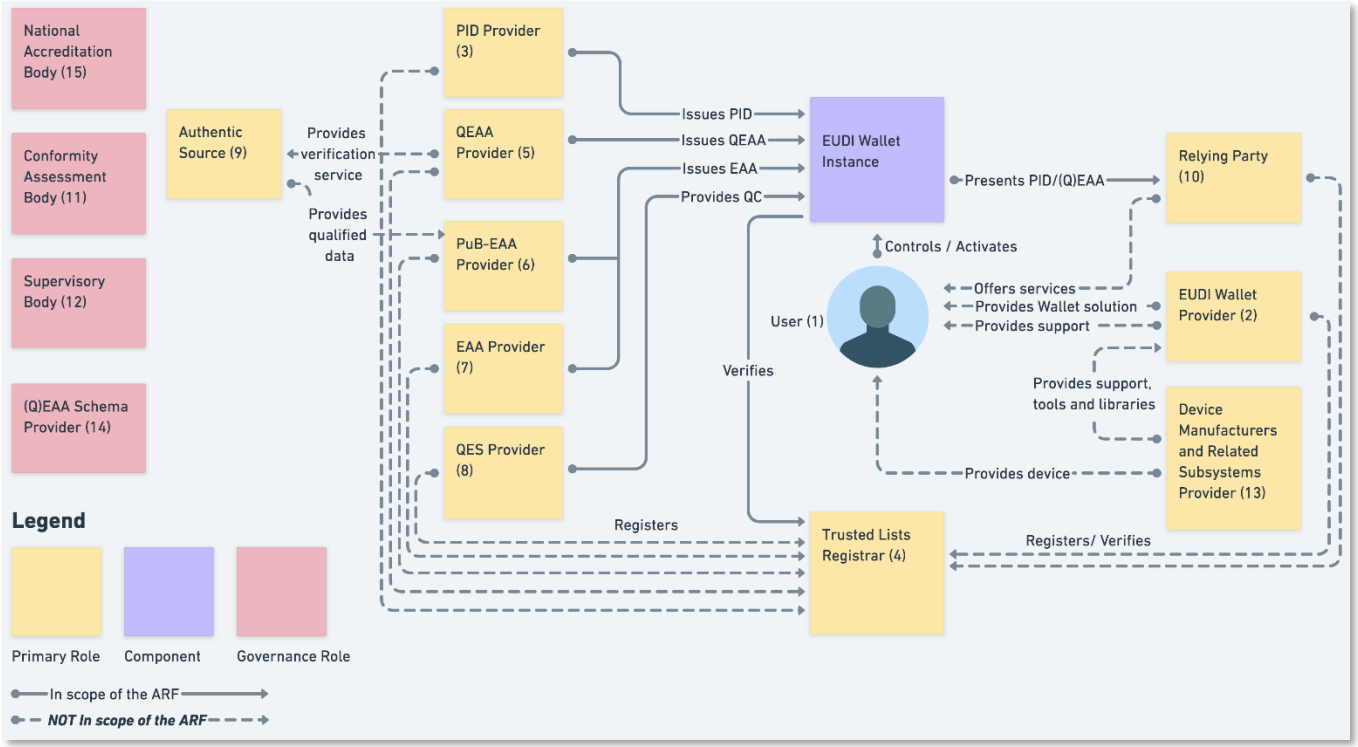
ARF Umfang

- ARF soll festlegen:
  - Umfeld: Rollen, Wallet Lifecycle
  - Anforderungen an PID und QEAA
  - Referenzarchitektur und Datenflüsse
  - Zertifizierungsanforderungen
- Aktuelle Version 1.4 besteht aus
  - bereits konkreter definiertem Core und Rulebooks
  - High-Level Anforderungen für Rest

ARF v1.4 Struktur

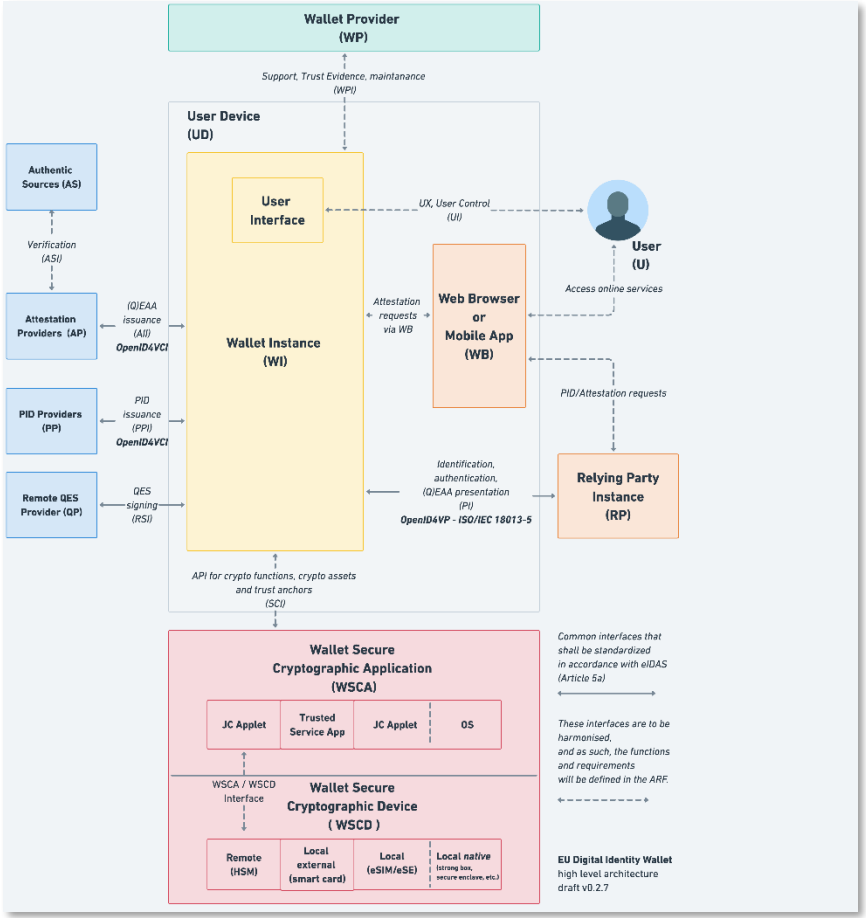
- Core Dokument
  - Konkret zu Ökosystem und Referenz-architektur (Komponenten)
  - Prinzipien des Vertrauensmodells
- High-Level Requirements
  - tw. konkret, tw. erst Grundsätze
  - u.a. Protokolle (noch nicht profiliert)
- Rule-Books
  - Personenidentifikationsdaten (PID)
  - mobiler Führerschein (mDL)
  - Pseudonyme
- Service Blueprints
  - User Journeys zu Ausgabe und Initialisierung; Athentifizierung, Präsentation von PID, Attestations, Signatur, .etc.
- Design Guide
  - Grundprinzipien UI/UX

Ökosystem



*Grafik aus EU Digital Identity Framework and Reference Document – Stand Mai 2024

Referenzarchitektur



- Trennung in
  - Wallet-Instanz
    - die „App“
  - Wallet Secure Crypto-Application/-Device
    - WSCA/WSCD; „Crypto“

*Grafik aus EU Digital Identity Framework and Reference Document - Stand Mai 2024

Eckpunkte aus ARF

- 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-HSM-System (vgl. ID Austria auf 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

High-level Requirements

- Eine Reihe an Anforderungen zu
  - Accessing Online Services
  - Mobile Driving License
  - PID / QEAA Rulebook
  - Relying Party Authentication
  - Pseudonyms
  - … uvm. (dzt. 50 topics adressiert)

High level requirements

A - Generic HLRs

Index	Requirement specification
ISSU_01	Wallet Providers SHALL ensure that their Wallet Solution supports the OpenID4VCI protocol specified in [OpenID4VCI], with additions and changes as documented in this Annex (see e.g. this Topic and [Topic 9]) and in future technical specifications created by or on behalf of the Commission.
ISSU_02	Wallet Providers SHALL ensure that their Wallet Solution supports the attestation formats specified in: • ISO/IEC 18013-5, see [ISO18013-5]. • "SD-JWT-based Verifiable Credentials (SD-JWT VC)", see [SD-JWT-VC]. with additions and changes as documented in this Annex and in future technical specifications created by or on behalf of the Commission.
ISSU_03	Wallet Providers SHALL ensure that their Wallet Solution supports the presentation protocols specified in: • ISO/IEC 18013-5, see [ISO18013-5]. • OpenID for Verifiable Presentations, see [OpenID4VP]. with additions and changes as documented in this Annex and in future technical specifications created by or on behalf of the Commission.
ISSU_04	The OpenID4VCI protocol specified in [OpenID4VCI] SHALL enable PID Providers and Attestation Provider to issue to a Wallet Instance a batch of multiple PIDs or attestations that are simultaneously valid and contain the same attributes.
ISSU_05	A Wallet Instance SHALL support a process to activate a newly issued PID or attestation, in accordance with Commission Implementing Regulation (EU) 2015/1502 section 2.2.2. The goal of the activation process is to verify that the PID or attestation was delivered into the Wallet Instance and WSCA of the User to whom it belongs. The Wallet Instance SHALL NOT allow a User to use a non-activated PID or attestation.
ISSU_06	After a Wallet Instance receives a PID or an attestation from a PID Provider or Attestation

Wallet Zertifizierung

- eIDAS Revision sieht Zertifizierung des Wallets vor
  - Grundsätzlich unter einem harmonisierten Schema des Cyber Security Act (CSA), dies ist mit und trotz EUCC im Wallet-Zeitplan unrealistisch
  - Eigenes Wallet-Schema soll unter CSA entstehen, dies braucht Zeit
  - Bis CSA anwendbar, können MS nationale Schemen anwenden
- Anforderungen an nationale Schemen in Untergruppe
  - Nationale Schemen können an nationale Wallets angepasst sein
  - Gemeinsame Liste an Risiken, die Schemen mitigieren müssen

Inhalte

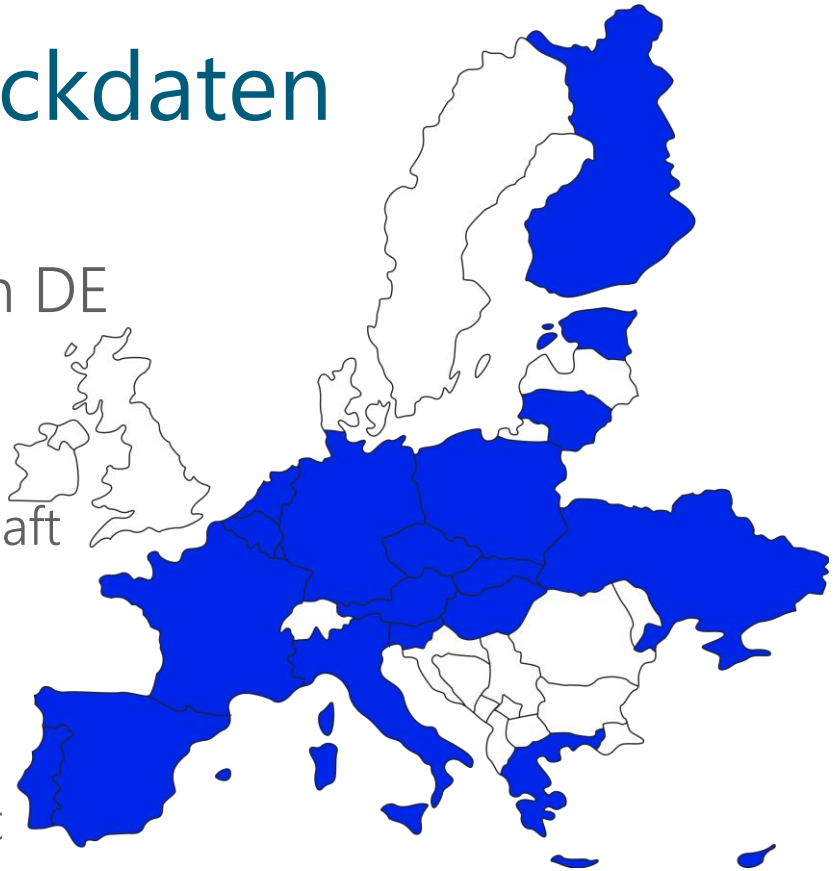
- eID in Österreich
- Toolbox-Prozess und Architektur-Referenzrahmen
- **Large Scale Pilot POTENTIAL**
- Zusammenfassung und Umsetzungspläne

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 BKA federführend
- Start 1. April 2023, Dauer 26 Monate
  - wird voraussichtlich etwas verlängert



Technische Inhalte

- Umsetzung ARF und Integration in 6 Use Cases
  1. Identifikation im E-Government
  2. Kontoeröffnung
  3. Digitaler Führerschein
  4. SIM Registrierung
  5. Qualifizierte Signatur
  6. eMedikation

Inhalte

- eID in Österreich
- Toolbox-Prozess und Architektur-Referenzrahmen
- Large Scale Pilot POTENTIAL
- **Zusammenfassung und Umsetzungspläne**

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
- DfRA mit Nov. 2024, damit Wallet Ausgabe Ende 2026

Umsetzungspläne

- ID Austria und Ausweisplattform sind in Produktion
  - teils bereits sehr nahe am ARF (z.B. ISO/IEC 18013-5)
  - teils andere Protokolle (z.B. SAML, OIDC vs. OIDC4VP)
- ID Austria / eAusweise sollen nahtlos in EUDI migrieren
  - Ansatz remote HSM (ID Austria; proximity herausfordernd)
  - Unter anderem über LSP POTENTIAL erprobt
  - Berücksichtigung etablierter Infrastruktur, zB ERnP

Quellen eIDAS Revision

- eIDAS Novelle (EU) 2024/1183
  - https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32024R1183
  - (noch keine konsolidierte Fassung abrufbar)
- Informationsseite EUDI Wallet
  - https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/
- Architekturreferenzrahmen „ARF“
  - https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/latest/
- Referenzumsetzung
  - https://github.com/eu-digital-identity-wallet/.github/blob/main/profile/reference-implementation.md
- Large Scale Pilots
  - DC4EU https://dc4eu.eu/
  - EWC https://eudiwalletconsortium.org/
  - NOBID https://www.nobidconsortium.com/
  - POTENTIAL https://www.digital-identity-wallet.eu/

a-sit.at/

Herbert.Leitold@a-sit.at