A-SIT

Von ID Austria und Ausweisplattform hin zu einem EU-Wallet

Arne Tauber

Inhalte

- Rolle A-SIT zu eIDAS
- Aktuelle Situation eID in Österreich
- Ausweisplattform
- Überblick und Stand eIDAS Revision
- Toolbox-Prozess und Architektur-Referenzrahmen
- Large Scale Pilot POTENTIAL
- Zusammenfassung

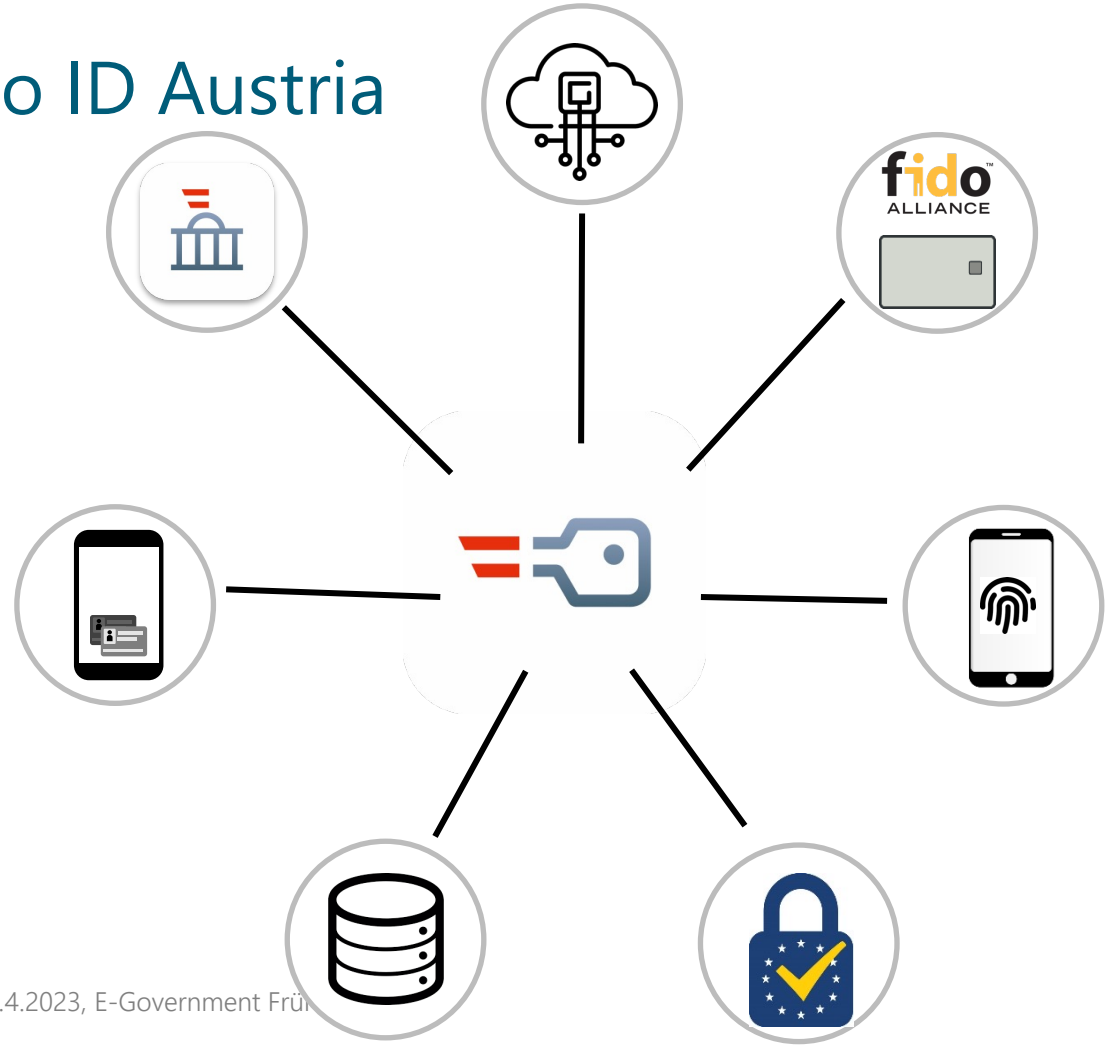
Über A-SIT und mich i.ZsHg. mit eIDAS

- A-SIT ist Verein, Mitglieder BMF, BRZ, TUG, DUK, JKU
  - u.a. QSCD-Bestätigungsstelle und akkr. Konf.-Bewertung eIDAS
- Ich selbst bin Generalsekretär von A-SIT, in eIDAS:
  - Einer der österr. Vertreter in Expert Group (Toolbox Prozess) und techn. Subgroup
  - In LSP POTENTIAL techn. Mgmt. in ARGE WALLET.AT und nationaler Vertreter in WP2 (Wallet Umsetzung)

Inhalte

- Rolle A-SIT zu eIDAS
- Aktuelle Situation eID in Österreich
- Ausweisplattform
- Überblick und Stand eIDAS Revision
- Toolbox-Prozess und Architektur-Referenzrahmen
- Large Scale Pilot POTENTIAL
- Zusammenfassung

Status Quo ID Austria



Inhalte

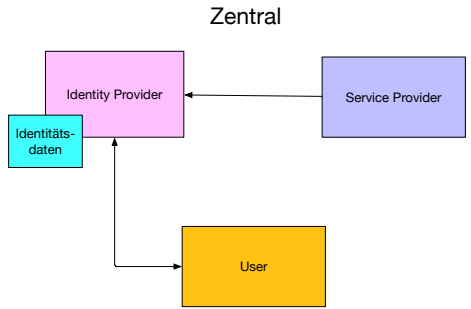
- Rolle A-SIT zu eIDAS
- Aktuelle Situation eID in Österreich
- Ausweisplattform
- Überblick und Stand eIDAS Revision
- Toolbox-Prozess und Architektur-Referenzrahmen
- Large Scale Pilot POTENTIAL
- Zusammenfassung

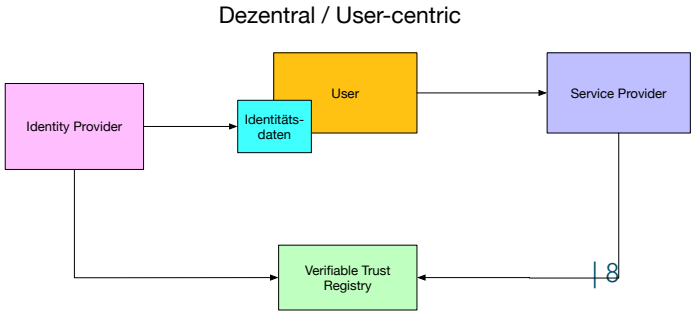
Hintergrund Ausweisplattform

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

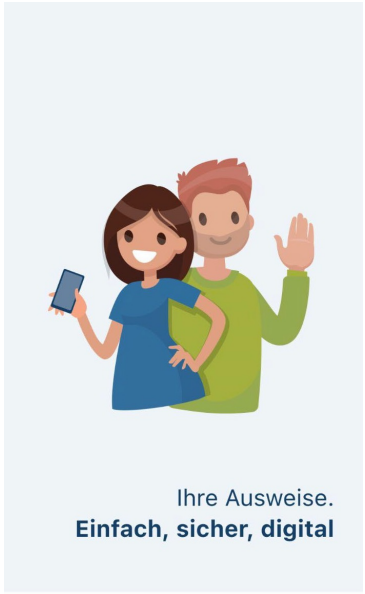
Dezentrale Identität

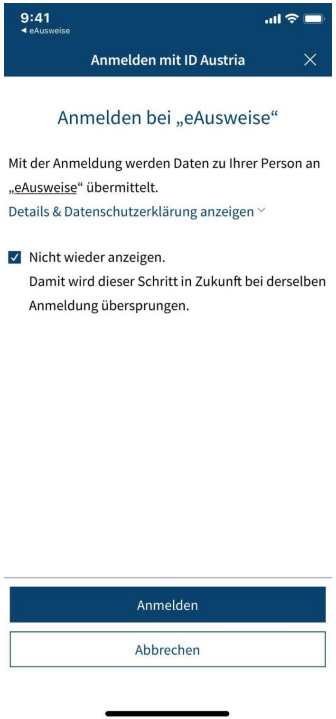
- Entkoppelung von Identity Provider und Service Provider/Prüfer
  - User dazwischen (wie bei physischem Ausweis)
    - Identitätsdaten/Attribute beim User
  - User-zentriert (Identitätsdaten bei User)
- Herausforderungen
  - Selective Disclosure / ZKP
  - Widerruf (Technisch / Fachlich)

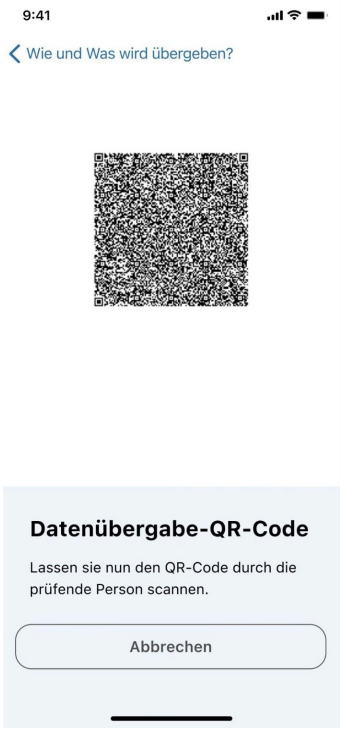




eAusweise App

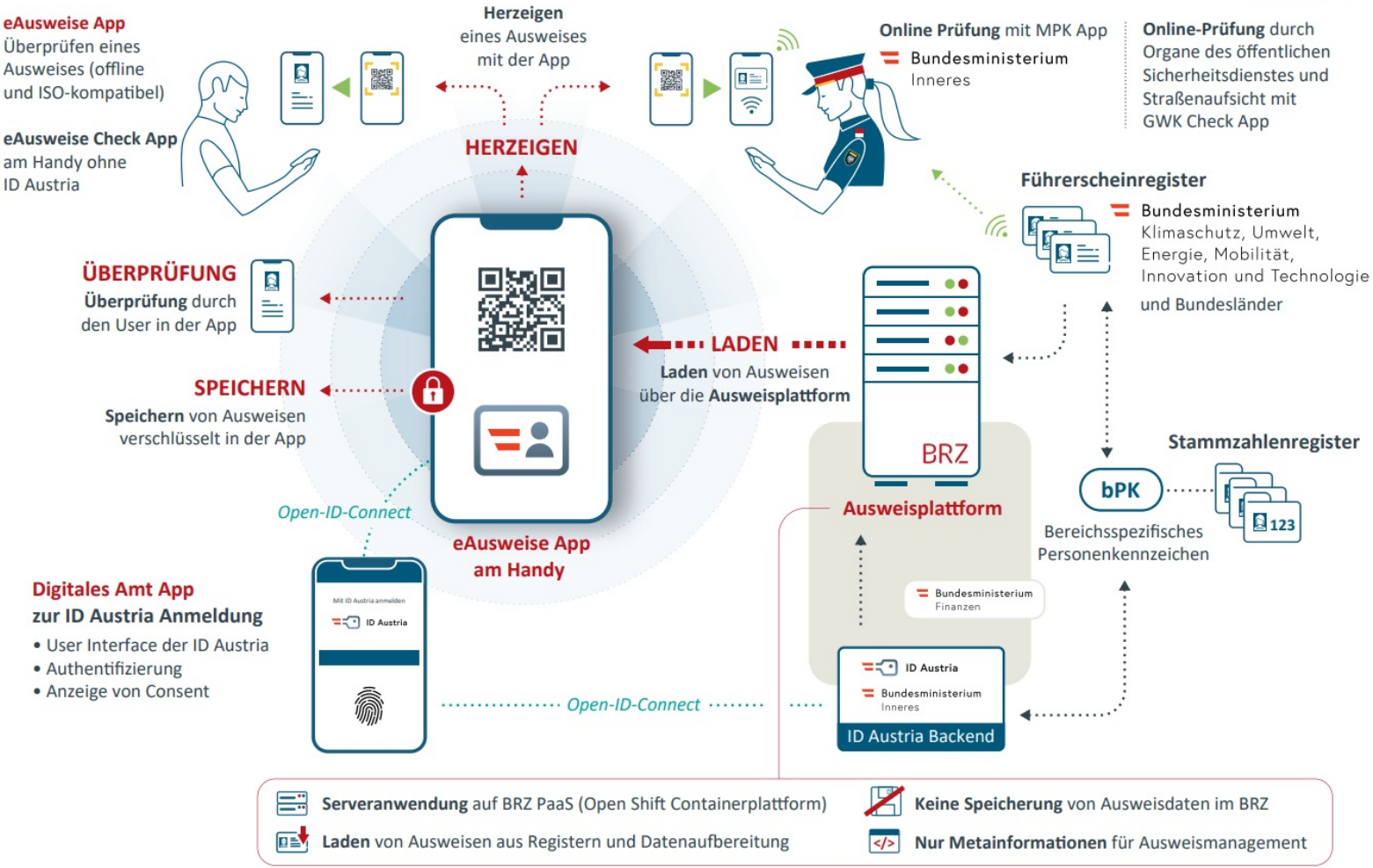




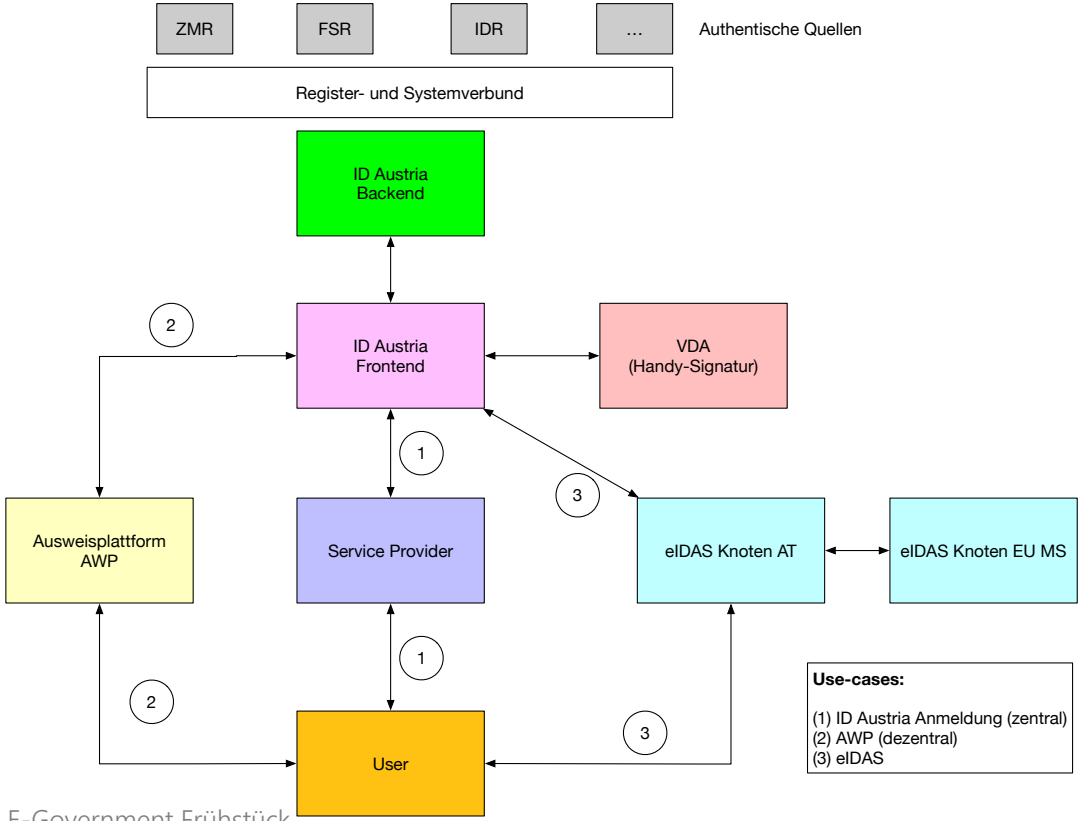


Ausweisplattform – Technischer Gesamtüberblick

BRZ



Gesamtarchitektur eID in Österreich



Inhalte

- Rolle A-SIT zu eIDAS
- Aktuelle Situation eID in Österreich
- Ausweisplattform
- Überblick und Stand eIDAS Revision
- Toolbox-Prozess und Architektur-Referenzrahmen
- Large Scale Pilot POTENTIAL
- Zusammenfassung

eIDAS Revision: Neue Konzepte

- Qualifizierte elektronische Attributsbescheinigungen (QEAA)
  - von qualifiziertem Vertrauensdiensteanbieter ausgestellt
  - authentische Quelle in allgem. Ausrichtung Rat gleichgestellt
    - oder durch öffentliche Stelle im Namen der authentischen Quelle
- EUid-Brieftasche aka „Wallet“ oder „EUDI Wallet“
  - Elektronisches Identifikationsmittel Vertauenswürdigkeit „hoch“
- Elektronisches Vorgangsregister (Ledger)
  - *Anm.* Europäisches Parlament schlug vor, dies zu streichen

Verpflichtungen der Mitgliedsstaaten

- Ausgabe EUDI Wallet und Notifizierung eID auf LoA hoch
  - 24 Monate nach Inkrafttreten der jeweiligen Umsetzungsrechtsakte
  - für privatwirtschaftliche Anwendungen verwendbar (bisher „möglich“)
- Zertifizierung von eID und Wallet
  - Ersetzt Peer-Review (für notifizierte weiterhin, wenn nicht zertifiziert)
- Auf Verlangen Nutzer:in Attribute durch QVDA zu prüfen
  - Attribute des Anhang VI wie Adresse, Alter, Bildungsabschlüsse, Qualifikationen, Familienzusammensetzung, Finanzdaten, …
- Registrierung vertrauender Beteiligter (Anwendungen)

Verpflichtungen Anwendung

- Vertrauende Beteiligte müssen Wallet akzeptieren, wenn sie
  - Online-Dienst einer öffentliche Stelle sind
  - als private Dienste starke Nutzerauthentifizierung benötigen
    - gesetzlich oder vertraglich, bis auf Kleinst- und Kleinunternehmen
      - Genannte Bereiche: Verkehr, Energie, Bankenwesen, Finanzdienstleistungen, soziale Sicherheit, Gesundheit, Trinkwasser, Postdienste, digitale Infrastrukturen, Bildung oder Telekommunikation
    - Spätestens 12 Monate nach Ausgabeverpflichtung der MS
  - als sehr große Plattformen gem. DSA Authentifizierung fordern
    - d.h. wenn über 45 Mio. Nutzer:innen

Ausgabe der EUDI Wallets

- EUDI Wallets können (bzw. müssen)
  a) von einem Mitgliedstaat,
  b) im Auftrag eines Mitgliedstaats oder
  c) unabhängig von einem Mitgliedstaat, aber von einem Mitgliedstaat anerkannt

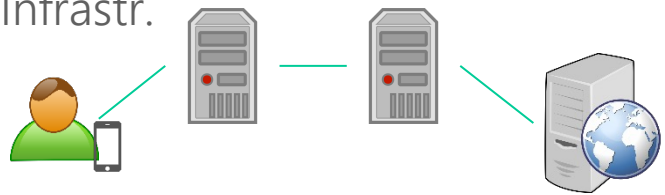
  herausgegeben werden
- Aktiviert über bestehende eID „hoch“ oder als eigenst. eID

Funktionen EUDI Wallet

- EUid Brieftasche muss für natürliche und juristische Person
  - Personenidentifikationsdaten bereitstellen (MS Verantwortung)
    - Im wesentlichen wie bisher Name, Geb.-Datum, Identifikator
    - Verpflichtung eindeutig & dauerhaft, wo gesetzl. vorgeschrieben
      - bisher „Eindeutige Kennung, die […] möglichst dauerhaft fortbesteht“
  - QEAA oder Daten aus auth. Quelle (über QVDA oder Register)
  - Online und Offline bzw. mit selektiver Offenlegung
  - Unterzeichnen über qualifizierte Signatur oder Siegel erlauben
- Dazu gemeinsame Standards und Schnittstellen über URA

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
  - Attribute entweder
    - Person Identification Data
    - EAA im Wallet oder in „Cloud“
  - Attribute über qualifizierten VDA oder aus authentischer Quelle

EUDI Wallet hat parallele Streams

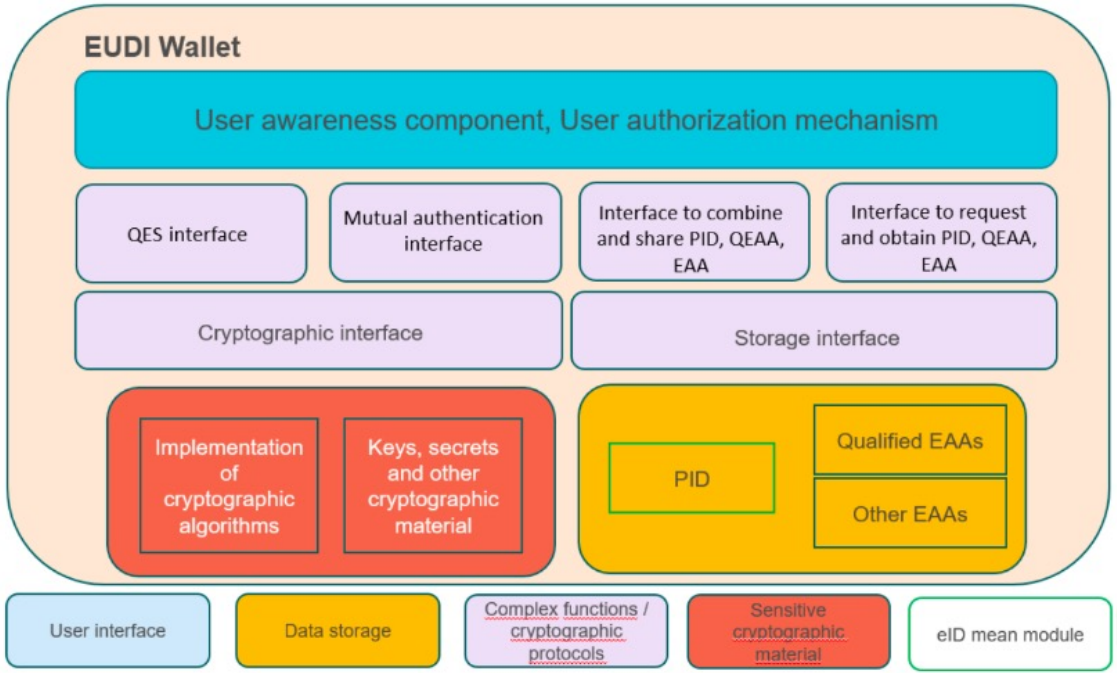
- Formell über Umsetzungsrechtsakte
  - Zu Funktionalität, Schnittstellen, Validierung, Onboarding *hoch* und Heben von *substantiell*, Zertifizierung
  - 6 Monate nach Inkrafttreten der Verordnung
    - als „technische und betriebliche Spezifikationen und Bezugsnormen“
- Parallel dazu laufen Arbeiten zu
  - Architekturreferenzrahmen (Vorbereitung Spezifikationen durch MS)
  - Referenz-Wallet (Vertrag EK mit „NiScy“ Netcompany-Intrasoft und Scytales)
  - Large Scale Pilots (vier Konsortien zu unterschiedlichen Use Cases)

  samt Koordination zwischen diesen.

Inhalte

- Rolle A-SIT zu eIDAS
- Aktuelle Situation eID in Österreich
- Ausweisplattform
- Überblick und Stand eIDAS Revision
- Toolbox-Prozess und Architektur-Referenzrahmen
- Large Scale Pilot POTENTIAL
- Zusammenfassung

High-Level Komponenten (Outline)



*Grafik aus EU Digital Identity Framework and Reference Document – Stand Feb. 2022

Eckpunkte aus ARF v1.0

- 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

Inhalte

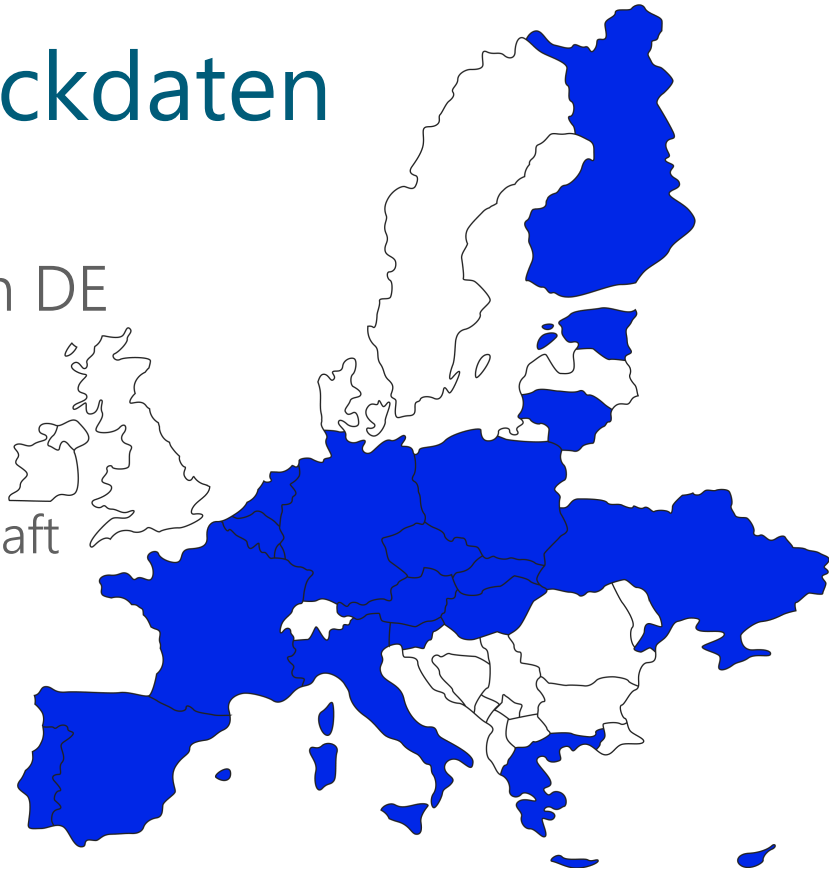
- Rolle A-SIT zu eIDAS
- Aktuelle Situation eID in Österreich
- Ausweisplattform
- Überblick und Stand eIDAS Revision
- Toolbox-Prozess und Architektur-Referenzrahmen
- Large Scale Pilot POTENTIAL
- Zusammenfassung

Hintergrund

- EK fördert seit einiger Zeit Large Scale Pilots in wesentlichen Politikbereichen
- Ebenso zum EUDI Wallet
  - 4 LSPs werden gefördert, vorauss.:
    - 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
- Start 1. April 2023, Dauer 26 Monate



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

a-sit.at/

Arne.Tauber@a-sit.at