A-SIT

Stand eIDAS Revision und EUDI

Herbert Leitold

Inhalte

- Rolle A-SIT zu eIDAS
- Überblick und Stand eIDAS Revision
- Toolbox-Prozess und Architektur-Referenzrahmen
- Large Scale Pilot POTENTIAL
- Zusammenfassung

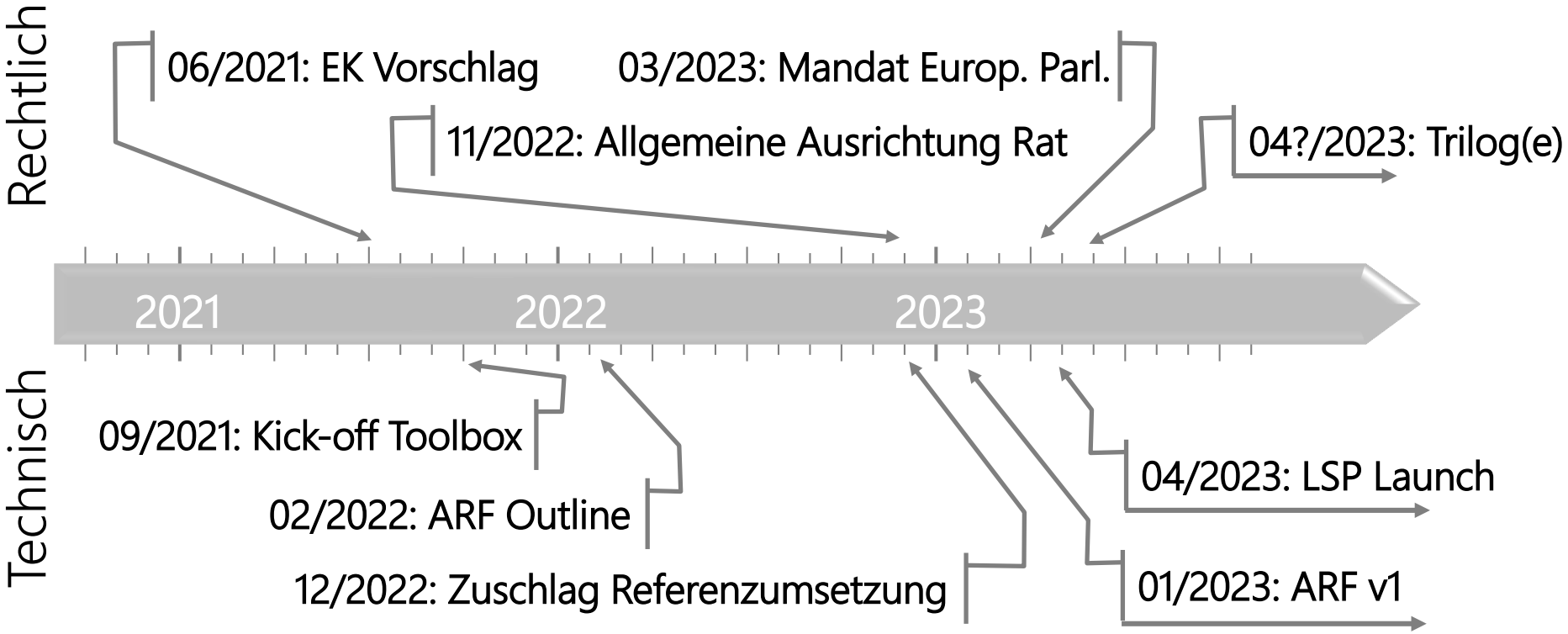
Über A-SIT und mich i.ZsHg. mit eIDAS

- A-SIT ist Verein, Mitglieder BMF, BRZ, TUG, DUK, JKU
  - u.a. QSCD-Bestätigungsstelle und akkr. Konf.-Bewertung eIDAS
- Ich selbst bin Gesamtleiter von A-SIT, dabei in eIDAS:
  - Mitglied der österreichischen Delegation in Kooperationsnetzwerk, Expert Group, Subgroup
  - Einer der österr. Vertreter in Wallet Toolbox Prozess
  - In LSP POTENTIAL Koordination in ARGE WALLET.AT und Leitung Use Case „qualifizierte Signatur“

Inhalte

- Rolle A-SIT zu eIDAS
- **Überblick und Stand eIDAS Revision**
- Toolbox-Prozess und Architektur-Referenzrahmen
- Large Scale Pilot POTENTIAL
- Zusammenfassung

Zeitlinie eIDAS Revision bisher



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

Einiges weiteres neues …

- Vorgeschlagene Änderungen sind umfangreicher, wie
  - Ausgabe qualifizierte Zertifikate per eID nur mehr LoA „hoch“
  - „Heben“ eID „substantiell“ auf „hoch“ über Fernverfahren
  - Abgleich von Datensätzen, d.h. record matching bei eID
  - Elektronische Archive (*Anm.*: EP schlägt Löschung vor), Rolle NIS2, ….

  … was aber in diesem Vortrag nicht wesentlich gesehen wird
- Auch Änderungen aus Trilog zu erwarten
  - Basis hier ist vor allem die allgemeine Ausrichtung des Rates

Verpflichtungen der Mitgliedsstaaten

- Notifizierung eID LoA hoch und Ausgabe zertif. EUDI Wallet
  - 24 Monate nach Inkrafttreten der jeweiligen Umsetzungsrechtsakte
  - für privatwirtschaftliche Anwendungen verwendbar (bisher „möglich“)
- Zertifizierung von eID und Wallet
  - Ersetzt Peer-Review (Wallet muss zertifiziert sein, notifizierte kann)
- 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

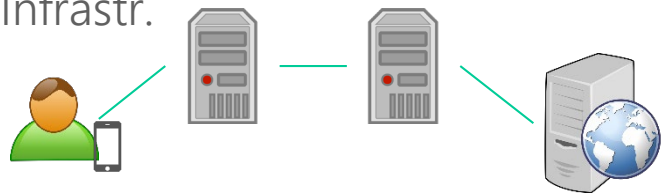
  herausgegeben werden
- Aktiviert über bestehende eID „hoch“ oder als eigenst. eID

Funktionen EUDI Wallet

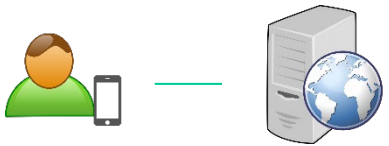
- EUid Brieftasche muss für natürliche und juristische Person
  - Personenidentifikationsdaten bereitstellen (MS Verantwortung)
    - Im wesentlichen wie bisher Name, Geb.-Datum, Identifikator
    - Verpflichtung eindeutig & dauerhaft, wo gesetzl. vorgeschrieben
      - bisher „Eindeutige Kennung, die […] 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

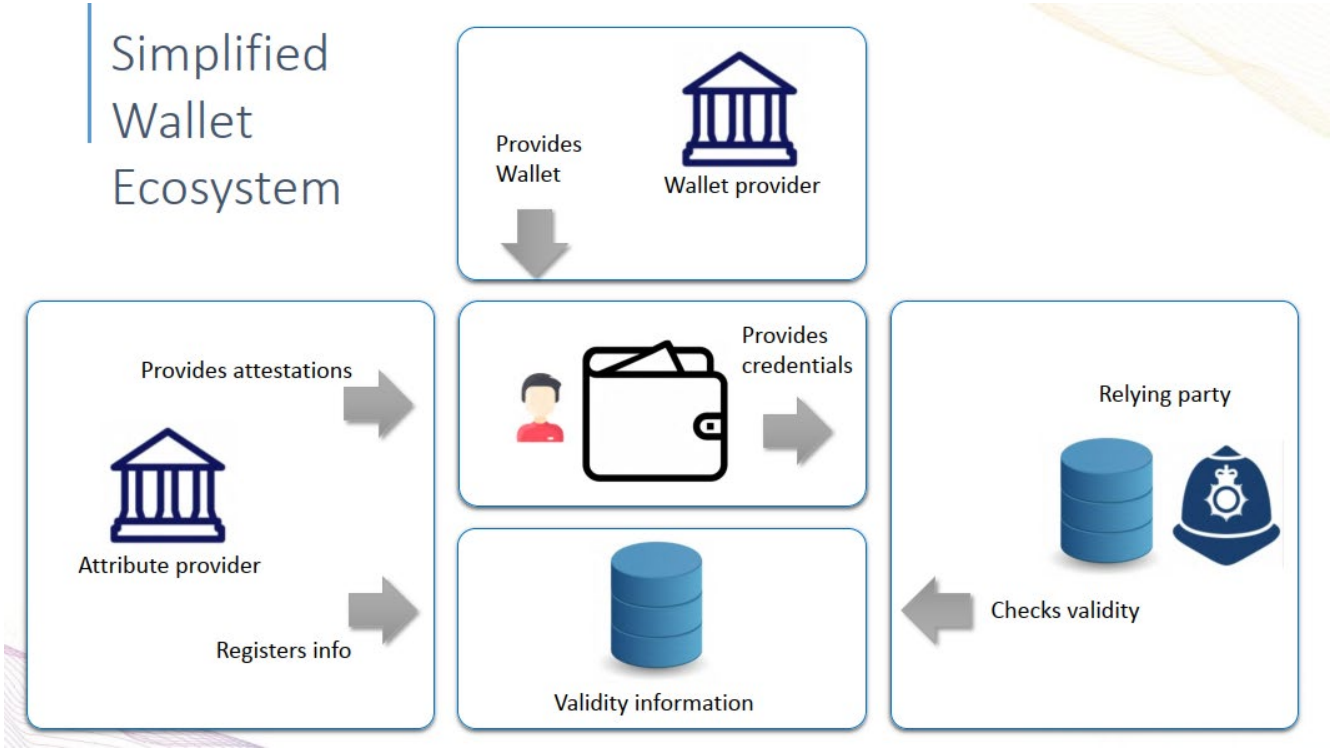
- Formell über Umsetzungsrechtsakte
  - Zu Funktionalität, Schnittstellen, Validierung, Onboarding *hoch* und Heben von *substantiell*, Zertifizierung
  - 6 Monate nach Inkrafttreten der Verordnung
    - als „technische und betriebliche Spezifikationen und Bezugsnormen“
- Parallel dazu laufen Arbeiten 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.

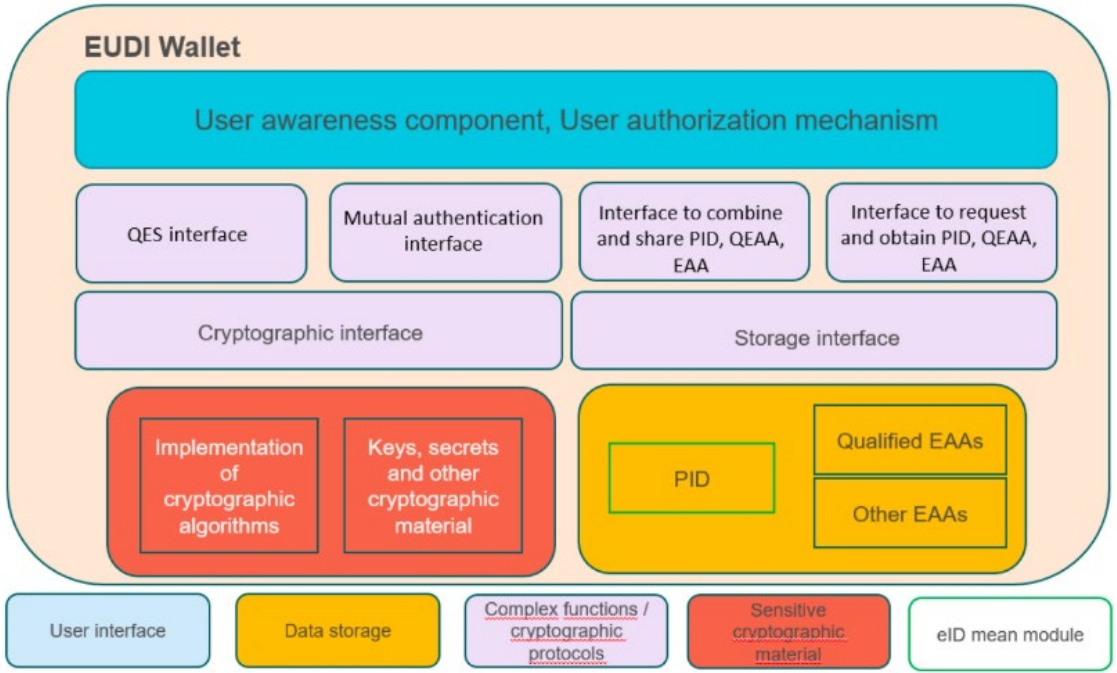
Inhalte

- Rolle A-SIT zu eIDAS
- Überblick und Stand eIDAS Revision
- **Toolbox-Prozess und Architektur-Referenzrahmen**
- Large Scale Pilot POTENTIAL
- Zusammenfassung

Ursprüngliche High-Level Sicht der EK



High-Level Komponenten (Outline)



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

ARF v1 Umfang

- ARF soll festlegen:
  - Umfeld: Rollen, Wallet Lifecycle
  - Anforderungen an PID und QEAA
  - Referenzarchitektur und Datenflüsse
  - Zertifizierungsanforderungen
- Version 1.0 hat noch signifikanten „backlog“ offener Punkte

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 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

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

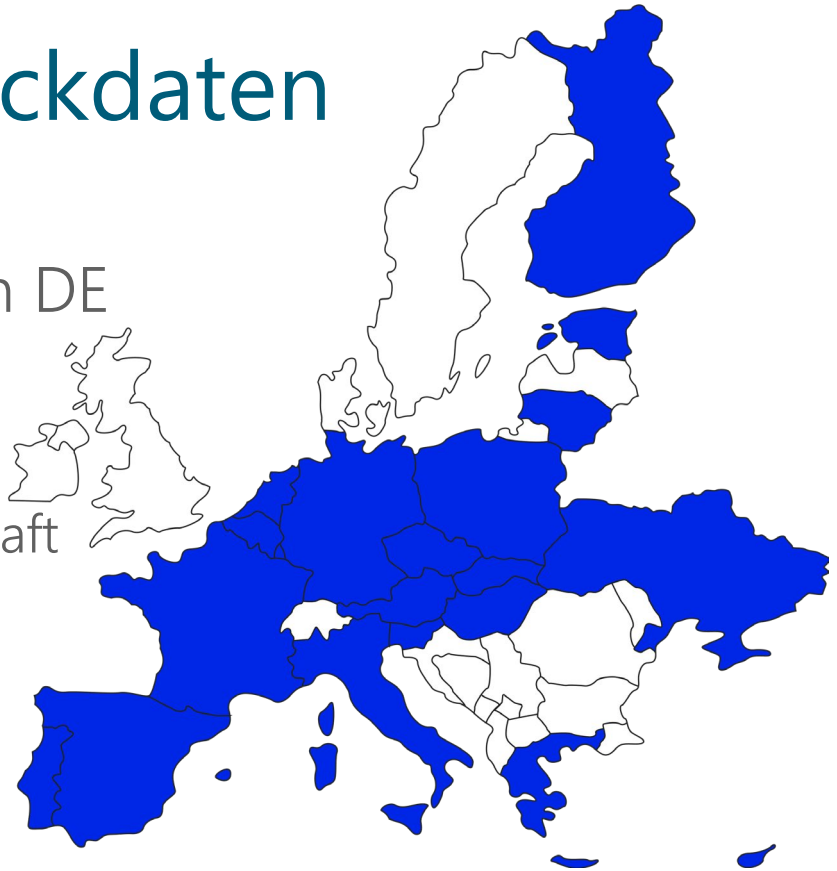
- Rolle A-SIT zu eIDAS
- Überblick und Stand eIDAS Revision
- Toolbox-Prozess und Architektur-Referenzrahmen
- **Large Scale Pilot POTENTIAL**
- Zusammenfassung

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

Inhalte

- Rolle A-SIT zu eIDAS
- Überblick und Stand eIDAS Revision
- 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

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. EP Committee Reports (ITRE, LIBE, JURI) bzw. 1st reading
- Architekturreferenzrahmen „ARF"
  - Outline: https://futurium.ec.europa.eu/en/digital-identity/toolbox (Regsiterieung 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