A — SIT · E-GOVERNMENT FRÜHSTÜCK 2026

EU Digital Identity Wallet

Aktuelle Entwicklungen & Showcase: KI-basiertes Onboarding

Arne Tauber

A-SIT Zentrum für sichere Informationstechnologie — Austria

Agenda

Von der Regulierung zur Umsetzung

Identifikation in Österreich — heute

ID Austria & eAusweise als Vergleichsbasis

ID Austria

Authentifizierung & Signatur

- Login: oesterreich.gv.at, FinanzOnline, Bank-Login
- Server-seitige QES + mobile App mit Push-Auth
- Web: UID/Passwort + Mobilgerät / FIDO
- Unterstützung App2App
- AT · eIDAS-notifiziert auf LoA high

eAusweise

Ausweise digital vorzeigen

- Führerschein, Berechtigungsnachweise
- Polizeikontrolle, Altersnachweis, Behördenservice
- Ausweisplattform, kryptografisch verifizierbar
- Kein bereichsspezifisches Personenkennzeichen
- Dezentral
- AT · ausgewählte Behördenkontexte

Übergang zum Wallet: *Beides geht zusammen — und wird EU-weit nutzbar.*

Wallet im Einsatz

Was sieht der/die Nutzer:in?

01

Service aufrufen

Bürger:in startet z. B. einen Antrag online — Service-Anbieter (RP) verlangt Identifikation.

02

Wallet öffnen

QR-Code oder Deep-Link öffnet die Wallet-App am Smartphone.

03

Daten freigeben

Wallet zeigt: „RP fragt Name, Geburtsdatum, Adresse“ — bewusste Zustimmung der Nutzer:in.

04

Bestätigung

Wallet liefert signierte Daten an die RP — Vorgang läuft durch.

01

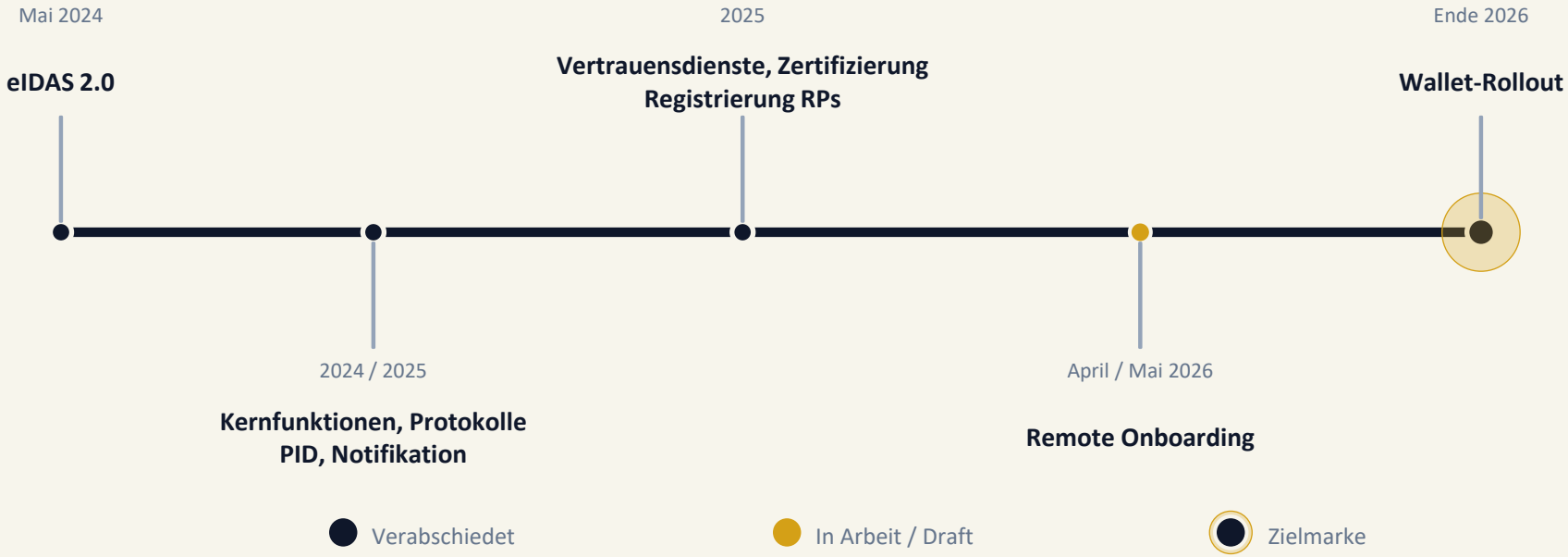
SEKTION 01

Rechtlicher Rahmen

Durchführungsrechtsakte & Zertifizierung

Durchführungsrechtsakte im Überblick

eIDAS 2.0 — vom Rechtsrahmen zur Umsetzung



Was steckt in den wichtigsten Akten?

Auswahl der für Verwaltung & Wallet-Rollout relevanten DfRAs

DfRA	Titel	Kerninhalt
2024/2979	**Kernfunktionalitäten der Wallet**	Sicherheitsarchitektur, Consent, Logging, Portabilität
2024/2982	**Protokolle & Schnittstellen**	Wallet ↔ Issuer ↔ Relying Party — Interoperabilität
2024/2977	**Personenidentifikationsdaten (PID) & EAAs**	Issuance, Revocation, Datenformate
2024/2981	**Zertifizierung**	Prüftiefen, Bewertungsmethoden, Common Criteria
2026/798	**Remote Onboarding**	LoA high digital — Referenz: ETSI TS 119 461

Zertifizierung: Nationales AT-Schema & CSA

Wer zertifiziert, wer erkennt an, wer haftet?

Nationales AT-Schema

Österreich · Übergangs-Regime

Überbrückung, bis CSA-Schema greift — inhaltlich abgestimmt.

Zertifizierungsstellen und Prüftiefe werden national definiert.

Status: Erstes notifiziertes Schema in EU durch Österreich.

CSA-Schema

EU-weit · Cybersecurity Act

Verpflichtend für notifizierte Wallets.

Basis für gegenseitige Anerkennung zwischen Mitgliedstaaten.

Status: Entwurf unter ENISA / ECCG.

Kernfrage für die Verwaltung: *Wer zertifiziert, wer erkennt an, wer haftet — das entscheidet über die Rollout-Geschwindigkeit.*

02

SEKTION 02

ARF & Technische Spezifikationen

Pseudonyme — ZKP — Age Verification — Signaturen — Business Wallet

Architecture and Reference Framework

Zentrale technische Referenz — lebend, nicht rechtsverbindlich

Was es ist

- Technische Referenz für Wallets und deren Ökosystem
- Datenmodelle, Protokolle, Trust-Modell, Sicherheitsanforderungen

Aktueller Stand

- Lebendes Dokument — laufend fortgeschrieben
- Wird durch Durchführungsrechtsakte verbindlich referenziert

Was sich bewegt

- Privacy-Bausteine: Pseudonyme, Zero Knowledge Proofs
- Proximity-Flows, Revocation, Trust-Model-Details

ARF v1.6 · ~200 Seiten · governed by EU Digital Identity Expert Group

ARF: Pseudonyme

Datensparsam by design — nicht nur sicher

Idee

- Wiedererkennbarer Auftritt ohne Preisgabe der Identität.
- Unterschiedliche Pseudonyme pro Dienst — keine Verkettung.

Typische Anwendungsfälle

- Dienste-Login, Foren, wiederkehrender Kontakt ohne Klarnamen.

Stand im ARF

- Konzeptionell verankert, Erzeugung im Wallet vorgesehen.
- Offen: Prüfbarkeit, Widerruf, Interoperabilität zwischen Wallets.

ARF: Zero Knowledge Proofs

Beweisen, ohne preiszugeben

Was gemeint ist

- z. B. „über 18”, ohne das Geburtsdatum zu offenbaren.

Abgrenzung

- Selektive Offenlegung (schon da): einzelne Attribute zeigen oder nicht.
- Echte ZKP zusätzlich: Unlinkability über mehrere Vorzeigevorgänge.

Stand im ARF

- In Diskussion — BBS+, SNARK, anonymous credentials, mehrere Ansätze.
- Noch nicht verbindlich spezifiziert — relevant u. a. für Age Verification.

Age Verification: EU Blueprint

Eigenständige App — Brücke zum Wallet

EU Blueprint

- Initiative der Kommission — eigenständige App für Altersnachweis.
- Übergangslösung bis zum breiten Wallet-Rollout.

Technische Nähe zum Wallet

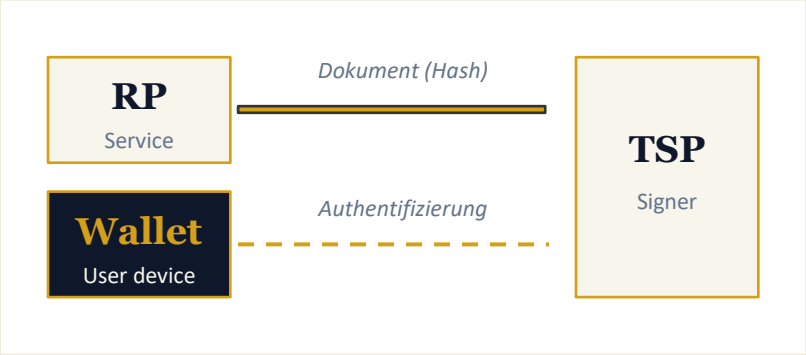
- Verifiable credentials, selektive Offenlegung — dieselbe Familie.
- Spitzname “Mini Wallet”

Verhältnis zum EUDIW

- Blueprint heute — Integration ins Wallet mittelfristig.
- Politisches Pilotthema für datensparsame Identifizierung.

Signaturen: RP/TSP-centric vs. Wallet-centric

Wie fließt das Dokument zum TSP?



RP/TSP-centric

- Dokument geht direkt RP → TSP.
- Wallet dient nur der Authentifizierung beim TSP.
- Näher am heutigen QES-Betrieb.

Wallet-centric

- Dokument fließt RP → Wallet → TSP.
- TSP kennt die RP nicht — Unlinkability als Privacy-Vorteil.

Signaturlandschaft Österreich

Was bedeutet der Umzug ins Wallet?

HEUTE

ID Austria · Handy-Signatur

serverseitige QES + Security-Layer
RP/TSP-centric only

MORGEN

EU Digital Identity Wallet

Neue Modelle & Standardmodell vermutlich wallet-centric, neue Specs (CSC), Hash-Sig & Stapelsignatur

A-SIT evaluiert aktuell

- Welche Signatur-Modelle sind mit dem heutigen Security-Layer in welcher Form kompatibel?
- Überblick der bestehenden Signaturservices (insbs. eingesetzte Signaturformate)
- Migrationsszenarien von Security-Layer hin zu Wallet Signaturspezifikationen (CSC)

Business Wallet: Hintergrund und Abgrenzung

Eigener Verordnungsvorschlag — derzeit im Rat verhandelt

Personal Wallet

natürliche Person

- Identitätsnachweis & Attribute einer Person
- Qualifizierte Signatur
- Proximity- & Remote-Flows

Business Wallet

juristische Person

- Repräsentiert eine Organisation — EUID als Kennung
- Multi-User-Berechtigungen (Personen mit Rollen)
- Lifecycle: Eintritt / Austritt / Rolle
- Siegel + Signatur als Nachweis

Gleicher technischer Unterbau

Dieselben Protokolle, Formate, Trust-Infrastruktur wie EUDIW · plus EU Digital Directory

Status: 3. Kompromisstext der CY-Präsidentschaft (3/2026) — Trilog ausstehend

Business Wallet: Features & Stand

Eigenes Projekt — folgt zeitlich nach der Personal Wallet

Attestate

Gewerbeberechtigung, Vollmachten, Zertifikate

Multi-User-Berechtigungen

Mehrere Personen mit Rollen, im Namen des Unternehmens

Elektronische Siegel

Siegel statt Signatur als Nachweisform

B2B-Verträge

Vertragsabschluss zwischen Unternehmen

Regulatorisches Reporting

Behördliche Meldungen automatisiert

Elektronische Zustellung

QERDS — Pflicht-Bestandteil im EBW

Reifegrad: *Weniger weit als die Personal Wallet. Einzelne LSPs adressieren B2B.*

03

SEKTION 03

Showcase KI-basiertes Identity Onboarding

Neue Use Cases durch Remote Onboarding explorieren

Neue Use Cases durch Remote Onboarding

Der DfRA 2026/798 öffnet das Feld — wir explorieren

CHANCE

Remote Onboarding auf LoA high bald rechtlich möglich.

Österreich kann damit neue Use Cases explorieren, die bisher physische Präsenz oder andere Verfahren (z.B. RSa Brief) erforderten.

Passwort-Reset

Heute: Behördengang oder RSa Brief
Mit Wallet: Recovery in Minuten via Selfie + NFC

Recovery nach Geräteverlust

Heute: manuelle Re-Registrierung, oft physisch
Mit Wallet: digitales Re-Onboarding, 90 Sekunden

Passfoto-Update (illustrativ)

Heute: physischer Termin alle 10 Jahre
Mit Wallet: App-Upload mit KI-Qualitätscheck

A-SIT Self-Ident PoC — Hybride KI-Architektur

Android-PoC — on-device + Remote, je nachdem was besser passt

Liveness & Face

Blink, 3D-Tiefe, Bewegung

Dokumente

Reisepass, Personalausweis · NFC + KI-OCR

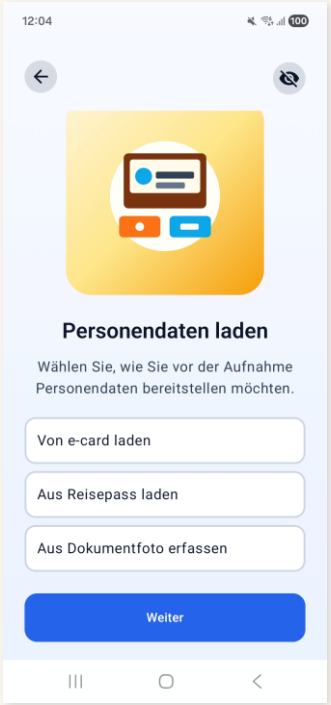
Datenschutzkonform

eIDAS · DSGVO

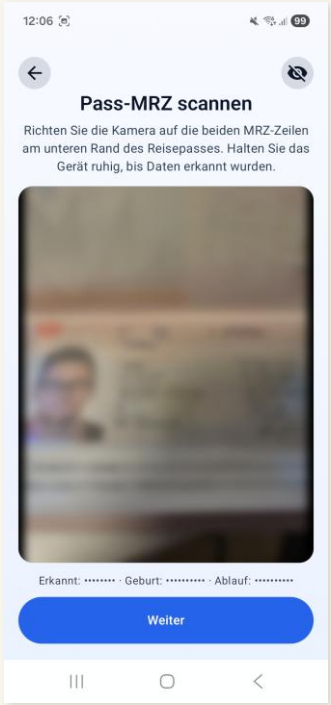
Self-Ident-Flow · Teil 1: Dokument auslesen

Quellenwahl → MRZ-Scan → NFC-Verifikation

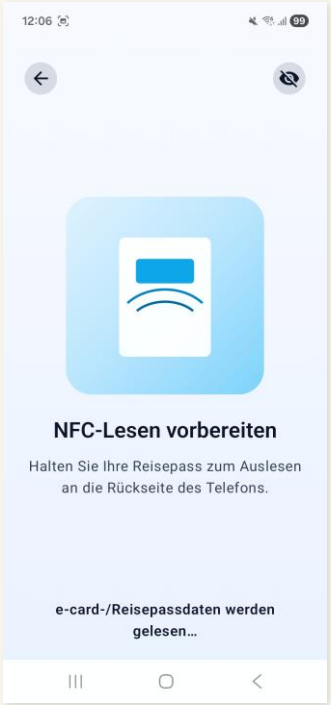
01 Quelle wählen



02 MRZ scannen



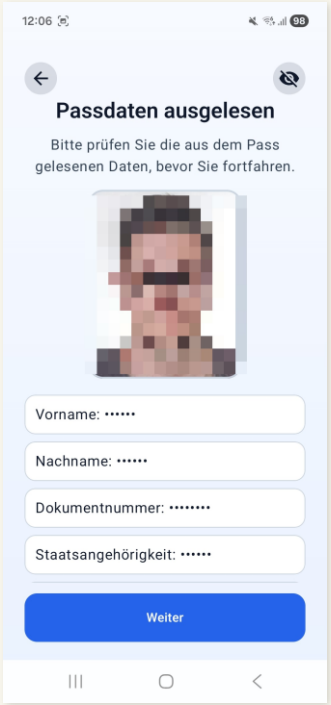
03 NFC-Chip auslesen



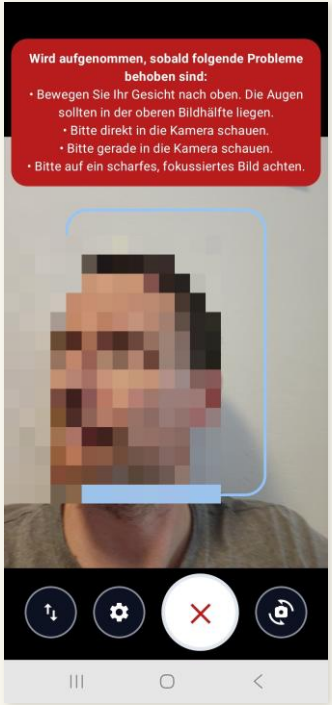
Self-Ident-Flow · Teil 2: Selfie & Vergleich

Pass-Daten verifiziert → Live-Capture → KI-Match

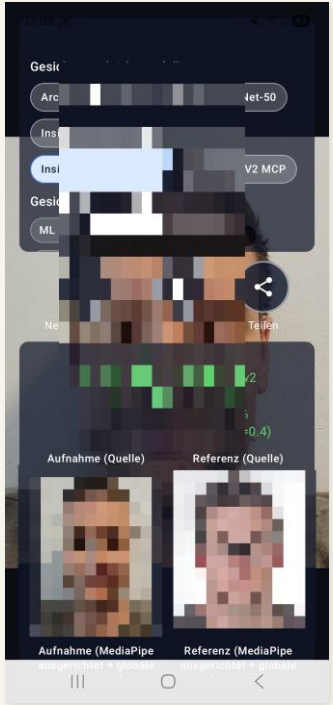
04 Daten verifiziert



05 Live-Selfie



06 Gesichtsvergleich



Risiken & Gegenmaßnahmen

Was KI-Onboarding aushalten muss

Presentation/Injection Attacks

RISIKO

Deepfakes, Masken, Screen-Replay täuschen die Kamera.

ANTWORT PoC

3D-Liveness, Blink-Erkennung, Bewegungsanalyse, Beleuchtungsprüfung
Camera/App Attestation.

Dokumentenfälschung

RISIKO

Gefälschte oder manipulierte Reisepässe / Ausweise.

ANTWORT PoC

NFC-Verifikation des eID-Chips, KI-Klassifikation, MRZ-Abgleich.

Ausblick

Was bis zum Rollout kommen muss — und wo A-SIT beiträgt

Was noch kommt

- Finalisierung Durchführungsrechtsakte
- Stabilisierung ARF in diversen Bereichen
- Klarheit zur Signatur-Migration im nationalen Kontext
- Umsetzung Wallet

Wo A-SIT beiträgt

- Zertifizierung
- Signatur-Evaluierung
- Innovation

Vielen Dank.

Arne Tauber

arne.tauber@a-sit.at · a-sit.at