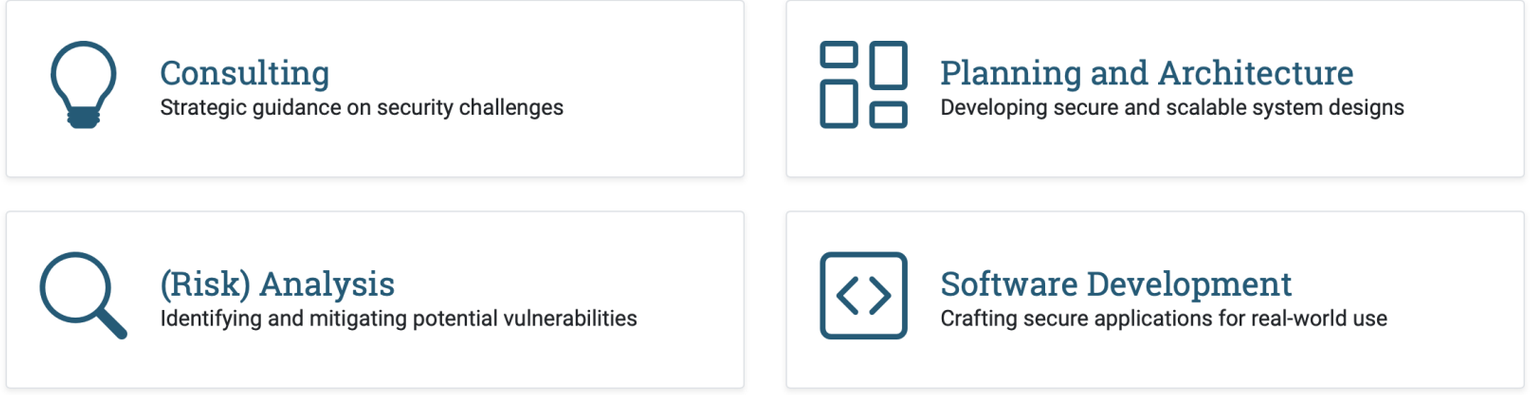
EUDI WALLET
An Austrian Perspective

Peter Teufl, A-SIT Plus GmbH

A-SIT/A-SIT PLUS – CORE TOPICS

Applied Cryptography, Cybersecurity, Consulting, Development

- https://plus.a-sit.at



Success stories:

- **2015-2016:** Cash Registers (specifications, cryptography) for the ministry of finance (BMF)
- **2019-NOW**: Consulting/Development for ID Austria/Ausweisplattform (“ID-card-platform”) (federal chancellery – BKA)
- **2021** Digital Green Certificate (Development for core components for creation and validation)
- **2021-2022** Digital ID Cards for pupils (Backend, Apps, Cryptography)
- **EUDI-Wallet (VALERA Wallet)**
  - Large Scale Pilot POTENTIAL: Results on https://wallet.a-sit.at
- **OSS** (Wallet, Attestation, etc.): https://github.com/a-sit-plus/

A-SIT

EUDI Wallet Challenges

LEGAL AND TECHNICAL COMPLEXITY

- Significant legal framework
- Technical protocol stack is still evolving
- Decoupled nature (issuing/presentation)
- Complex trust/revocation landscape
  - EAA (PID/PUB-EAA/Q-EAA/)… issuers
  - Wallet Issuers
  - Wallet Instances
  - Public/private RPs over Europe
- Certified components
- High security/privacy requirements

Commission Implementing Regulation (EU) 2024/2977 – Person Identification Data set and Issuance of Electronic Attestations of Attributes for the European Digital Identity Wallet,

Commission Implementing Regulation (EU) 2024/2979 – Integrity and Core Functionalities of the European Digital Identity Wallet,

Commission Implementing Regulation (EU) 2024/2980 – Procedures and Technical Specifications for Notification by Member States,

Commission Implementing Regulation (EU) 2024/2981 – Certification of the European Digital Identity Wallet and Related Services,

Commission Implementing Regulation (EU) 2024/2982 – Protocols and Interfaces Supported by the European Digital Identity Wallet,

Commission Implementing Regulation (EU) 2025/846 – Unequivocal Matching of a Person When Using the European Digital Identity Wallet,

Commission Implementing Regulation (EU) 2025/847 – Handling and Notification of Security Breaches Relating to the European Digital Identity Wallet,

Commission Implementing Regulation (EU) 2025/848 – Registration of Relying Parties Using the European Digital Identity Wallet,

Commission Implementing Regulation (EU) 2025/849 – Format and Procedures for Submission of Information on Certified European Digital Identity Wallets

VAST RANGE OF USE CASES WITH DIFFERENT REQUIREMENTS

ONE WALLET for

- KYC with/without ID-matching for X-Border, national use cases
  - Tax, eHealth, registering bank accounts, presenting the driving license
  - Identity Matching typically requires a central component
- Pseudonymous to anonymous
  - Online Shops, Age Verification, Tickets, etc.
- Proximity vs. Remote vs Supervised vs Unsupervised
  - Driving licenses, Identity Cards in proximity and remote versions, supervised vs unsupervised
- Different security/privacy requirements
  - Less protocol related privacy requirements for KYC use cases: e.g., holder key can be used multiple times
  - Other requirements for anonymous use cases
    - E.g., collusion problem with classic protocols for anonymous age verification use cases
    - holder key MUST not be reused
    - but less security requirements

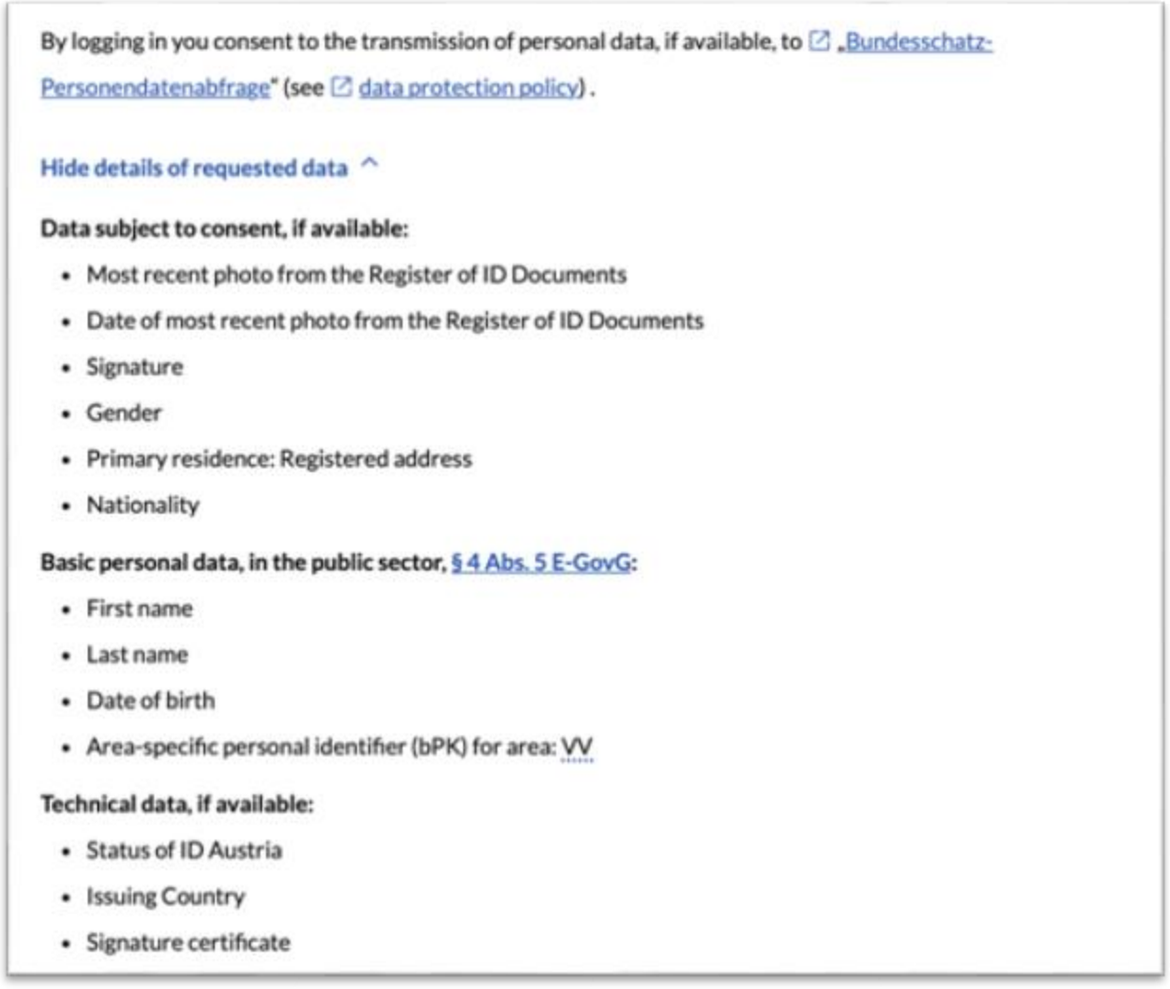
A-SIT

EXTENDING AND INTEGRATING INTO EXISTING SYSTEMS

for the Austrian landscape

- ID Austria
  - Central OIDC/SAML IDP
  - Attributes: basic, address, vehicle registrations, photo, gender, nationality …
  - Wide range of public/private relying parties (tax, bank registration, insurance, eHealth, qualified signature for every user)
- Ausweisplattform “ID-card platform”: driving license, vehicle registration, age verification, digital ID
- eIDAS1 incoming/outgoing
  - matching infrastructure
- **Challenge: Servicing the user/application base while transitioning to the EUDI-Wallet**

Highlighting existing attributes:
ID Austria Consent Screen for banking account registration at www.bundesschatz.at



By logging in you consent to the transmission of personal data, if available, to „Bundesschatz-Personendatenabfrage“ (see data protection policy).

Hide details of requested data

Data subject to consent, if available:

- Most recent photo from the Register of ID Documents
- Date of most recent photo from the Register of ID Documents
- Signature
- Gender
- Primary residence: Registered address
- Nationality

Basic personal data, in the public sector, § 4 Abs. 5 E-GovG:

- First name
- Last name
- Date of birth
- Area-specific personal identifier (bPK) for area: VV

Technical data, if available:

- Status of ID Austria
- Issuing Country
- Signature certificate

A-SIT

TRIANGLE SECURITY/PRIVACY/USER EXPERIENCE

- Strong requirements for **User Experience/Privacy/Security**
- Not possible to fulfill all of them and if the **user gets left behind there will be no adoption**
- Examples
  - Security vs Privacy
    - Requirements on cryptographic key storage: Remote PID Holder Keys vs. Tracing the user
  - Security vs UI/UX
    - Multi-factor authentication (including passwords) for mobile use cases in exposed environments for mobile use cases
  - Privacy vs UI/UX
    - Understandable privacy options (selective-disclosure, trust, logs on device, offline vs online use, anonymous vs. KYC clarity)
  - Security vs Security
    - Passwords vs biometric authentication (risks strongly depends on the environment)
    - Device vs. Device (latest device with strongbox requirements vs. unpatchable older devices)
  - Privacy vs. Privacy
    - No Identifier vs. PIDs that represent a unique hash

A-SIT

OTHER EXAMPLES

- Zero Knowledge Proofs
  - Especially important for anonymous use cases (collusion, tracing)
  - hardware, availability, PQC-ready?
- PID and Identifiers
  - no, maybe, yes, PID as unique hash (and thus a static ID)
- Revocation
- Showing of multiple credentials
  - Combining multiple EAAs with different holder keys and respecting usability/privacy/UX
- Different privacy impacts on protocols for different use cases
- PQC transition

EUDI Wallet
Austrian LSP Perspective

LSP-POTENTIAL LESSONS LEARNED – EXISTING SYSTEMS

Coverage for existing services

- ID Austria service providers (for non-AT users at least the KYC use cases)
- ID-card-platform and the current digital credentials (driving license, vehicle registration etc.)
- eIDAS1 incoming infrastructure

LSP approach

- Providing adapters for EUDI Wallets, which create bridges between the new wallet world and the existing systems
  - Non-AT users: At least for KYC cases and x-border ID-Matching
- Keeping existing proximity cases within the ID-card-platform until x-border use cases emerge
- Continuation of service (we MUST NOT assume that every service provider is able to switch from current protocols to eIDAS2 at 2026/12/24)

A-SIT

LSP-POTENTIAL LESSONS LEARNED – PRIVACY

Dealing with heterogenous use cases

- KYC public, KYC private, KYC with/without ID matching, pseudonymous, anonymous etc.
- Clearly define security/privacy properties for each use case (from anonymous to KYC with ID matching), multiple examples:
  - showing a PID with the same holder-key is fine, but it is a MUST NOT for anonymous age-credentials (tracing the user with the holder-key)
  - involvement of central systems is fine for e.g., public e-gov use case but a MUST NOT for a pseudonymous use case involving a private RP
  - Having classic cryptography for PID etc. is fine but not for age verification (e.g., collusion)

LSP-POTENTIAL LESSONS LEARNED – MULTIPLE FORM FACTORS

App Wallet as basis, but

- Need to have web-based solutions that do not require an app
- Mandatory for an inclusive system
- Cleary define for which use cases a web-based system is applicable (again: public e-gov service vs. anonymous age-verification)

LSP-POTENTIAL LESSONS LEARNED – ID MATCHING

eIDAS1 ID matching in Austria

- Central system, matching external users with existing Austrian identities or creating new identities on the fly
  - E.g., using the German E-ID to bind the ID-Austria/eAusweise Apps to load an Austrian driving license/vehicle registration

eIDAS2 matching

- Not fully clear yet, multiple paths need to exist:
  - Central matching for the bridge to existing systems (like eIDAS1)
  - Matching at PUB-EAA issuer for non-AT wallet users
  - Matching directly at selected RP categories
  - Matching for eIDAS1 remains in place

A-SIT

LSP-POTENTIAL LESSONS LEARNED – SECURITY

Multiple authentication factors

- server-verified password or similar (knowledge)
- possession of key/device (smartphone and app, or FIDO Token etc.)
- Local knowledge (PIN on device) or property (biometrics) that protect the possessed key

How to use those factors/security of the platforms

- Mobile use cases and environments: e.g., using the wallet in public transport with shoulder-surfing
  - where possible, extending cryptographically bound sessions so that not all factors are required every time
  - shifting to device only authentication where possible (e.g., biometrics for mobile use cases)
  - Giving the user the choice on authentication method (e.g., PIN vs biometrics for third factor)
  - No “central” factors, keys for privacy-relevant use cases (age verification etc.)
- Focus on a risk-based approach where possible, deactivating critical vulnerable devices, notifying the users on newly registered devices etc., providing clear recovery scenarios in case of attacks, vulnerabilities
- Technical: using the best possible options on current devices (hardware-based key elements, attestation mechanisms etc.)
- Web-based approach vs. app approach

A-SIT

User FIRST

EUDI Wallet Opportunities

OPPORTUNITIES

- Digital Ids are a core building block
  - for Digital Sovereignty
  - for digitalization
- Require a strong fundament
  - Core eGov infrastructure (authentic sources, interfaces for public/private applications)
  - European data processing/operations
  - Know-How and development: cryptography, privacy, security
  - Collaboration across Europe for x-border use cases, OSS solutions
    - Universities, companies, public sector …

Sources

SOURCES

- eIDAS2 VO: https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng
- POTENTIAL: https://www.digital-identity-wallet.eu
  - VALERA Wallet/Issuers etc.: https://wallet.a-sit.at
- ID-Austria and related (Ausweisplattform)
  - https://www.id-austria.gv.at/de
  - Tech Details: https://www.id-austria.gv.at/de/developer
- OSS A-SIT: https://plus.a-sit.at/open-source.html
  - WARDEN Supreme: https://github.com/a-sit-plus/warden-supreme
  - Attestation validation libraries, client code and documentation

A-SIT