EUDI Wallet

Peter Teufl, peter.teufl@a-sit.at

A-SIT / A-SIT Plus / ISEC

A-SIT/A-SIT PLUS/ISEC

- Located in Graz (at ISEC) and Vienna
  - https://www.a-sit.at
  - https://plus.a-sit.at
  - OSS: https://github.com/a-sit-plus/
- Strong collaboration with ISEC/Graz University of Technology
  - Group “Secure Applications” https://www.isec.tugraz.at/research-area/secureapplications/
- Core AT/EU e-gov technologies provided by the team in Graz

A-SIT AND PROJECTS (A-SIT PLUS SINCE 2015)

- RKSV (2015)
  (consulting, specification, demo code, validation)
- Grüner Pass (2021)
  (EU taskforce, code for validating/creating codes, apps)
- ID Austria (2015-)
  (core architecture, security, mobile security components)
- AWP (2021-)
  (consulting, security, specification)
- Schülerausweis (2022-2023)
  (issuing/signing documents, wallet/verification apps)
- Large Scale Pilot – POTENTIAL (2023-)
  https://wallet.a-sit.at


TAXI 878
Fahren ohne Grenzen.

ULBL Herbert
PFITZNERGASSE 3
8053 GRAZ
ATU27928106

Kennz: 3168 G 3168 TX
Kassa-ID: 01010-3168-0

QUITTUNG

Beleg	Trans	Zeit	Datum
3712	3314	20:02	12/07/17

	MWSt	Betrag
Fahrpreis 10%	10	21,60
B E Z A H L T (EUR):		21,60

MWSt	EUR	Netto	Brutto
10,00%	1,96	19,64	21,60

EUDI Wallet Brainstorming

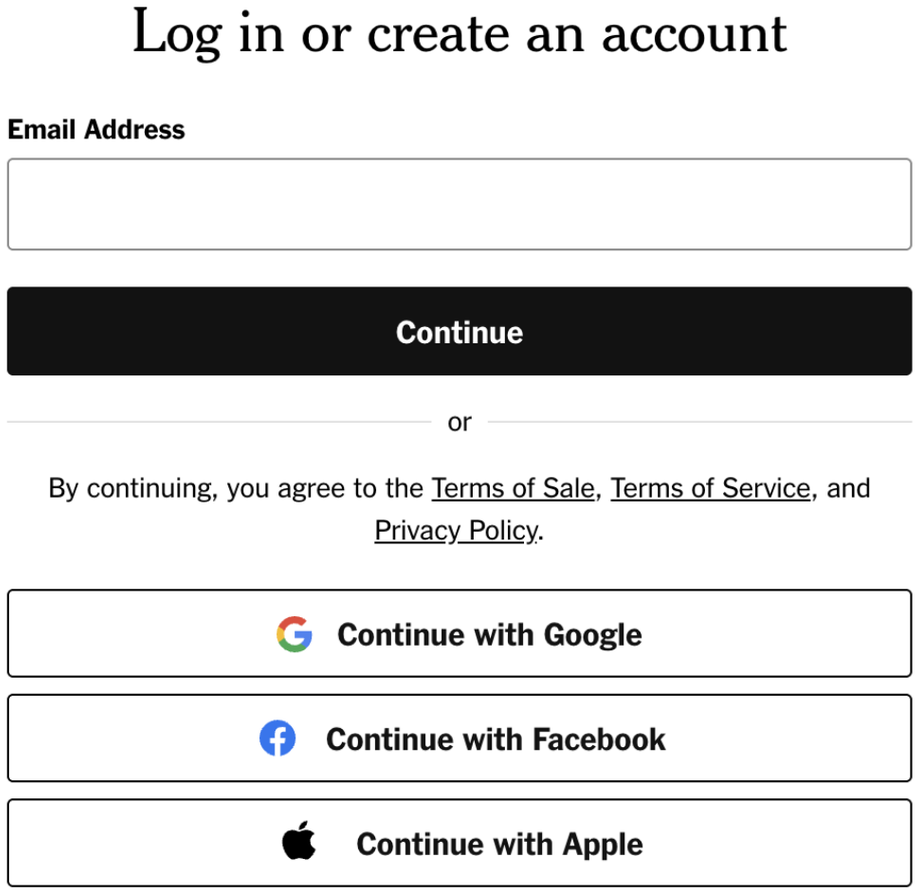
EUDI WALLET BRAINSTORMING

External …

Classic Central IDPs
&
Austrian Landscape

CENTRAL IDENTITY PROVIDERS (IDPS)

- Widespread IDPs are of central nature and based on OIDC
- Apple/Google/Meta/GitHub/Microsoft/…
- All have in common:
  - OIDC protocol stack (sometimes also SAML)
  - Central registry for applications and governance (guidelines, limits, possibility to revoke applications)
  - Auth providers, consent and information for the user
- ID Austria is one of those:
  - SAML/OIDC protocols
  - Governance: EU/Austrian Law
    - AT: eGovG
    - EU: eIDAS1 regulation



A-SIT

CENTRAL IDENTITY PROVIDERS (IDPS)

Summary

- Based on standards, well-known and established for private/public use cases
  - Many advantages for use cases due to central nature and widespread adaption: e.g., pseudonyms as used by Apple (together with hide-my-email)
  - Easy to implement dynamic/sector specific IDs
  - Easy to verify applications, provide security features due to central nature
  - …
- However, two main problems caused by the “central nature”
  - **Privacy**: The central system knows exactly which applications are used by the users (Profiling/Tracing).
  - **Offline** use is not possible; connection to the central system is required

EIDAS1

- Current European approach is eIDAS1:
  defines SAML based protocols for federated login with national IDPs
- System is of central nature and based on SAML (not yet adapted for OIDC)
- Core difficulty:
  - Identity Matching
  - Complexity, minimal use cases, only a minimum set of attributes
  - When a German User logins to an Austria Service Provider, the identity of the German User needs to be matched with existing Austrian records, or an entry needs to be created that is uniquely identifiable for subsequent logins

DEMO AND EXPLANATIONS

External…

- Service Provider Registration
  - https://eid.egiz.gv.at/anbindung/registrierung/registrierung-am-ida-spr/
- ID Austria Login demo with https://www.bundesschatz.at
  - Example highlights the use of multiple attributes
  - Important achievement, since bank accounts in Austria can be legally registered by using ID Austria (and the eIDAS1 infrastructure)

Ausweisplattform

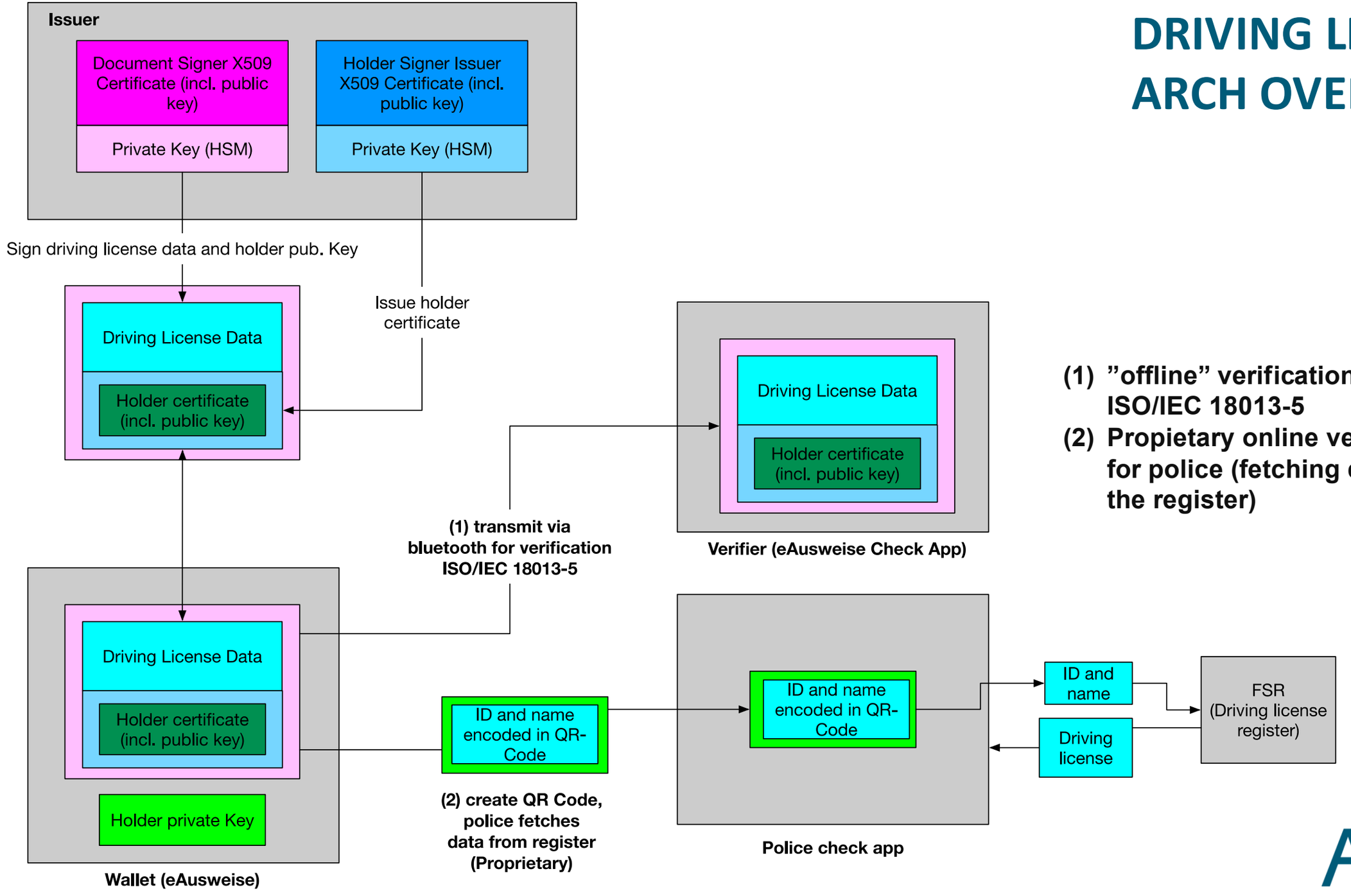
AUSWEISPLATTFORM – EXISTING AUSTRIAN DECENTRAL APPROACH

Ausweisplattform

- Austrian law allows to store the driving license, vehicle registration, age verification, and digital ID as Electronic Attribute Attestation (EAA, important term for EUDI Wallet) within the eAusweise App
- Offline/Proximity use case
  - Verifications of EAAs via eAusweise Check App (data transferred ”offline” via Bluetooth)
  - or for the police via a QR code that contains the required IDs to retrieve information from authentic sources
- **Core process**
  - Via ID Austria, a user can get data from authentic sources (registers), such as the driving license, vehicle registration, etc.
  - Data is stored (signed) according to ISO/IEC 18013-5 in eAusweise App
  - Presentation of data via Bluetooth to eAusweise Check App. To prove ownership of the signed document, the private holder key is used.
  - Verifier checks signature and possession of holder key (by letting the user sign a challenge with the holder key) and checks the revocation state of the EAA
- **Link:** https://www.oesterreich.gv.at/eausweise.html

A-SIT

DRIVING LICENSE ARCH OVERVIEW



(1) ”offline” verification via ISO/IEC 18013-5

(2) Propietary online verification for police (fetching data from the register)

AUSWEISPLATTFORM SUMMARY

- **Ausweisplattform** and its apps already use a decentral/offline capable approach
  - Already uses the ISO/IEC 18013-5 protocol stack, will also be used for EUDI Wallet
- **Current status**
  - Revocation due to legal constrains, privacy concerns and complexity
  - Currently only for proximity cases since remote/online cases not yet fully standardized (➔ EUDI Wallet)
  - TRUST and Security
    - e.g., remote attestation is used to limit eAusweise check app as verifier currently so that data cannot be misused by
    - no service provider registry yet (➔ EUDI Wallet)
  - No European governance/acceptance (➔ EUDI Wallet)

A-SIT

Towards the EUDI Wallet

TOWARDS THE EUDI WALLET

eIDAS2 regulation, main goals:

- Extend eIDAS1 use cases
  - Private, public, use-cases categories (remote/proximity),
    broader acceptance (banks, eHealth, driving license, private verifiers, etc.)
- Provide a decentralized solution, to achieve best-possible privacy
- Mandatory for member states (wallet issuing and acceptance)
- Establish trust/governance for the wallet
- Every wallet user needs to have access to a qualified digital signature
  (that is already in place for Austria for a long time, even though not mandatory within eIDAS1)
  - And standardize the way to sign documents (CSC standards)
- Align with other concepts (SDG etc.)
- Create/extend existing protocol stack for decentral use cases
  - ISO protocol family
  - OIDC VP, OIDC VCI
  - Verifiable Credentials, SD-JWTs

A-SIT

TOWARDS THE EUDI WALLET

- **eIDAS2 – legal aspects**
  - eIDAS2 regulation is already in force and mandates the issuing of the wallet for all member states by 24.12.2026
  - Implementing acts are still being released (legal documents that provide details for various aspects/components)
  - **eIDAS2 regulation**: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32024R1183
  - **Implementing act list**: https://www.eid.as/implementing-acts/

- **eIDAS2 – technical aspects**
  - Architecture Reference Framework (ARF) provides technical details (still work-in-progress)
    - https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/architecture-and-reference-framework-main.md
  - Large Scale Pilots (LSPs): various funded projects for creating prototypes and interop-tests for the various wallet implementations: core functions and use case specific aspects: e.g., eHealth, driving license, bank account registration, signature
    - POTENTIAL: https://www.digital-identity-wallet.eu
    - And others…

A-SIT

EUDI Wallet
Selected Topics

A-SIT

EUDI WALLET DIVE-IN

- Selection of important topics
  - (D1) Protocol stack
  - (D2) EAAs (PID/PUB-EAA/Q-EAA/EAA)
  - (D3) Issuing and presentation (decentral nature)
  - (D4) Selective disclosure
  - (D5) Relying parties/verifiers
  - (D6) Trust
  - (D7) Privacy

(D1) PROTOCOL STACK

External…

(a short overview compiled with O3 model of ChatGPT)

main idea is to give you an overview on the involved protocols

(D2) EAAS (PID/PUB-EAA/Q-EAA/EAA)

(EAA) Electronic Attestation of Attributes

- Protocol stacks: ISO/SD-JWT
  - Different formats, but same properties
    (issuing/presentation decoupling, selective disclosure, decentral trust model)
- PID/PUB-EAA/Q-EAA/EAA
  - Technically all the same, all are EAAs
  - Legally there are significant differences
    - **PID**: Personal Information Data, mandatory, special requirements
      can only be issued by dedicated PID-issuers
    - **PUB-EAA**: e.g., a driving license or an eHealth record,
      any attestation from a public authentic source. Signed by qualified seal
    - **Q-EAA**: an EAA, which is processed and signed by a dedicated trust-service-provider
    - **EAA**: any other EAA, that does not have high-quality requirements

A-SIT

(2) EAA?

- Consider an EAA as
  - a data structure with a unique ID and one or more attributes
  - E.g., for the PID:
    - urn:eu.europa.ec.eudi:pid:1
    - Attributes:
      - Name, date-of-birth, portrait etc.
  - The attributes of an EAA can be disclosed selectively (except, when there are legal requirements for mandatory release)

(2) EAA?

PID

- Legal: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202402977
- Technical (rulebook): https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/annexes/annex-3/annex-3.01-pid-rulebook.md

Others (from Valera, our LSP contribution)

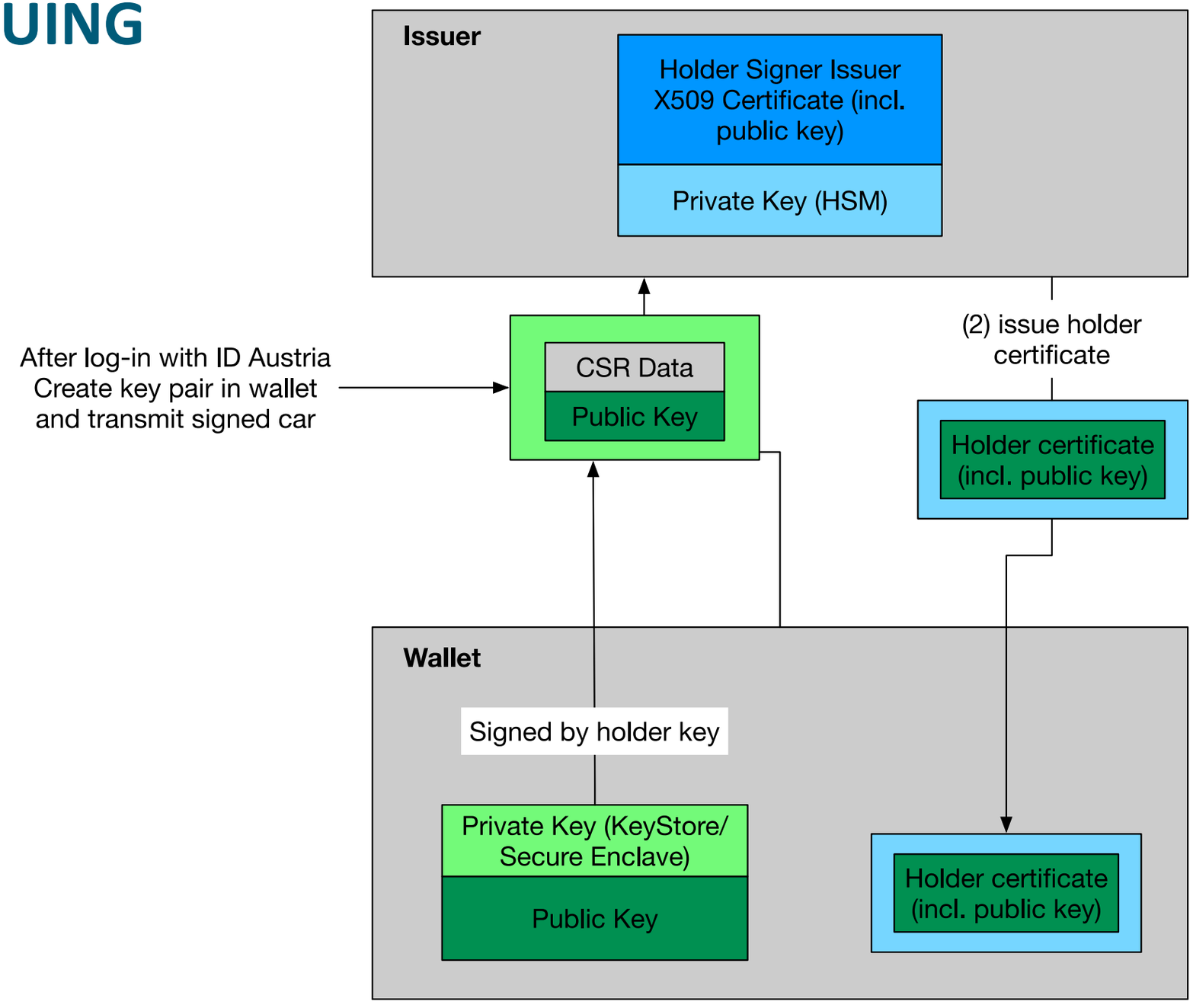
- https://github.com/a-sit-plus/credentials-collection

(D3) ISSUING AND PRESENTATION (DECENTRAL NATURE)

- Example from Ausweisplattform, but applies also to EUDI Wallet
- Focus on general process, not on specific protocol stack

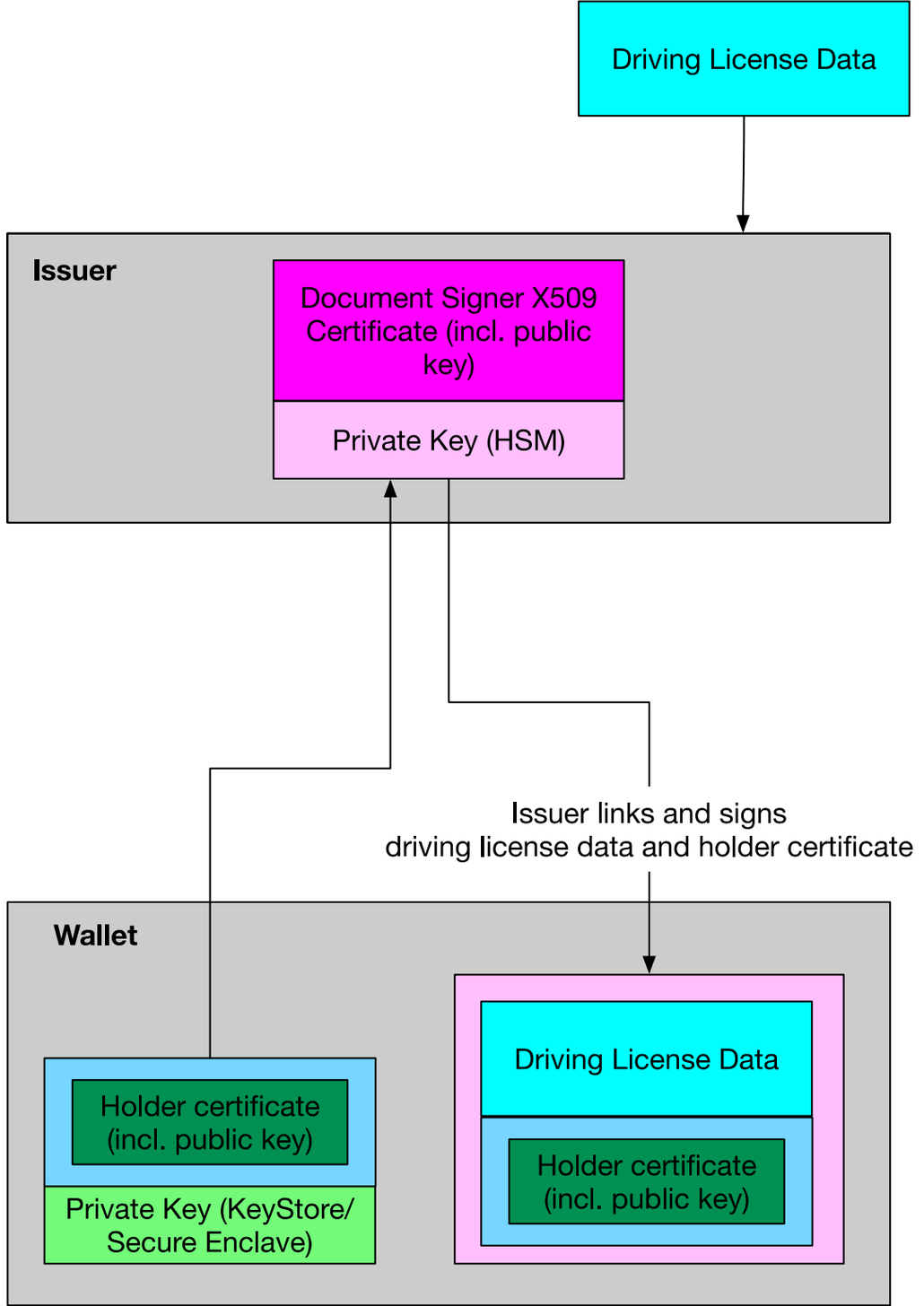
DRIVING LICENSE – ISSUING HOLDER CERTIFICATE

- eAusweise App connects to Backend and logs-in with ID Austria
- Key pair is generated within KeyStore/Secure Enclave
  - Attestation statement is generated
- CSR is signed by private key and sent to PKI
- PKI signs CSR and issues holder certificate which is stored in the wallet app
- App is ready for receiving the driving license

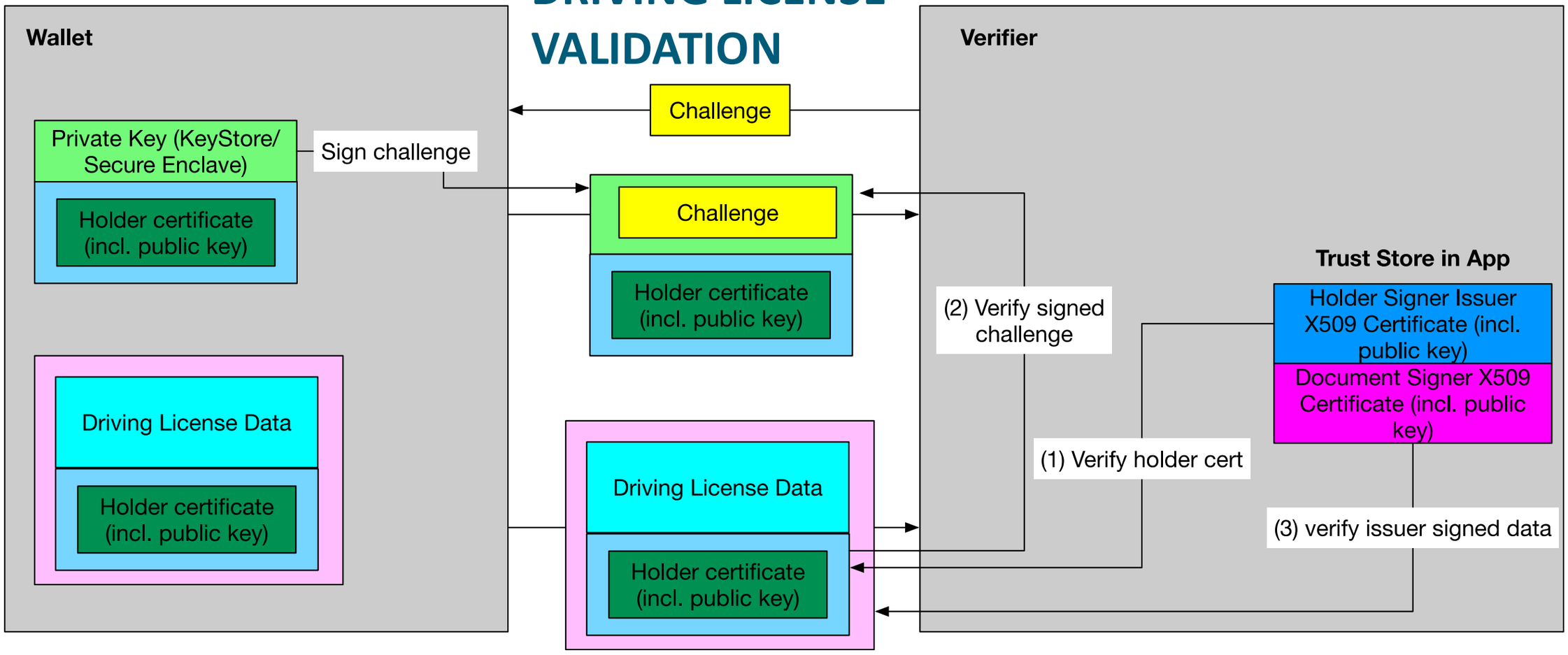


DRIVING LICENSE – ISSUING

- eAusweise App has a log-in session with the backend (e.g., initiated by ID Austria) and an issued holder certificate
- Driving license data is fetched from the authoritative source and bound to the holder certificate (by signing both in one structure)
- Data structure is transferred to the wallet app



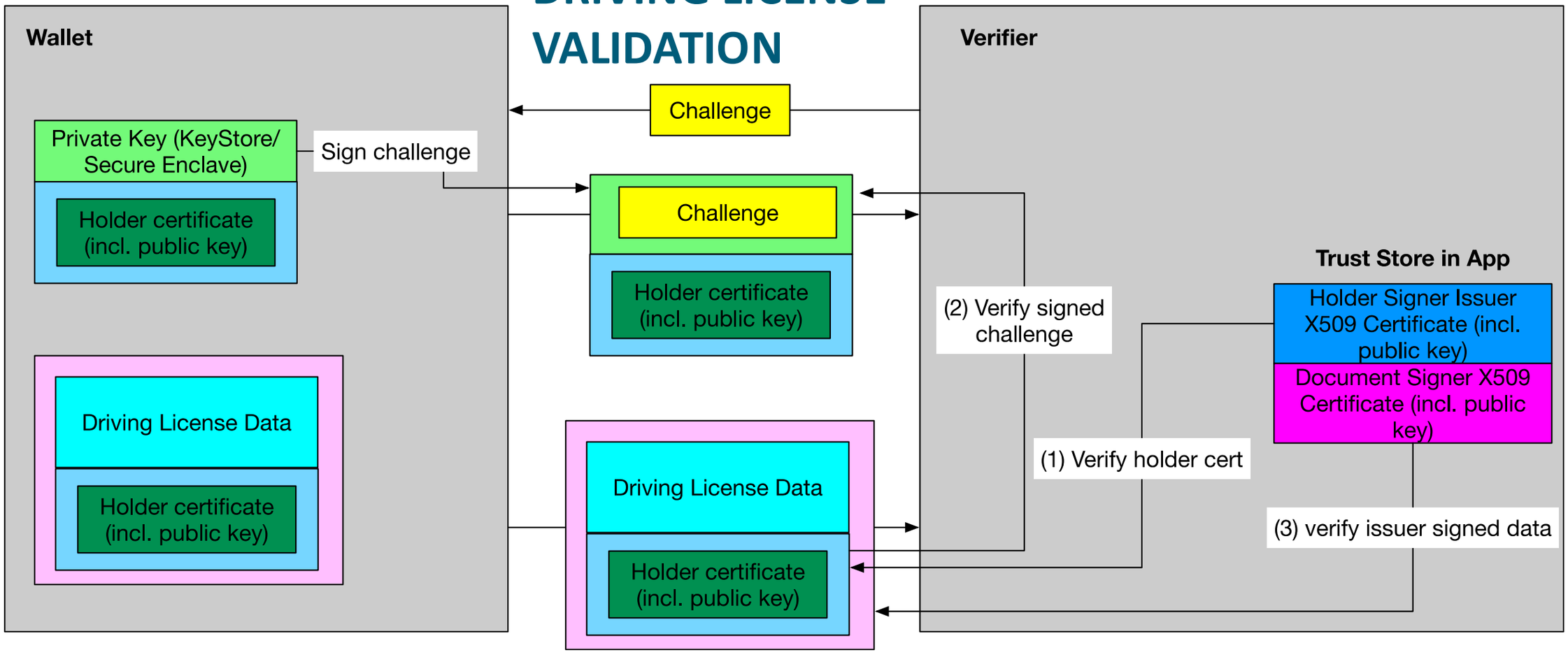
DRIVING LICENSE VALIDATION



- Verifier sends challenge to wallet app
- Wallet app signs challenge with holder certificate private key and transmits issuer signed data structure to verifier app
- Verifier extracts holder certificate from data structure, validates this with the Holder Signer Issuer certificate and then validates whether the challenge was signed with the corresponding private key (and if it is the same challenge as sent before)
- Verifier knows now that the holder defined during issuing currently presents the driving license

A-SIT

DRIVING LICENSE VALIDATION



- Verifier now validates the signed data structure with the document signer certificate
- If valid: verifiers knows that the other wallet app is the correct holder and that the driving license is valid (issued by a trusted issuer)

- Verifier still needs to check whether the checked person is the same as the one within the driving license (photo, real world)

A-SIT

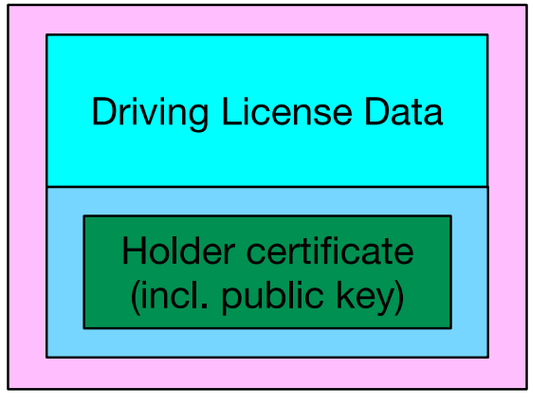
(D4) SELECTIVE DISCLOSURE

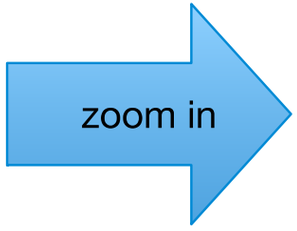
- EAAs typically multiple attributes (e.g., driving license), but not all attributes are required for all use cases (GDPR, other legal aspects, minimal data approach)

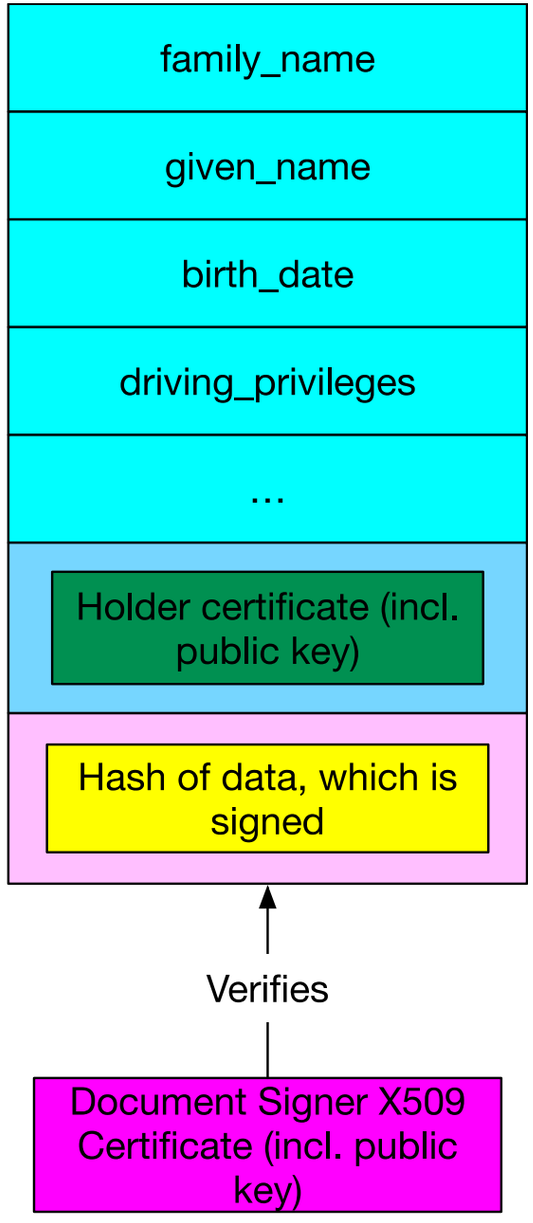
- Typical verifier approach:
  - Verifier sends requests for data to the user:
    - List of EAAs and the required attributes
    - User gets the list of requested data and is able to deselect attributes (selective disclosure)
  - Short demo with https://wallet.a-sit.at

A-SIT

ISO DATA STRUCTURE – ZOOM IN



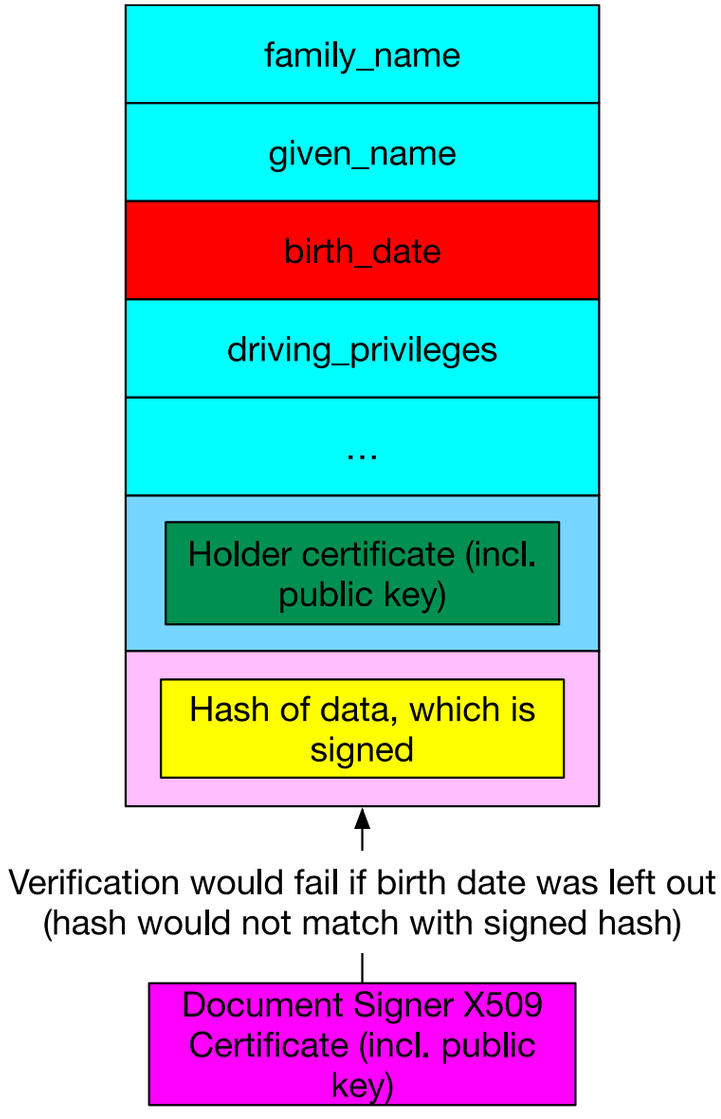




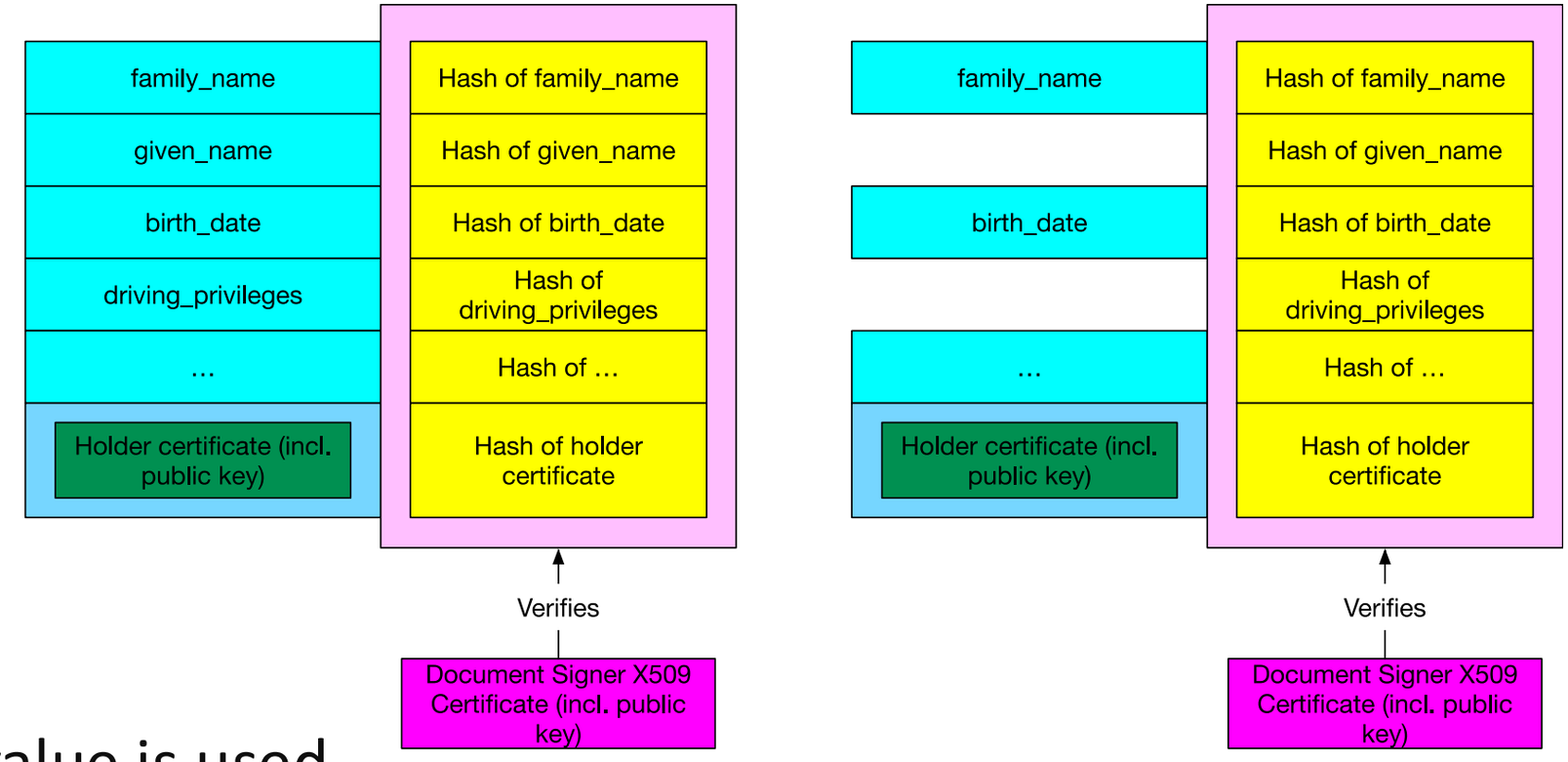
- How is the data encoded?
- For each element of the driving license there is a corresponding field in the data structure
- Current information within the slides:
  - Only the whole structure could be handed out
  - Selective disclosure of a subset of elements is not possible
- So, how does the ISO-standard achieve selective disclosure?

ISO DATA STRUCTURE – ZOOM IN

- Validation would fail when one or multiple elements would not be disclosed to verifier



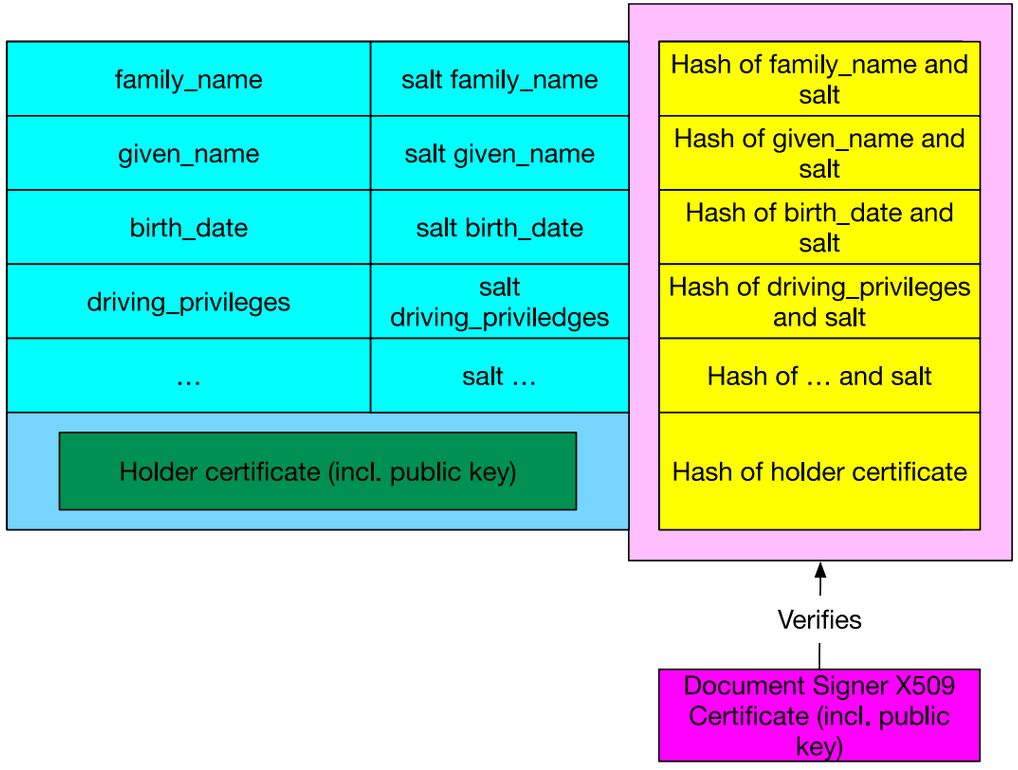
ISO DATA STRUCTURE SELECTIVE DISCLOSURE

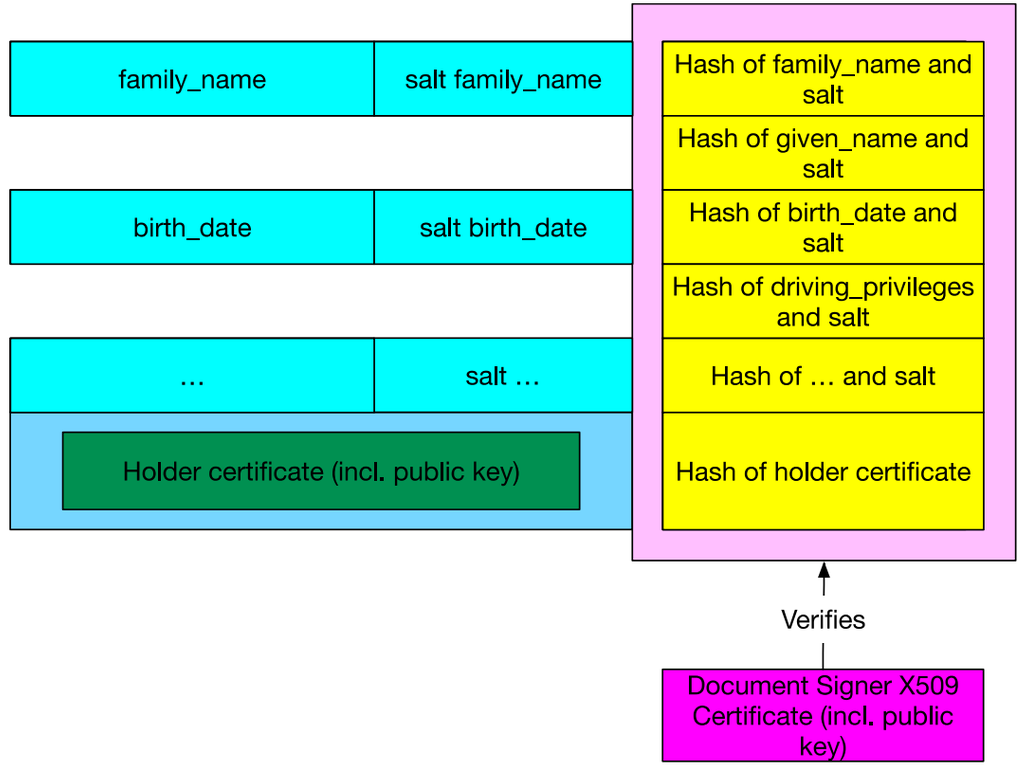


- Thus, not a single hash-value is used
  but each data element is hashed and the hash-table is signed
- Thus, we can remove single or multiple elements
  and the structure can still be validated,
  since the hash can be calculated for the single data elements
  and compared with the values in the signed hash-table

A-SIT

ISO DATA STRUCTURE – SELECTIVE DISCLOSURE





- Solved by adding a salt for each data element, which is hashed together with the data
- When we now remove elements (and their salt),
  the receiver cannot pre-calculate the hashes
  since salt values are not transmitted for “not-disclosed” elements
- For the transferred elements the salt is also transmitted,
  thus the verifier can calculate the hash correctly
  and find it (if not manipulated) in the signed hash-table

A-SIT

SELECTIVE DISCLOSURE EXAMPLES (DATA STRUCTURE)

- ISO encoded as CBOR/COSE (binary)
- However, same architecture here: SD JWT
  https://www.ietf.org/archive/id/draft-fett-oauth-selective-disclosure-jwt-02.html

Hash table which is transmitted,
hashes are calculated on value and salt


```
{
  "iss": "https://example.com/issuer",
  "sub_jwk": {
    "kty": "RSA",
    "n": "pm4bOHBg-oYhAyPWzR56AWX3rUIXp11_ICDkGgS6W3ZWLts-hzwI3x65659kg4hVo9dbGoCJE3ZGF_e
    "e": "AQAB"
  },
  "iat": 1516239022,
  "exp": 1516247022,
  "hash_alg": "sha-256",
  "sd_digests": {
    "sub": "z4xgEco94diTaSruISPiE7o_wtmcOfnH_8R7X9Pa578",
    "given_name": "PvU7cWjuHUq6w-i9XFpQZhjT-uprQL3GH3mKsAJl0e0",
    "family_name": "H-Relr4cEBMlenyK1gvyx16QVpnt4MEclT5tP0aTLFU",
    "email": "ET2A1JQLF85ZpBulh6UFstGrSfR4B3KM-bjQVllhxqY",
    "phone_number": "SJnciB2DIRVA5cXBrdKoH6n45788mZyUn2rnv74uMVU",
    "address": "0FldqLfGnERPPVDC17od9xb4w3iRJTEQbW_Yk9AmnDw",
    "birthdate": "-L0kMgIbLXe3OEkKTUGwz_QKhjehDeofKGwoPrxLuo4"
  }
}
```


Release (data and salt), elements can be omitted, verifier is still able to calculate hash values from salt/data and compare them with signed hash table


```
{
  "sd_release": {
    "sub": "[\"2GLC42sKQveCfGfryNRN9w\", \"6c5c0a49-b589-431d-bae7-219122a9ec2c\"]",
    "given_name": "[\"eluV5Og3gSNII8EYnsxA_A\", \"John\"]",
    "family_name": "[\"6Ij7tM-a5iVPGboS5tmvVA\", \"Doe\"]",
    "email": "[\"eI8ZWm9QnKPpNPeNenHdhQ\", \"johndoe@example.com\"]",
    "phone_number": "[\"Qg_O64zqAxe412a108iroA\", \"+1-202-555-0101\"]",
    "address": "[\"AJx-095VPrpTtN4QMOqROA\", {\"street_address\": \"123 Main St\", \"loca
    "birthdate": "[\"Pc33JM2LchcU_lHggv_ufQ\", \"1940-01-01\"]"
  }
}
```

(D5) RELYING PARTIES/VERIFIERS

- RPs need to be registered before they can request data
  (and thus, are trusted by the wallet)
- For ID-Austria such a system is already in place
  by having the legal and technical framework
  (technical reqs. comparable to Google/Apple etc., however governed by law)
- Main purpose: verify the legality of RPs, but even more important:
  being able to deactivate RPs when misuse is detected (by having a legal basis to act)
- Interesting aspects:
  - RP registries need to provide APIs so that data can be extracted via public access
  - allows for independent monitoring of RPs, the requested data and misuse

(D6) TRUST

- Complex and in-depth topic
- Trust changes significantly due to the decentral nature
  - Central systems do not verify the verifiers, but the local wallet is responsible
  - Trust needs to be established for many components
    - Issuers (Signers of the EAAs)
    - Wallets themselves
    - Relying Parties (also offline)
    - Revocation Lists
    - Qualified Signatur Providers
  - Technically there is a simple answer: PKI,
    but on a large scale getting the whole trust model in place
    and cover every member state will be a significant challenge
  - Establishment of technical/legal/org processes within the EU

A-SIT

(D7) PRIVACY

Privacy Issues? We are decentral, so everything is solved…?
NO! The complexity increases and many mistakes can be made!

Examples:

- Tracing when having anonymous use cases (e.g., age verification)
- Collusion between issuers and verifiers
- Combined presentation
- Identity Matching for public use cases
- IDs are BAD, that’s why we have the ultimate Hash (called the PID)
- KYC vs. pseudonyms vs. anonymous use cases
- Revocation

Outlook
Austria / EU

LSP (LARGE SCALE PILOT)

- A-SIT/BRZ/BKA
  - LSP – Potential
    - Valera is our contribution: wallet, verifier, issuer
    - Very successful within Europe, many interop tests
    - OSS
      - https://wallet.a-sit.at
      - https://a-sit-plus.github.io
  - However
    - LSP covers only a part (wallet/issuer/verifier)
      other things are missing: trust, in general revocation, RP-registries
    - Contributions of us and other are not ready for productive use
    - Focus on protocols and prototyping,
      but not on the integration in national infrastructure

A-SIT

ID-AUSTRIA/AWP/WALLET/NATIONAL REQUIREMENTS

- Need to consider current Use Cases and infrastructure
  - ID Austria, OIDC infrastructure and governance, used by all Service Providers
  - Wallet protocols would require a complete change of the procotol stack, thus there need to be proxies etc. (eIDAS2 covers such aspects)
  - AWP is decentral in nature, however there are also different use cases not yet covered by the EUDI wallet (also there is currently no European legal basis for MDL EAAs, or vehicle registrations etc.)
  - ID Matching gets much more complicated due to the decentral nature
  - eIDAS1 infrastructure and use cases need to be covered (for whole Europe not only for Austria)
  - Many technical changes, standards not ready etc.

SUMMARY…

The next years?