SSI and PKI – enabling attribute attestations

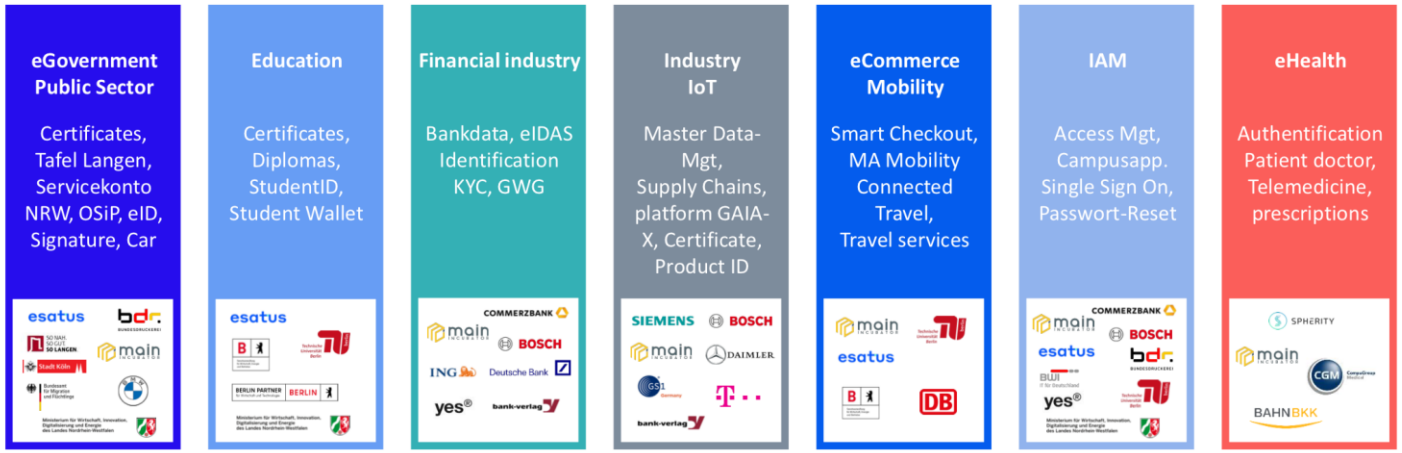
- 18.10.2023
- Vienna, 15. CA- DAY
- Christian Seegebarth Business Development - D-Trust/IDunion

The IDunion consortium is led by 15 consortium partners

Konsortialpartner

main INCUBATOR | bdr BUNDESDRUCKEREI | Technische Universität Berlin | BOSCH | esatus
yes® | SIEMENS | DB | Stadt Köln | bank-verlag
ING | T LABS | ifis internet-sicherheit. | GS1 Germany | SPHERITY

In total, we are working on 35 use cases in the areas of eGovernment, education, finance, industry/IOT, eCommerce/mobility, IAM, and eHealth



Struktur of the „new" eIDAS Regulation

Current structure

Chapter I – General provisions

Chapter II – Electronic Identification

Chapter III – Trust Services

- Section 1 General provisions
- Section 2 Supervision
- Section 3 Qualified Trust Services
- Section 4 Electronic Signatures
- Section 5 Electronic Seals
- Section 6 Electronic time stamps
- Section 7 Electronic registered delivery services
- Section 8 Website authentication

Chapter IV – Electronic documents
Chapter V – Delegations of powers and implementing provisions
Chapter VI – Final provision

New structure

Chapter 1 – General provisions

Chapter II – Electronic Identification
Section I Electronic identification (European Digital Identity Wallet)
Section II Electronic Identification schemes
Section III Cross–border reliance on electronic identification means

Chapter III – Trust Services

- Section 1 General provisions
- Section 2 Supervision
- Section 3 Qualified Trust Services
- Section 4 Electronic Signatures
- Section 5 Electronic Seals
- Section 6 Electronic time stamps
- Section 7 Electronic registered delivery services
- Section 8 Website authentication
- Section 9 Electronic attestations of attributes
- Section 10 Qualified electronic archiving services
- Section 11 Electronic ledgers

Chapters IV, V, VI
ANNEX V – Requirements for Electronic Attestations of Attributes
ANNEX VI – Minimum List of Attributes

Source: DG CNECT at European Signature Dialog 21 Juni 2021

Definition

- Serves as proof that an electronic document was issued by a legal entity and proves the integrity and origin of the document
  - ✗ Replaces the personal signature
  - ✓ Proof of origin

Types

- Advanced electronic seal (eIDAS Art. 3 Abs. 26)
- Qualified certificate for electronic seal (eIDAS Art. 3 Abs. 30)
- Qualified electronic seal (eIDAS Art. 3 Abs. 27)
  (Difference: secure seal creation device)

Technical Implementation

- Softoken/ smart card / remote seal creation

Legal effect

- An electronic seal shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic seals.
  (eIDAS Art. 35; Abs. 1)
- A qualified electronic seal shall enjoy the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked.(eIDAS Art. 35 (2))

When will QEAA reach legal effect – a rough estimate

- At the moment there are three drafts in discussion in the trilogue (The trilogue started March 2023)
- eIDAS 2.0 will be adopted by December 2023
- Implementing Acts will be designed probably up until the end of 2024
- National Legislation must be adjusted (e.g. Vertrauensdienste Gesetz in Germany) by the end of 2025?
  E.g. automated access to authentic sources
- Technical Laws must be adjusted in the years that follow

-> there won't be a QEAA available before the End of 2026 or Early 2027

In parallel some more processes must be implemented:

A certification needs standards; the EUDI Wallet Architecture Reference Framework (ARF) must have a useful maturity level.

As well, Certification Audit Bodies and National Accreditation Bodies (NAB) must be empowered (e.g. the DAkkS in Germany)

All together we will probably see QEAAs in 3 to 4 years

Two phase model

1. Phase – qualified sealed Verifiable Credentials (qVC) are possible today

Verifiable Credentials can be sealed according **eIDAS Art. 3 Abs. 27.**

The necessary technology is readily available in the market e.g., qualified seal cards, sealing servers, and remote sealing services.

Advantage: **The identification and validation of the issuer of every credential is possible**.

This is available for all EAAs and VCs and expands the trust model above and beyond QEAAs

For all the above mentioned cases: only the hash value of the credential will be transferred and sealed

Signature formats are mentioned in the Commission Decision EU 1506/2015:

ASN.1: CAdES (EN 319 122-1 and 2) builds on CMS IETF RFC 5652.

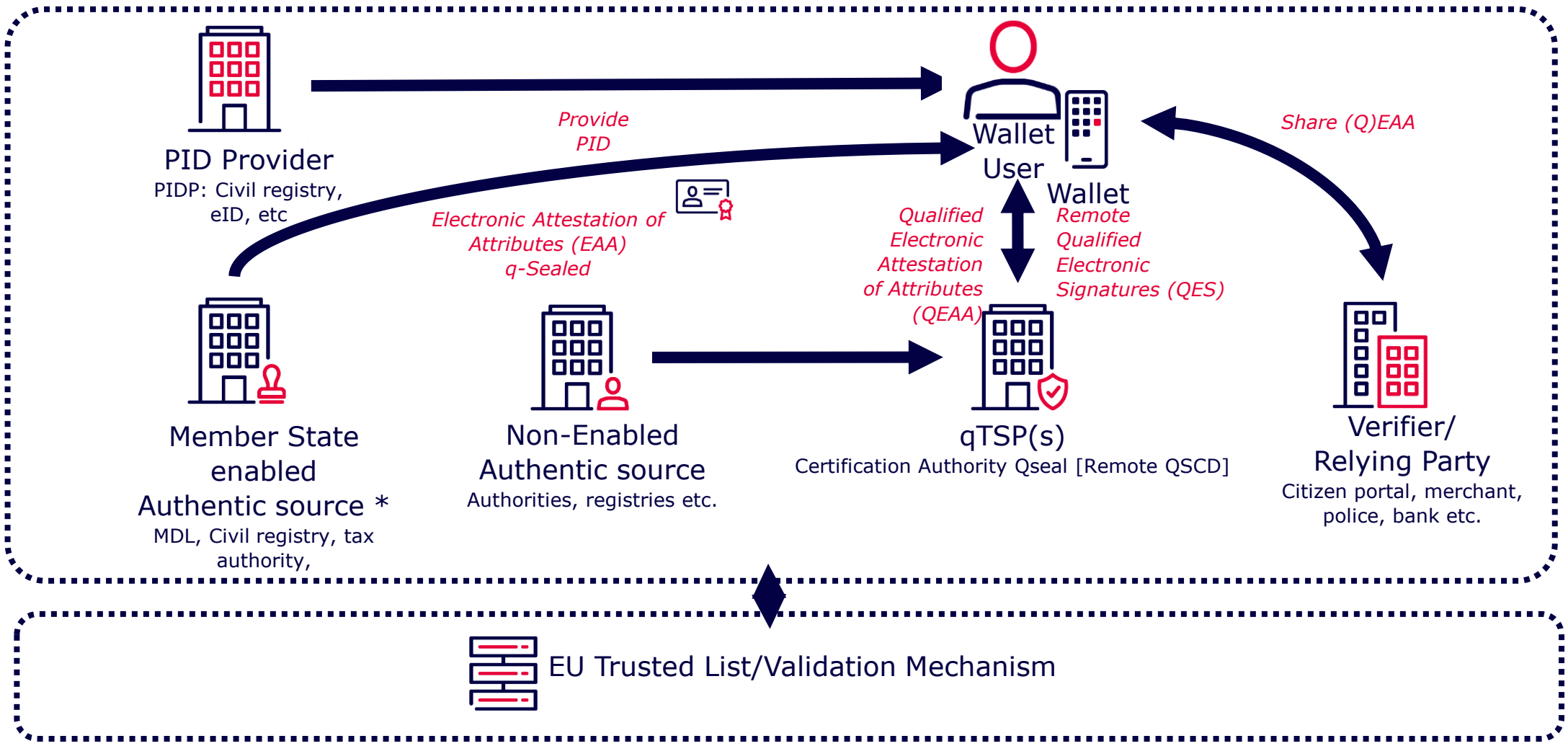
JSON: JAdES (TS 119 182-1) builds on JWS IETF RFC 7515

PDF: PAdES (EN 319 142-1 and 2) builds on PDF signatures

XML: XAdES (EN 319 132-1 and 2) builds on W3C XML signatures

2. Phase from 2027/28

QEAAs will are available and provide their legal effect. eIDAS 2.0 will be expanded upon by national technical law



*Articel 45d(a) & Articel 3 (45a) eIDAS proposals of the council (General approach)

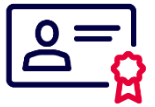
Terms

EAA Authentic Source

- E.g. drivers license, tax number etc. under control of the Member State.
- Member State notifies service to the EU (eIDAS proposals of the council - General approach)

QEAA Trust Service Provider

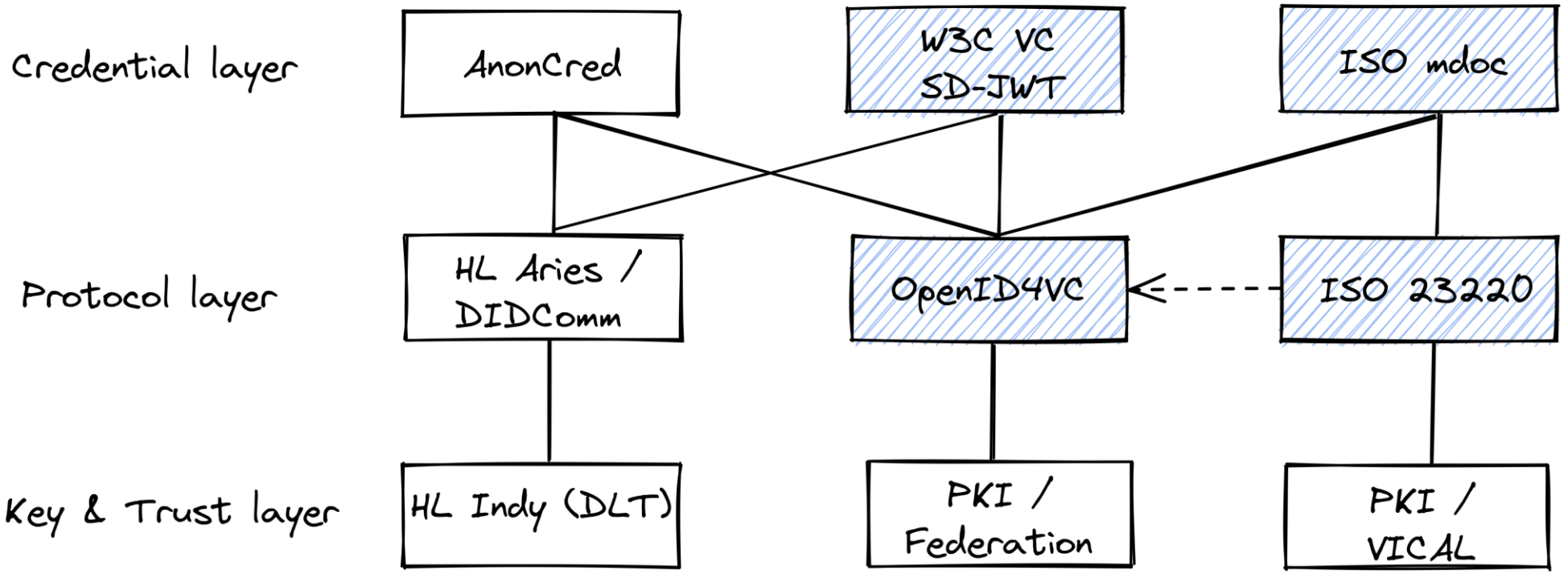
- Annex IV der eIDAS 2.0, QEAAs shall develop the same legal effect as original documents



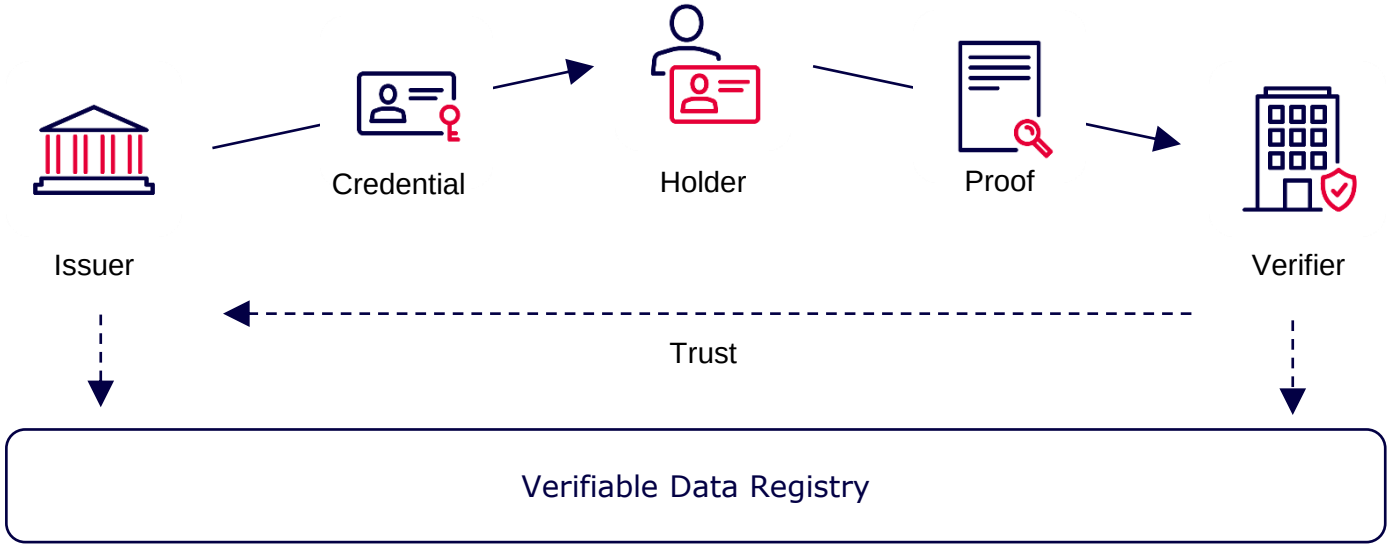
qVC Issuer

- Recommendation, creates more trust in the issued credential, due to the provided proof of origin

Evolution of the IDunion TechStack towards eIDAS 2.0

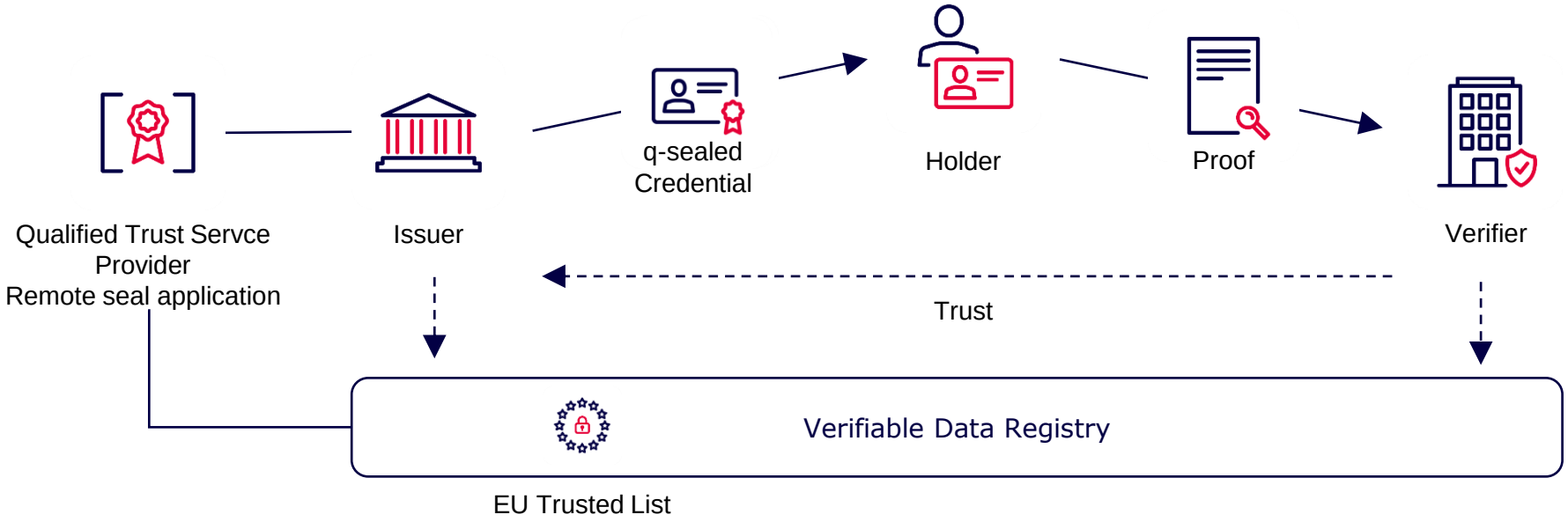


Roles and trust model in the SSI world



- Roles in the SSI-ecosystem: Issuer, Holder and Verifier
- IDunion Techstack 2.0: OpenID4VC protocol and SD-JWT credential-formats (eIDAS 2.0 / ARF 1.0)

Legal Security via Sealed Credentials



Process

1. Issuer issues sealed credential using remote sealing service
2. Holder presents Issuer-sealed credential
3. Verifier validates issuer of the seal against the EU Trusted List and seal against OCSP

Advantage

- Todays legal effect according to eIDAS 1.0 Art. 3 Abs. 27 and eIDAS Art. 35 (2)
- Full compatibility SD-JWT nach eIDAS 2.0 / ARF 1.0 and JAdES-Signature according to ETSI Standard
- Credential contains identity
- Verifier can check EU Trusted List
- No DLT necessary

Schematic depiction of a qualified sealed verifiable credentials

Verifiable Credentials as JSON / SD-JWT (see eIDAS ARF 1.0)

Signature according to JAdES Standard (ETSI TS 119 182-1) (here AdES-BASELINE-B Profile)

Header


```
{
 ”alg": ”ES256",
 ”cty": ”vc+sd-jwt",
 ”x5c": ”0bsadasdf ….",
 ”sigT": "2023-04-04T17:28:15Z",
}
```


Qualified seal contains the Identity of the issuer validated against the EU Trusted List

Payload

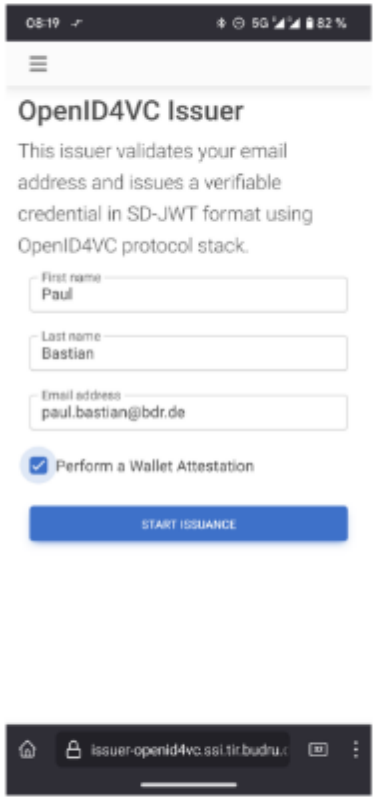

```
{
 "iss": "https://issuer-openid4vci.tir.budru.de”,
 "type": ”VerifiedEmail",
 ”iat":  1681397970,
 ”exp": 1682261970,
 ”first_name": ”Erika",
 ”family_name": ”Mustermann",
 ”email": ”openid@demo.de",
 "cnf": {
  "jwk": {
   "kty": ”EC",
   ”crv": ”P-256",
   ”x": "cPgUu7pKEzETXU22203qwO-trNqC5cAhvCkII9keYOk “
   ”y": "7g7SmlAipbGVVxn8AH6t0NGWS3Nkna7tgekL2esHgTg “
  }
 }
}
```


Signature


```
ZGFzaXN0a2VpbmVlY2h0ZXNp
Z25hdHVyMWRhc2lzdGtlaW5lZ
WNodGVzaWduYXR1cjJkYXNpc
3RrZWluZWVjaHRlc2lnbmF0dXI
zZGFzaXN0a2VpbmVlY2h0ZXN
pZ25hdHVyNQ==
```

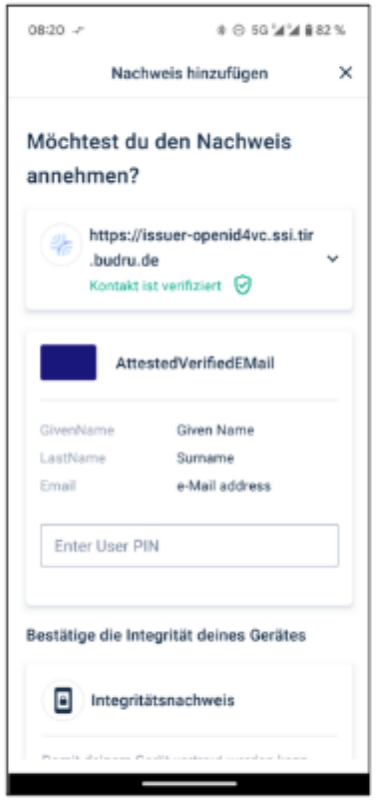

Qualified Seal of the issuer

Demo of End-to-End Issuance with Wallet Attestation and Device Binding



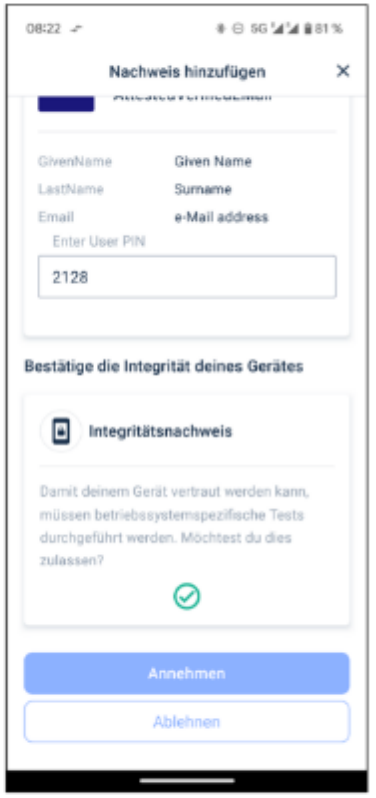
issuer's website as a starting point

Wallet invocation with deeplink or QR-Code



Issuer Authentication with eIDAS 1 QWAC or EV certificates

UserPIN as a security feature of OpenID4VCI



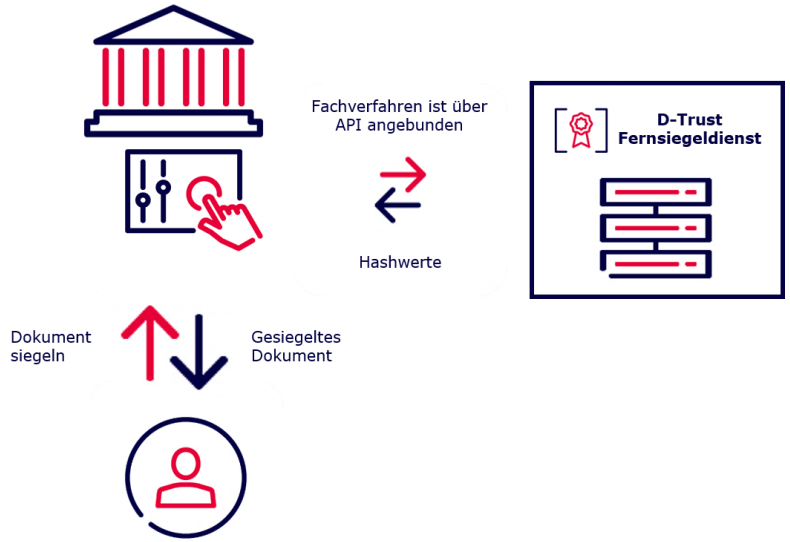
Wallet Attestation for eIDAS Type-1 high assurance credential

W3C SD-JWT VC issued after validation of wallet attestation

What is necessary

Connect the issuer software or wallet to a qualified seal creation device:

- Sealing smart card operated by issuer
- Sealing Server operated by issuer
- Remote sealing service of a qTSP



The qTSP operates the sealing device for the issuer

In all three cases only transport of the hash value is necessary

The wallet can validate the seal against EU Trusted List and OCSP

Commission Implementing Decision (EU) 2015/1505 -> ETSI TS 119 612

Christian Seegebarth
Senior Expert Trusted Solutions
D-Trust GmbH
E-Mail: christian.seegebarth@bdr.de

Teil der Bundesdruckerei-Gruppe

Trust Services as presented in the eIDAS Regulation ensure Security and Transparency in the Digital World

Electronic Signature
Individual digital
signature

Electronic Seals
Reliable digital stamp
for government agencies and companies

Time Stamp
Official time as with an
electronic photo ID

Website Certificate (QWAC)
Secure identification
of a website operator

Registered Delivery Service
Secure digital messages just like with
the post office or bailiff

Validation Service
The automatic independent checker

Qualified Preservation Service
The permanent digital archive