QEAAs in der eIDAS 2.0:
Revival für die Verbindung
aus PKI und Attributen

eIDAS 2.0 Proposal der EU-Kommission

80% der EU Bürger sollen 2030 Zugang zur European Digital Identity Wallet haben.

Mitgliedstaaten müssen **Bürger (und Unternehmen)** mit einer eID und einer EUDI Wallet ausstatten. Nur Staaten (oder in deren Auftrag) dürfen Identitäten herausgeben.

Die EUDI Wallet soll Bürgern die Wahl geben, welche Aspekte (Attribute) ihrer **Identität, Daten und Zertifikate** sie mit Dritten (Behörden und Private) teilen.

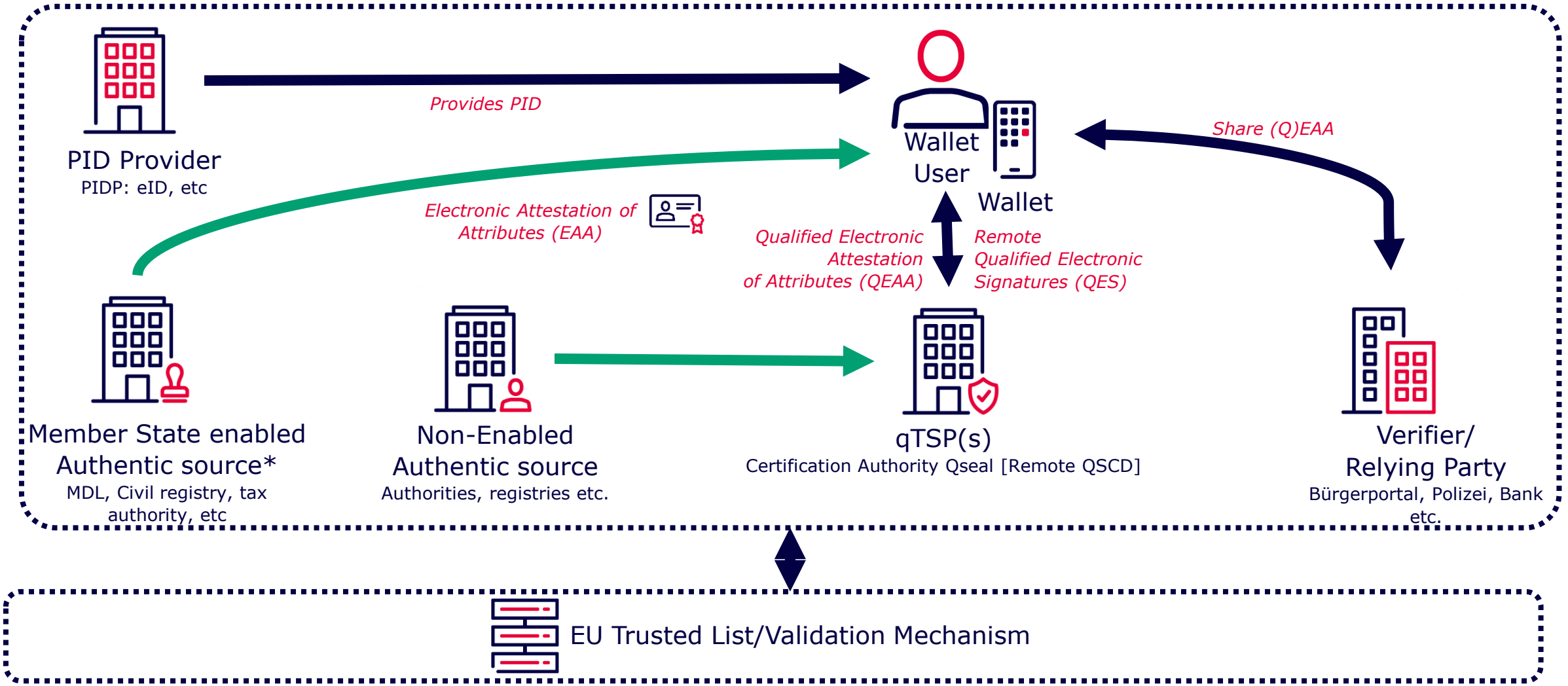
Dazu werden die **Vertrauensdienste** insbesondere um die qualifizierte Attestierung elektronischer Attribute (**QEAA**) ergänzt.

EUDI Wallet

- Online und Offline Funktionalität
- Vertrauensniveau hoch
- QEAA, QES und Q-Siegel Funktionalität

Technische Vorgaben werden durch das Architecture Reference Framework (ARF) definiert.

eIDAS 2.0 Architektur Überblick – *Basierend auf EU Wallet Architecture Reference Framework (ARF)*

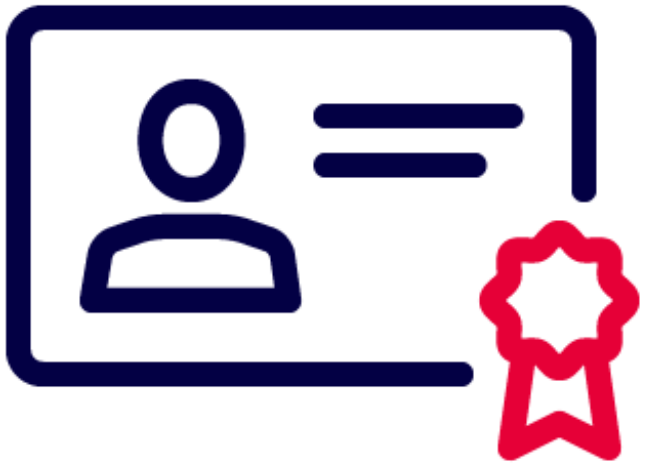


*Artikel 45d(a) des eIDAS-Proposals

Was macht ein QEAA aus?

Kryptographische Sicherung der Attributsdaten, die durch einen eIDAS konformen Antragsprozess geprüft und validiert werden…

…in Zukunft vor allem die Attribute des eIDAS 2.0 Entwurfs Anhang VI anhand der Anforderungen aus Art. 45b ff. iVm Annex V eIDAS-Entwurf.



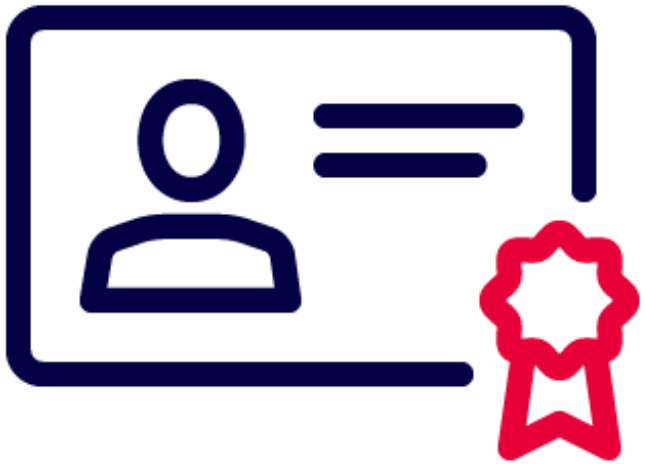
Artikel 45d

Member States shall ensure that measures are taken to allow qualified providers of electronic attestations to verify by electronic means at the request of the user, the authenticity of the following attributes against the relevant authentic source at national level or via designated intermediaries recognised at national level, in accordance with national or Union law and in cases where these attributes rely on authentic sources within the public sector:

1. Address
2. Age
3. Gender
4. Civil status
5. Family composition
6. Nationality
7. Aducational qualifications, titles and licenses
8. Professional qualifications, titles and licenses
9. Public permits and licenses
10. Financial and company data

Welche Anforderungen muss ein QEAA erfüllen?

- Kann nur von einem **qualifizierten Vertrauensdienst** (QTSP) ausgestellt werden
- **Identifizierung** des Nutzers auf qualifiziertem Niveau (in der Regel durch PID)
- Verifiziert über eine Schnittstelle zum relevanten staatlichen Register -> **Pflicht des Mitgliedsstaates zur Schaffung der Schnittstelle**
- Einhaltung von **organisatorischen Maßnahmen** (Datentrennung, separate Einheit)
- Einhaltung **formaler Anforderungen an den Datensatz** (Nutzerdaten, Ausstellender QTSP, Gültigkeit, etc)
- **Siegelung** des Datensatzes durch den QTSP



Wie läuft die Ausstellung eines QEAA generell ab?

1. Antragssteller wendet sich an QTSP
(über Endanwendung, Wallet, etc.)

2. **Qualifizierte Identifizierung** des Antragsstellers gem. Art 24 Abs. eIDAS
(eID, EUDI, QES, QSeal, Handelsregister etc.)

3. Validierung des Attributs durch den QTSP
(durch Identifizierung, automatisierte **Registerabfrage über eine Registerschnittstelle**)

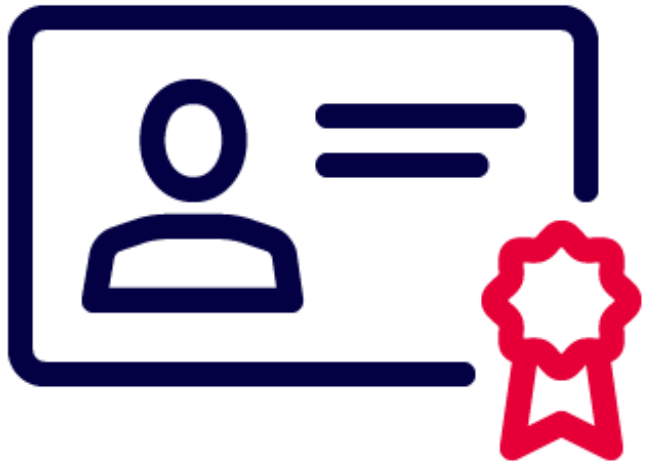
4. Sicherung des Attributs durch den QTSP gem. gesetzlichen Anforderungen und **anwendbaren Standards**
(W3C, mdl, etc.)

5. Ausgabe des QEAA
(über **Wallet-schnittstelle**, an Antragsteller oder Endanwender)

EAA über eine autorisierte öffentliche Stelle

- Aus dem Ratsentwurf der eIDAS 2.0 (Art. 45 da)
- An sich “nur” EAA, aber im Beweiswert gleichgestellt
- Insbesondere für wichtige Attribute gedacht, z.B. Führerschein, Reisepass etc

- Folgende Voraussetzungen:
  - Entsprechende Einhaltung der QTSP-Vorschriften
  - Signatur/Siegelung des Datensatzes mit QES/QSeal
  - Regelmäßige Prüfungen der autorisierten Stelle (Audits)
  - Notifikation der autorisierten Stelle an EU-Kommission



Einsatzmöglichkeiten

Potential der Digitalisierung aller öffentlichen Nachweise und Erlaubnisse vom Schulzeugnis über die Heiratsurkunde bis hin zum Angelschein

- Einreichung von QEAA als Ergänzung von Registerabfragen im digitalen Verwaltungsverfahren
- Schaffung einer digitalen Organisations-ID
- Digitalisierung von Prozessen, in denen bisher Originaldokumente (oder beglaubigte Kopien) erforderlich waren
- Im Unternehmensbereich: Know your customer und Complianceprozesse

Wie grenzen sich QEAA von anderen Möglichkeiten zur Abbildung von Attributen ab?

Attribute in Zertifikaten	Gesiegelte elektronische Dokumente	**QEAA**	SSI-Credentials	Nachweise in geschlossenen Systemen (Nutzerkonten)
+ Standardisiert	+ Standardisiert	+ Standardisiert	+ Dezentralität und vermeintliche Selbstbestimmung	+ Hohe Behördensouveränität
+ Etabliert	+ Einfach einsetzbar	+ Verknüpfung mit EUDI	+ Keine Übersiegelung nötig	+ OZG-Konform
+ Maschinenlesbar	+ Immer mehr in Praxis eingesetzt	+ Selective Disclosure	- Wenig reife verbreitete Standards	- Nur innerhalb des Systems nutzbar
- Kein selective disclosure möglich	+ stark an eine herkömmliche Urkunde angelehnt	+ Maschinenlesbar	- Datenschutzfragen	- Probleme bei internationaler Verwendbarkeit
- alle Daten öffentlich	- uU nicht maschinenlesbar und walletkompatibel	+ Weite Auswahl an Attributen	- Fehlende Kryptoagilität	- Probleme bei Beweisführung
- Begrenzte Auswahl an Attributen	- uU kein selective disclosure	- Abhängigkeit von QTSP	- Initial Trust Problem	
		- Zentrale Datenhaltung beim QTSP		

+ Vorteil

- Nachteil

Vielen Dank.

Andreas Wand
Business Development Manager

E-Mail: andreas.wand@d-trust.net

Teil der Bundesdruckerei-Gruppe

Back Up

Zwei Phasen Modell

1. Phase – qualifiziert gesiegelte Verifiable Credentials (qVC) sind heute möglich indem Verifiable Credentials durch qualifizierte Siegel nach **eIDAS Art. 3 Abs. 27 gesiegelt** werden.

Im Markt eingeführte Technologien: Siegelkarten, Siegelserver oder Fernsiegeldienst.

Vorteil: **Identifizierung und Validierung des Issuers in jedem Credential enthalten**.
Dieser Vorteil ist dann allen EAA und VCs möglich und geht damit weit über die kommenden QEAA hinaus.
Bem: in allen drei Fällen wird der Hashwert des Verifiable Credentials vom Issuer gesiegelt.
Die Signaturformate aus den ETSI Standards:
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 – ab ca. 2027

QEAA sind erhältlich und erzeugen ihre gesetzliche Wirkung. Die eIDAS 2.0 wird durch Fachgesetze erweitert.

Schematische Darstellung eines qualifiziert gesiegelten Verifiable Credentials

Verifiable Credentials als JSON / SD-JWT (siehe eIDAS ARF 1.0)

Signatur möglich nach JAdES (TS 119 182-1) (hier AdES-BASELINE-B Profile)

Header


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


Siegelzertifikat mit Identität des Ausstellers kann gegen EU Trust List geprüft werden

Payload


```
{
 "iss": "https://d-trust.de",
 "type": ”OrgIdentity",
 "cnf": {"jwk": {"kty": "RSA","n": "0vx7ag","e": "AQAB" } },
 "credentialSubject": {
  ”name": ”company XY",
  ”regEntry": ”HRB 001",
  ”domain": ”company-xy.de",
  ”did": ”did:indy:idunion:12345",
  "email": ”info@company-xy.de ",
  "address": {
   "street_address": "Musterstr. 23",
   "locality": "Berlin",
   "country": "DE"
  }
 }
}
```


Signature


```
ZGFzaXN0a2VpbmVlY2h0ZXN
pZ25hdHVyMWRhc2lzdGtlaW5l
ZWNodGVzaWduYXR1cjJkYX
Npc3RrZWluZWVjaHRlc2lnbmF
0dXIzZGFzaXN0a2VpbmVlY2h
0ZXNpZ25hdHVyNQ==
```


Qualifiziertes Siegel des Ausstellers