

TeleTrust-EBCA "PKI-Workshop" 2024

Berlin, 10.10.2024

"Von Verifiable Credentials dezentraler Systeme (SSI) zu qualifizierten Attestations of Attributes der eIDAS 2.0"

Christian Seegebath, D-Trust

Struktur des Vortrages

Governance eIDAS

Trust Framework und Formate

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

Trust Services der eIDAS Verordnung



Elektronische Signatur

Die individuelle digitale Unterschrift



Elektronisches Siegel

Der verlässliche digitale Stempel für Behörden und Unternehmen



Website-Zertifikat (QWAC)

Die sichere Identifizierung eines Website-Betreibers oder einer Relying Party



Validierungsdienst

Der automatische unabhängige Prüfer



Einschreib- und Zustelldienst

Die sichere digitale Nachricht wie bei der Post oder dem Gerichtsvollzieher



Zeitstempel

Die offizielle Zeit wie ein elektronischer Fotobeweis

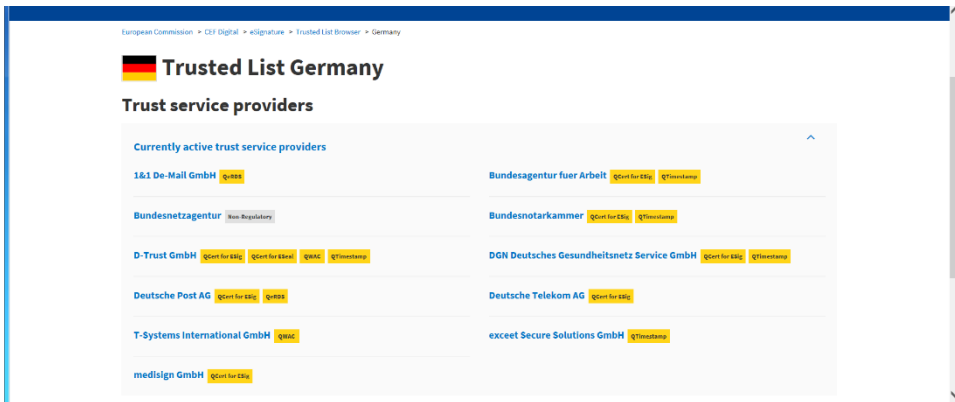


Bewahrungsdienst

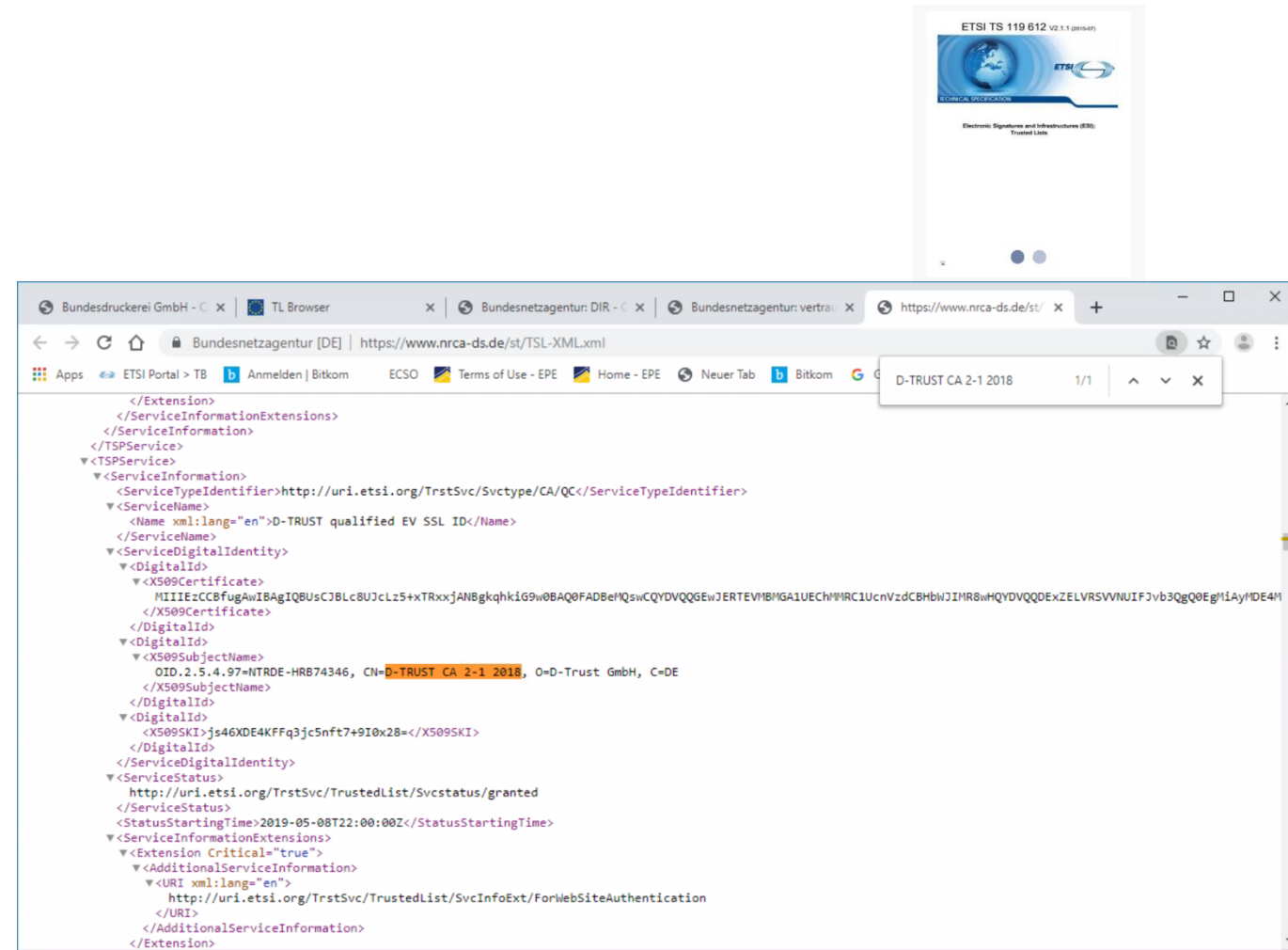
Beweiswerterhaltung

Validieren gegen die EU Trusted List (Trust Anchor eIDAS)

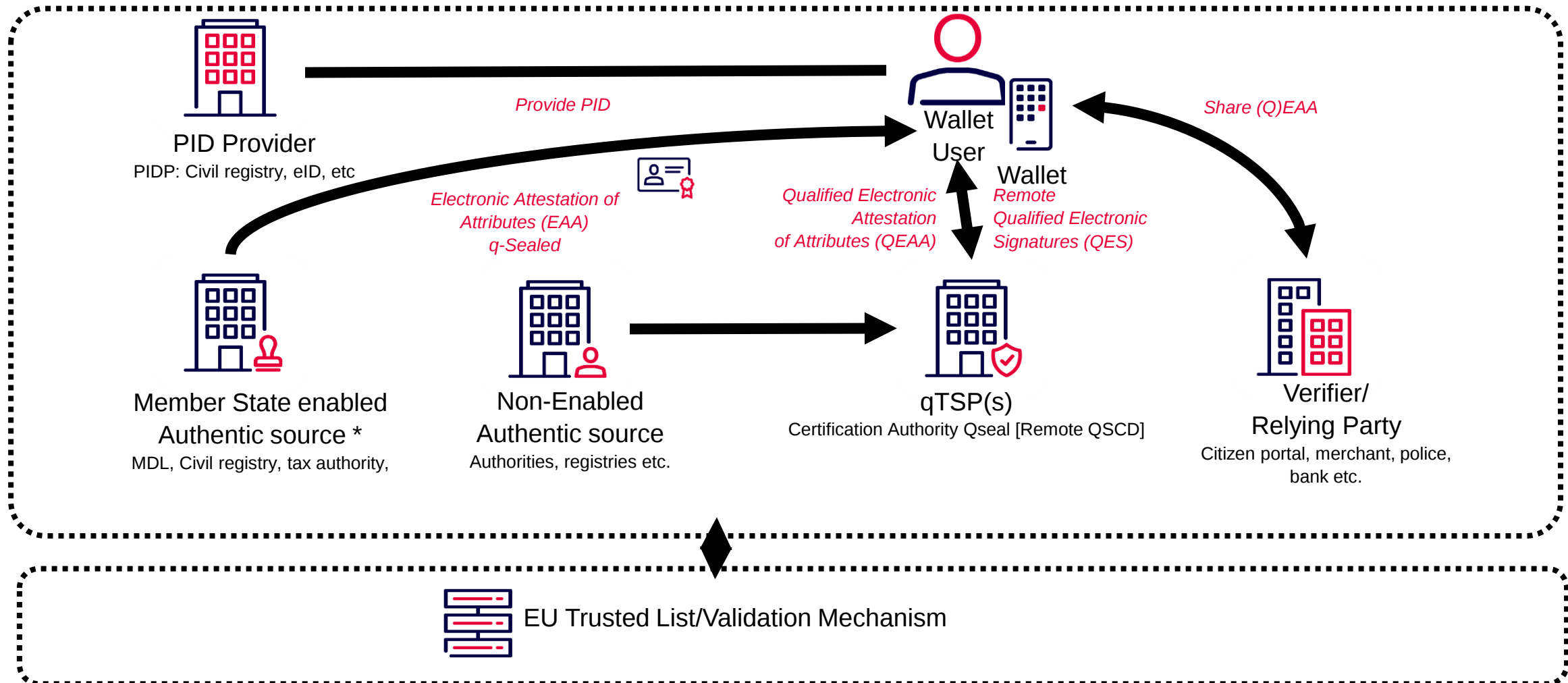
Durchführungsbeschlusss EU 2015/1505
ETSI TS 119 612



[eIDAS Dashboard \(europa.eu\)](https://europa.eu/eidas)



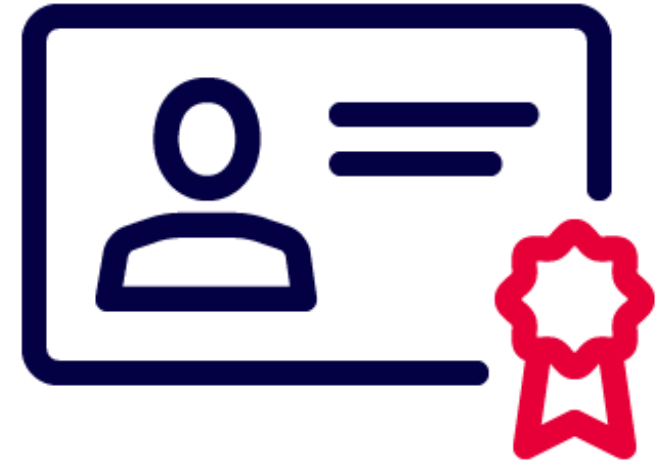
eIDAS 2.0 Architektur Überblick – Basierend auf EU Wallet Architecture Reference Framework (ARF)



*Article 45 f & Article 3 (46) eIDAS 2.0

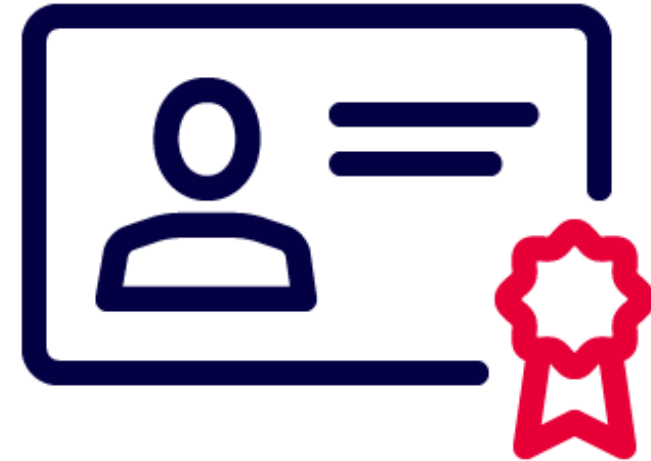
Pub-EAA über eine autorisierte öffentliche Stelle

- eIDAS 2.0 (Art. 45 f)
- 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

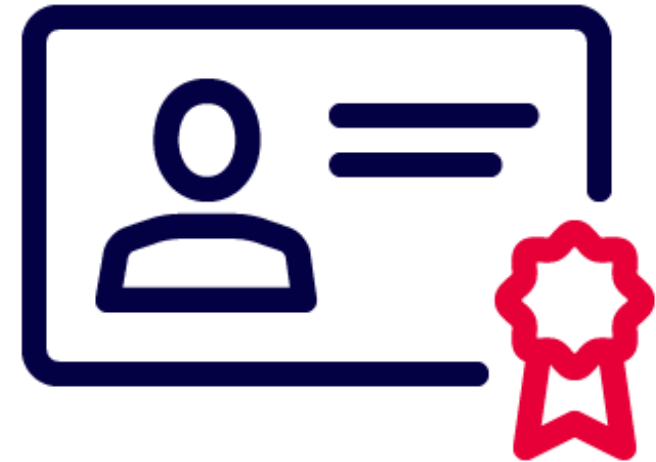


Welche Anforderungen muss ein QEAA erfüllen?

- 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, aber erst bei Wirksamwerden der eIDAS 2.0**
- Einhaltung von **organisatorischen Maßnahmen** (Datentrennung, separate Einheit) → Wird im Prototyp aufgeblendet.
- Einhaltung **formaler Anforderungen an den Datensatz** (Nutzerdaten, Ausstellender QTSP, Gültigkeit, Format etc)
- **Siegelung** des Datensatzes durch den QTSP



- Nur grundsätzliche Anforderungen an TSP allgemein (z. B. technisch organisatorische Maßnahmen)
- Kann von jedermann ausgestellt werden, auch vom Nutzer selbst
- Noch keinerlei technische Anforderungen oder Spezifizierung in ARF
- Auch Mittel zum Integritätsschutz des Datensatzes noch nicht festgelegt. **Unser Vorschlag QSiegel/QES**
- Keine Validierung des Attributs, nur Selbstangabe des Issuers.
- Keine Identifizierung des Users erforderlich.
- Kein spezieller Beweiswert; darf nur nicht pauschal abgelehnt werden



Trust Anchor ARF v1.4

A Trusted List Registrar is a party responsible for maintaining, managing, and publishing a Trusted List. Within the EUDI Wallet ecosystem, Trusted Lists exist for the following entities:

- Wallet Providers,
- PID Providers,
- QEAA Providers,
- PuB-EAA Providers,
- Access Certificate Authorities for: Relying Parties, PID Providers, QEAA Providers, PuB-EAA Providers.

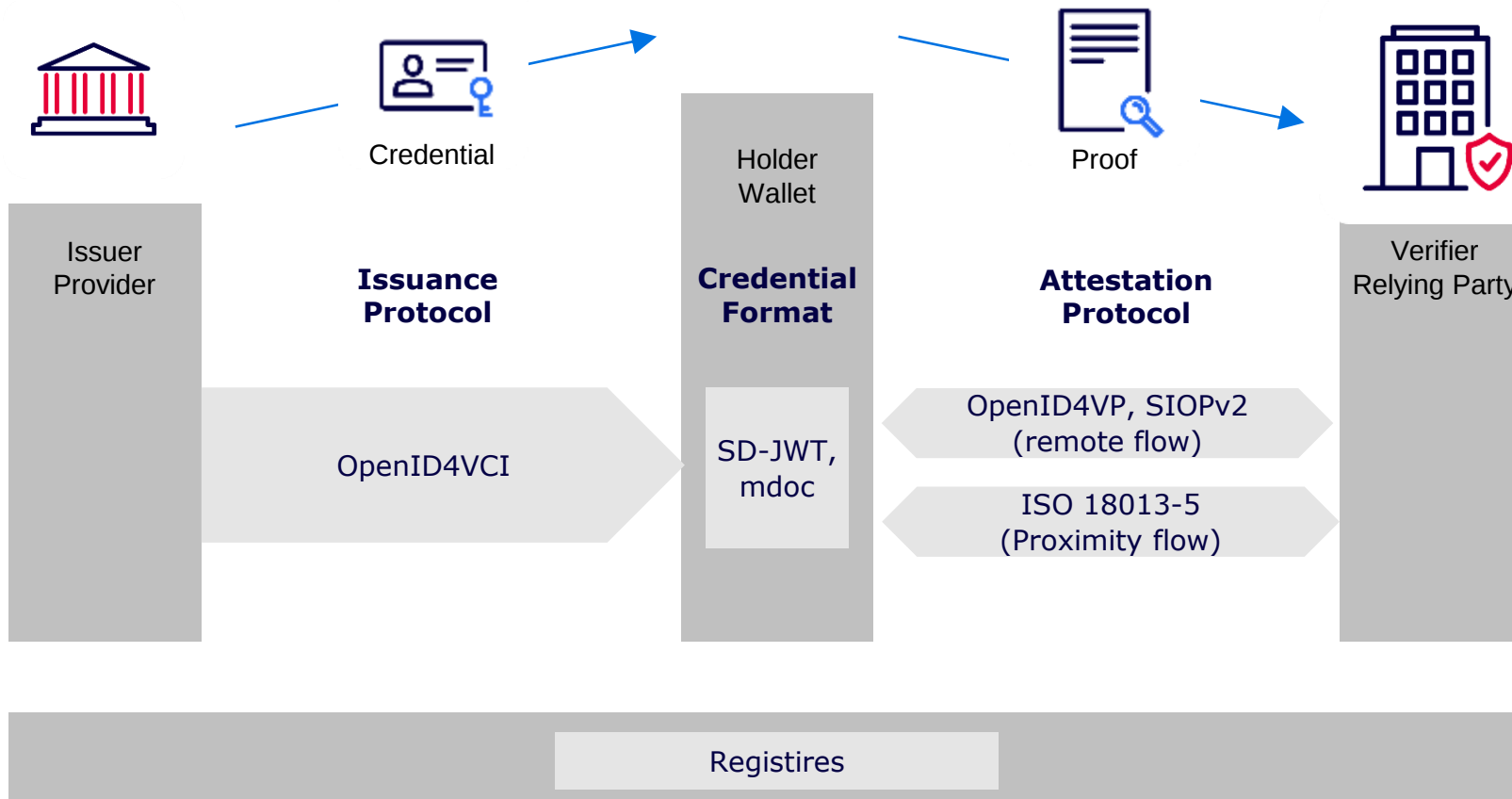


Trusted Lists primarily contain the Trust Anchors of the relevant entities. A Trust Anchor can be represented as a unique identifier and a cryptographic public key to be used to verify signatures or seals issued by that entity. From ARF v1.4 - Annex 2: PID Providers, PuB-EAA Providers, Wallet Providers and Relying Party Access Certificate Authorities must be notified by a Member State to the Commission. As part of the notification process, the trust anchors of these parties must be included in a Trusted List.

Member States will provide Trusted Lists for PID Providers, QEAA Providers and PuB-EAA Providers, in compliance with Article 22 (-> Durchführungsbb. EU 2015/1505 -> ETSI TS 119 612)

These Trusted Lists may also include non-qualified EAA Providers, but this is not mandatory. Alternatively, domain-specific trusted lists or alternative solutions for managing the trust anchors may be provided for EAA Providers

Protokolle im ARF 1.4



Jeder Mitgliedsstaat kann sein eigenes Tust Framework in eIDAS realisieren z.B:

- OpenID Federation
- X509 PKI
- EBSI etc.

Schematische Darstellung eines qualifiziert gesiegelten Verifiable Credentials

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

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

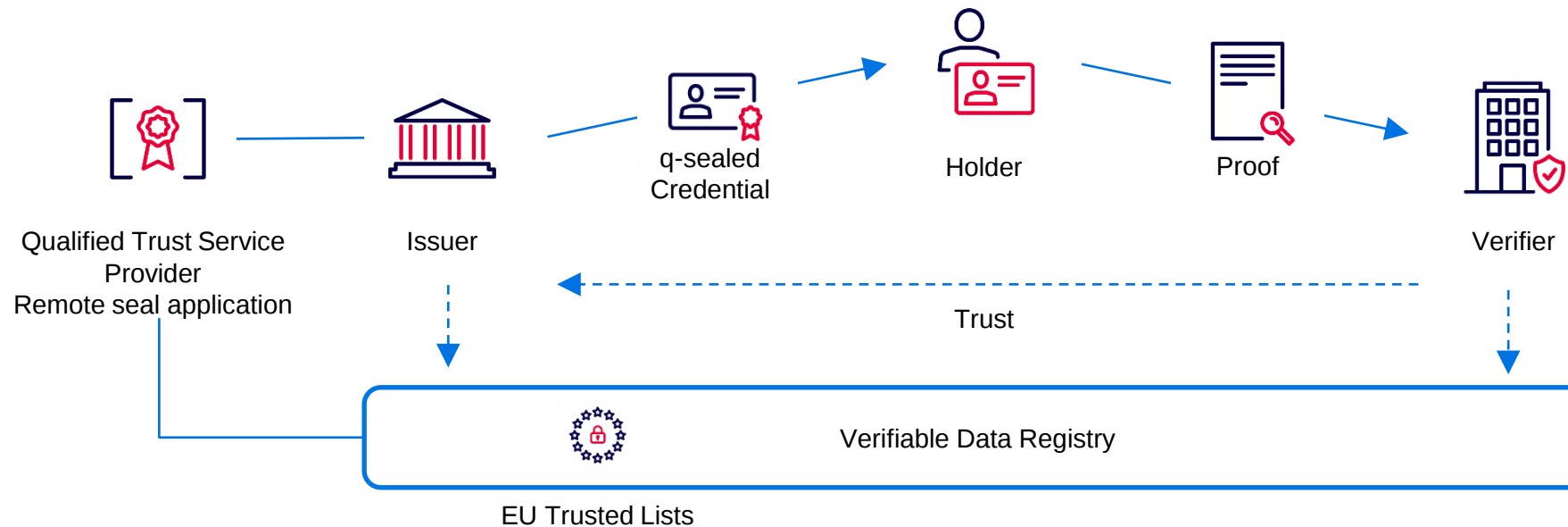
Payload

```
{
  "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

```
ZGFzaXN0a2VpbmVIY2h0ZXNp
Z25hdHVyMWRhc2lzdGtlaW5lZ
WNodGVzaWduYXR1cjJkYXNpc
3RrZWluZWVjaHRlc2lnbmF0dXI
zZGFzaXN0a2VpbmVIY2h0ZXN
pZ25hdHVyNQ==
```

Qualifiziertes Siegel des Ausstellers



Ablauf

1. Issuer stellt mit Siegeldienst gesiegelte Credentials an Holder aus
2. Holder präsentiert dem Verifier gesiegeltes Credential
3. Verifier validiert Siegel des Issuers bei EU Trusted List und prüft Sperrliste bei D-Trust

Vorteile

- Schon jetzt rechtliche Sicherheit durch durch qualifizierte Siegel nach eIDAS 1.0 Art. 3 Abs. 27
- Volle Kompatibilität mit SD-JWT nach eIDAS 2.0 / ARF 1.0 und JAdES-Signaturen nach ETSI Standard
- Identifizierung und Validierung des Issuers in jedem Credential enthalten
- Verifier kann EU Trusted List prüfen
- Keine DLT notwendig

Beispiel: Organisation Kenner einer juristischen Person

Payload

```
{
  "iss": "https://d-trust.de",
  "type": "OrgIdentity",
  "cnf": { "jwk": { "kty": "RSA", "n": "0vx7ag", "e": "AQAB" } },
  "credentialSubject": {
    "name": "D-Trust GmbH",
    "regEntry": "NTRDEF1103R.HRB74346B",
    "domain": "example.com",
    "did": "did:indy:idunion:12345",
    "email": "info@dexample.com",
    "address": {
      "street_address": "Kommandantenstrasse 15",
      "locality": "Berlin",
      "country": "DE"
    }
  }
}
```

Heute verwendet in qualifizierten Siegeln in der Datenbank EPREL (European Product Registry for Energy Labelling)

The LPID is defined in the Regulation (EU) 2024/1183 as "person identification data" means a set of data that is issued in accordance with **Union or national law** and that enables the establishment of the identity of a natural or legal person, or of a natural person representing another natural person or a legal person. "

Definition EUID

Directive EU 2017/1132

DURCHFÜHRUNGSVERORDNUNG (EU) 2015/884 DER KOMMISSION
vom 8. Juni 2015

Business Registers Interconnection System (BRIS) Register

D-Trust GmbH - Germany

Registered office: Berlin, Germany

Registration number: HRB74346B

Company type: Gesellschaft mit beschränkter Haftung 

Business Register ID: F1103R 

EUID: DEF1103R.HRB74346B

https://e-justice.europa.eu/content_find_a_company-489-en.do

Christian Seegebarth

Senior Expert Trusted Solutions

E-Mail: christian.seegebarth@bdr.de

Please note: This presentation is the property of D-Trust GmbH.
All of the information contained herein may not be copied, distributed or published,
as a whole or in part, without the approval of D-Trust GmbH.

© 2024 by D-Trust GmbH

Part of
Bundesdruckerei
group

