TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

TeleTrusT-Informationstag "Elektronische Signatur und Vertrauensdienste"

Berlin, 27.09.2023

A new hope:

Qualified Electronic Attestation of Attributes (QEAA) as a new essential eIDAS trust service

Dr. Kim Nguyen, D-Trust GmbH & TeleTrusT Board Member

It is a period of digitalization.

In 2014, the eIDAS Regulation created a European framework for trust services and electronic identification.

However, in the period that followed, the use of these means fell sometimes short of the possibilities. In particular, only qualified sealed PDF data was often used for electronic proof, and an infrastructure for exchange was slow to form in many member states.

But in summer 2021, the EU Commission published a draft for eIDAS 2.0 in which these points were addressed.

With the new tool of eIDAS 2.0 and QEAA,
the goals of digitalization shall be preserved
and digital sovereignty in the EU can be preserved...

Vision of a European digital identity ecosystem for seamless, secure and verifiable exchange of digital evidence

2010

German eID

2017

Smart-phone as card reader

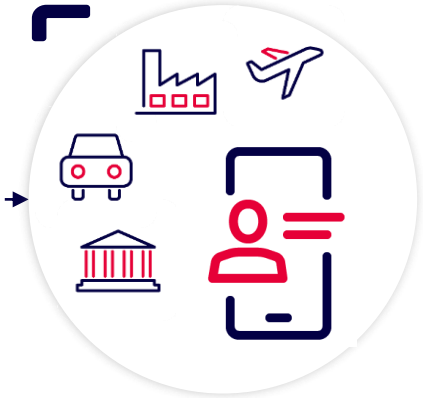
2023

Smart-eID

eIDAS revision

- European digital identity ecosystem
- EU member states must make ID wallets available - according to current planning, approx. in Q4/2025

2025



eIDAS 2.0 Proposal of EU-commission

80% of EU citizens should have access to European Digital Identity Wallet in 2030.

Tested at the European level as part of a Large Scale Pilot **(LSP)** from June 2023-2025

The EUDI Wallet should give citizens the choice of which aspects (attributes) of their **identity, data and certificates** they share with third parties (public and private).

Member states must provide **citizens (and companies)** with an EUDI wallet. Only states (or on their behalf/recognition) may issue identities. The basis of the wallet is the **derived eID as Personal Identification Data (PID)**

Trust services, in particular qualified attestation (assertion) of electronic attributes (**QEAA**), will also be part of EUDI.

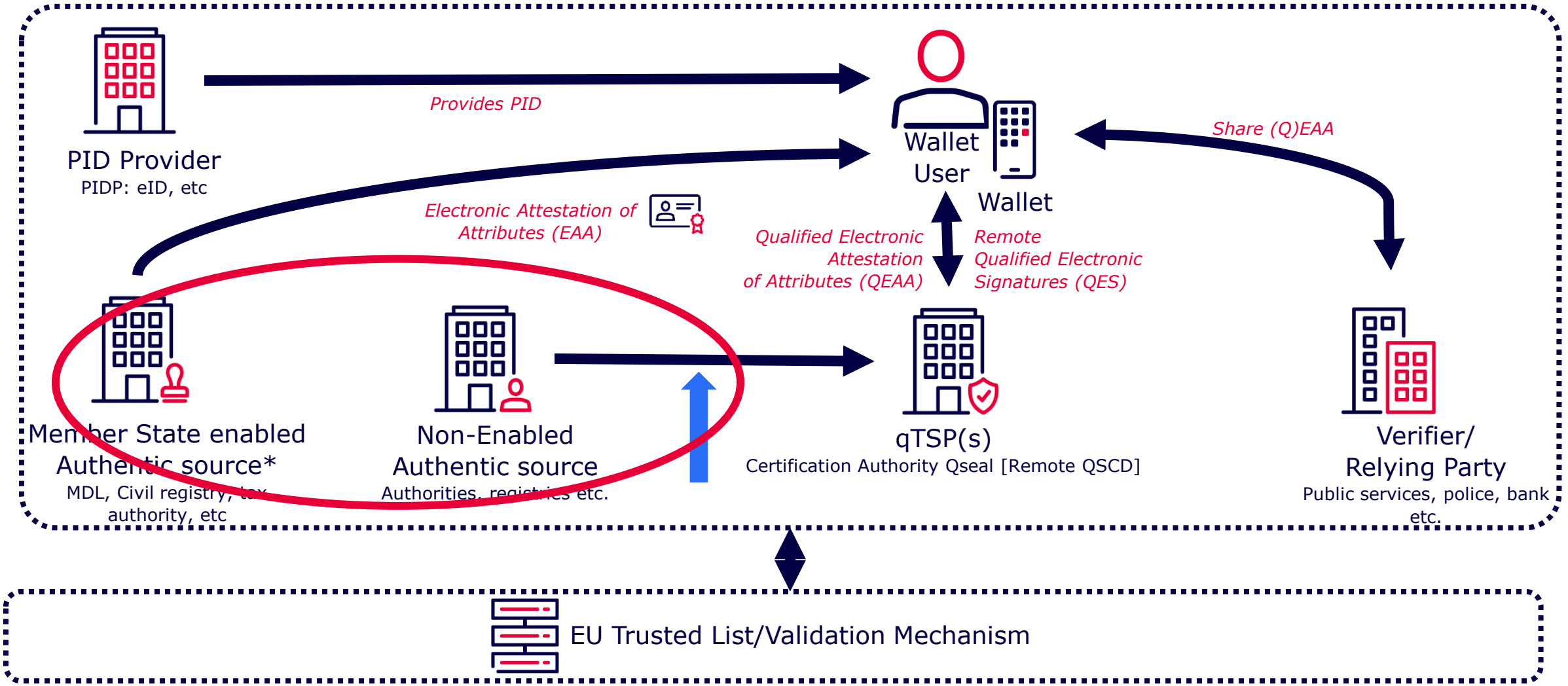
EUDI Wallet

- Online and offline functionality
- Trust level „high"
- QEAA, QES und Q-Seal functionality

At German national level currently open technical evaluation process with **"Beyond EU Digital Identity Wallet".**

Technical specifications are defined by the Architecture Reference Framework **(ARF)**.

eIDAS 2.0 architecture overview– *Based on EU Wallet Architecture Reference Framework (ARF)*

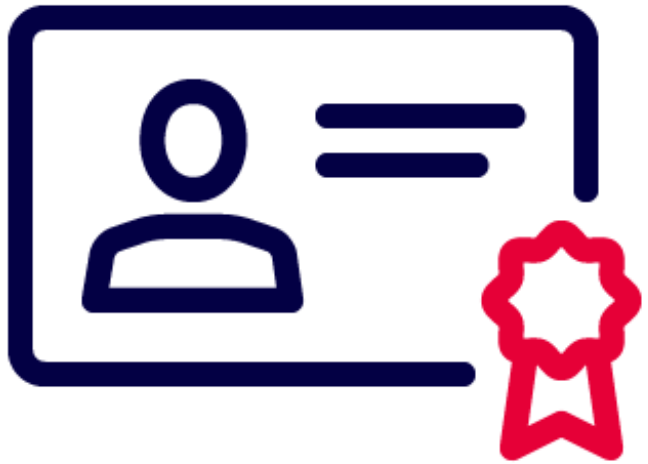


*Artikel 45d(a) des eIDAS-Proposals

What defines a QEAA?

Cryptographic protection of attribute data, which is verified and validated by an eIDAS-compliant application process.

In the future, especially the attributes of the eIDAS 2.0 draft Annex VI based on the requirements from Art. 45b and following in connection with Annex V eIDAS draft.



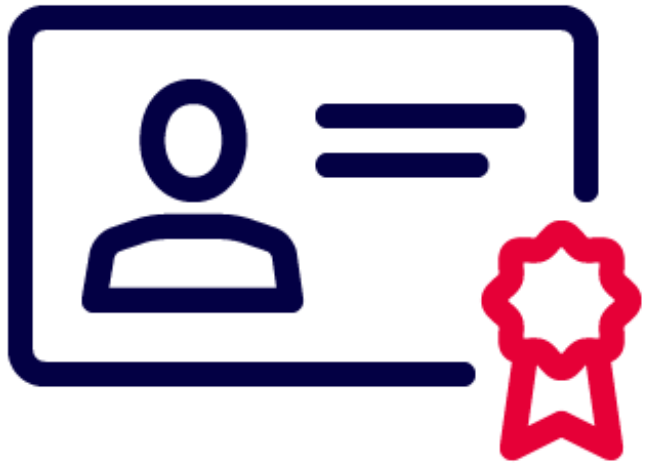
Article 45d

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. Educational qualifications, titles and licenses
8. Professional qualifications, titles and licenses
9. Public permits and licenses
10. Financial and company data

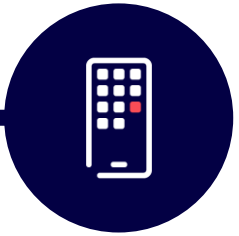
What requirements does a QEAA have to meet?

- Can only be issued by a **qualified trust service provider** (**QTSP**)
- **Identification** of the user at a qualified level, Art 24 eIDAS (usually by PID).
- Verified via an interface to the relevant state register (authentic source) -> **Obligation of the member state to provide the interface.**
- Compliance with **organizational measures** (data separation, separate unit)
- Compliance with **formal requirements for the data set** (user data, issuing QTSP, validity, etc). Through ARF specification generally to the format of **VC in SD-JWT**
- **Sealing** of the data set by the QTSP

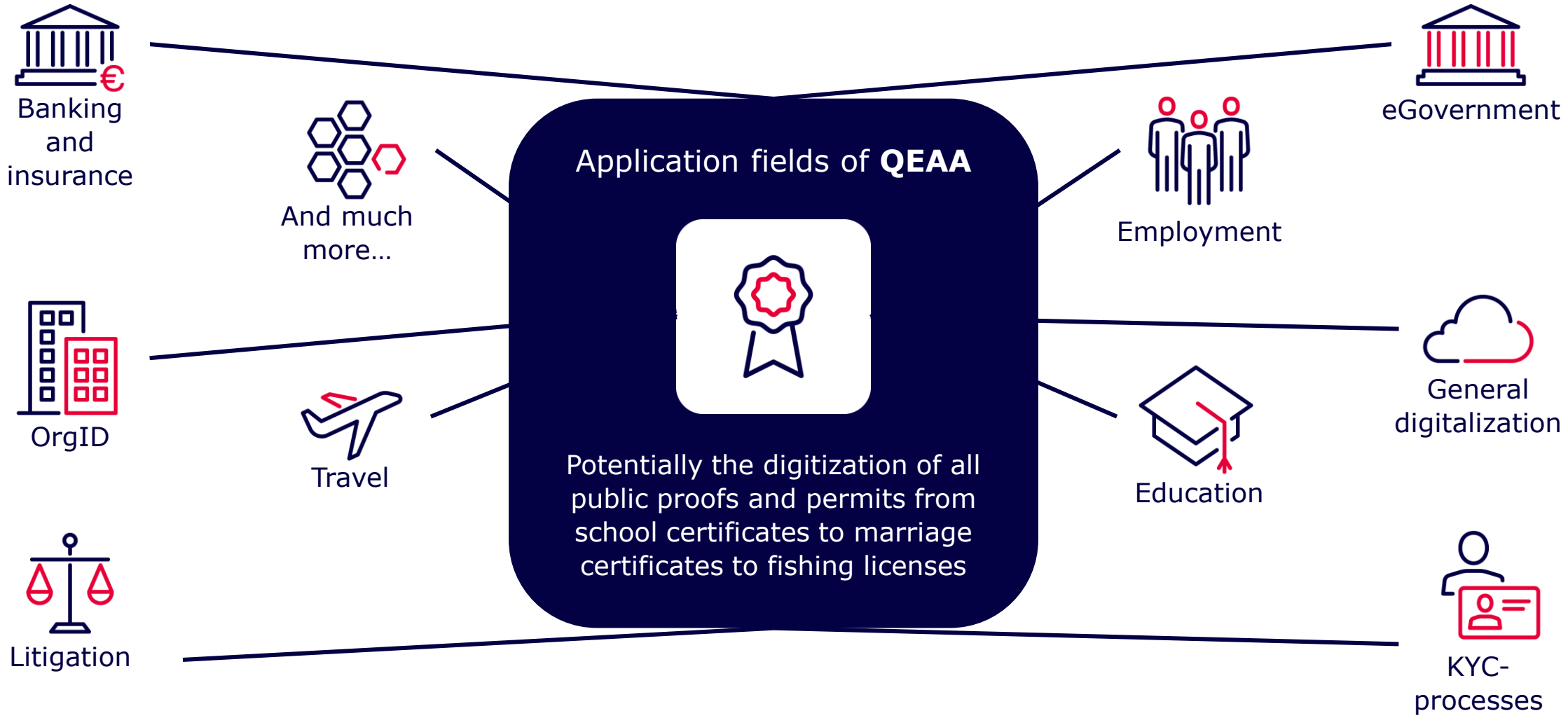


What is the general process for issuing a QEAA?

1. QEAA-Applicant contacts QTSP (via end-use application, wallet, etc.)
2. **Identification** of the applicant according to Art 24 I eIDAS (eID, EUDI, QES, QSeal, company register etc.)
3. **Validation** of the attribute by the QTSP (through identification, automated register check, via a register API)
4. **Protection** of the attribute by the QTSP according to legal requirements and **applicable standards.** (W3C, mdl, etc.)
5. **Issuance** of the QEAA (via **Wallet-API** to applicant or relying party)



Where can a QEAA be used?



How does QEAA distinguish itself from other ways of presenting electonic attributes?

Attributes in (qualified) certificates	Sealed electronic documents	**QEAA**	SSI-Credentials	Verifications in closed systems (eg OZG-Nutzerkonten)
+ standardized	+ standardized	+ standardized	+ de-centrality and alleged self-determination	+ high adminitrative sovereignty
+ already established	+ easy usable	+ connection with EUDI	+ no over-sealing for archiving needed	+ OZG-conformity
+ machine-readible	+ More and more used in practice	+ selective disclosure		
	+ Strongly based on a conventional document	+ machine-readable	- barely mature common standards	- Only usable within the closed systems
- No selective disclosure possible		+ wide selection of attributes	- GDPR problems	- problems for cross border usage
- All data public	- possibly not machine-readable and wallet-compatible		- missing crypto-agility	- problems for evidence demonstration
- limited selection of attributes		- dependency on QTSP		
	- possibly no selective disclosure	- central data storage at QTSP	- initial trust problem	

Thank you very much.

Dr. Kim Nguyen
Managing Director and TeleTrusT-Vorstand

Teil der Bundesdruckerei-Gruppe

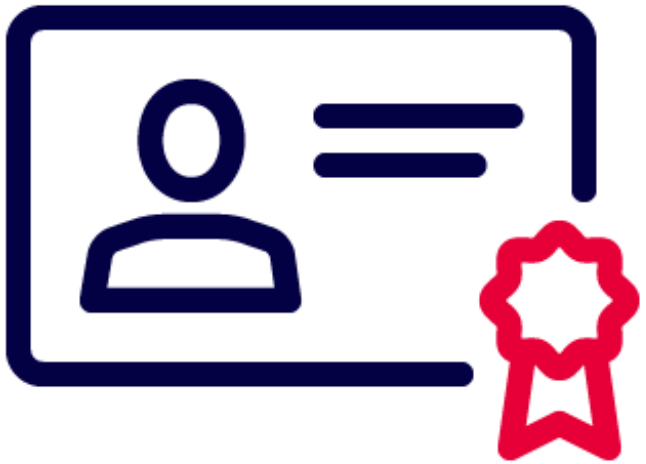
Back Up

EAA by an enbaled reliable source

- Origin: council-draft of eIDAS 2.0 (Art. 45 da)
- Per se „only" EAA, but equal in evidential value
- In particular aimed for special and important attributes e.g. mobile driving license, digital travel credential etc

- Following requirements:

  - Corresponding compliance with QTSP regulations
  - Signing/Sealing of the data set with QES/QSeal
  - Regular audits of independent conformity assessment body
  - Notification of enabled authentic source at EU-commission



Two phases model

1. phase – qualified sealed verifiable credentials (qVC) are already possible today by connecting Qseal and verifiable credentials.

Available technology: seal cards, seal servers or remote sealing service.

Advantage: identification and validation of the issuers included in every credential. This advantage is then available to all EAAs and VCs and thus goes far beyond the upcoming QEAA.

Note: in all three cases the hash value of the Verifiable Credential is sealed by the issuer. The signature formats from the 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 ~ 2027

QEAA are available and generate their legal effect. The eIDAS 2.0 is extended by specialized laws.

Schematic description of a qualified sealed verifiable credential

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

Signatur possible according to JAdES (TS 119 182-1) (here AdES-BASELINE-B Profile)

Header


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


Seal certificate with identity of issuer can be checked against EU Trust List

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"
  }
 }
}
```

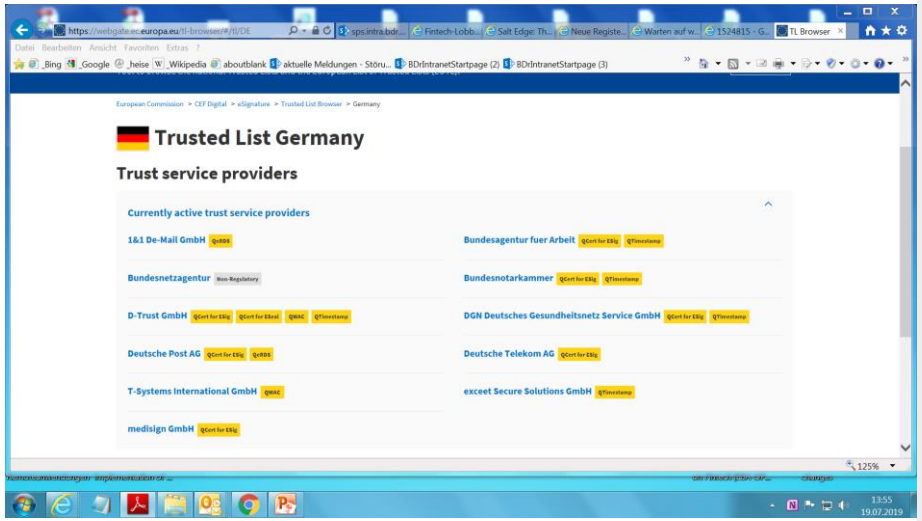

Signature

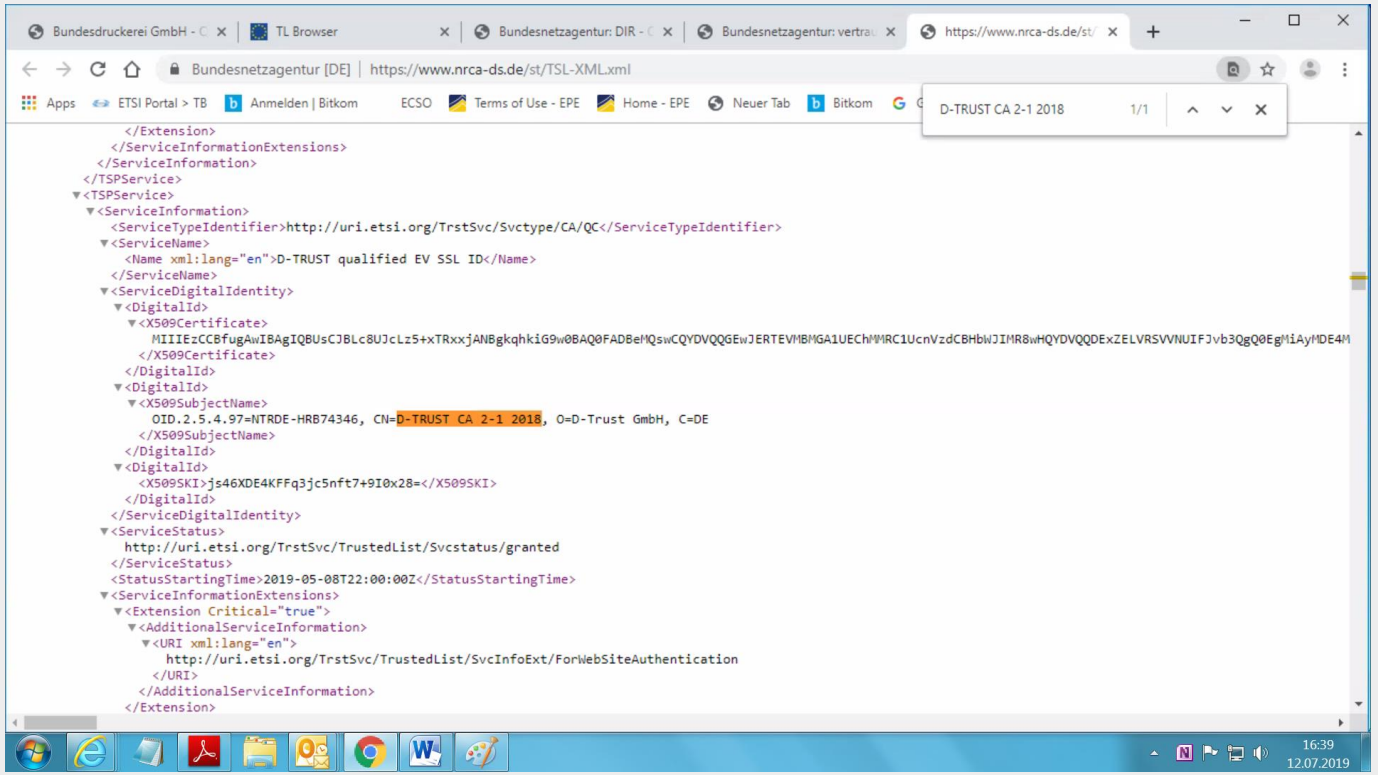

```
ZGFzaXN0a2VpbmVlY2h0ZXNp
Z25hdHVyMWRhc2lzdGtlaW5lZ
WNodGVzaWduYXR1cjJkYXNpc
3RrZWluZWVjaHRlc2lnbmF0dXl
zZGFzaXN0a2VpbmVlY2h0ZXN
pZ25hdHVyNQ==
```


Qualified Seal of the issuer

Validation against EU Trusted List

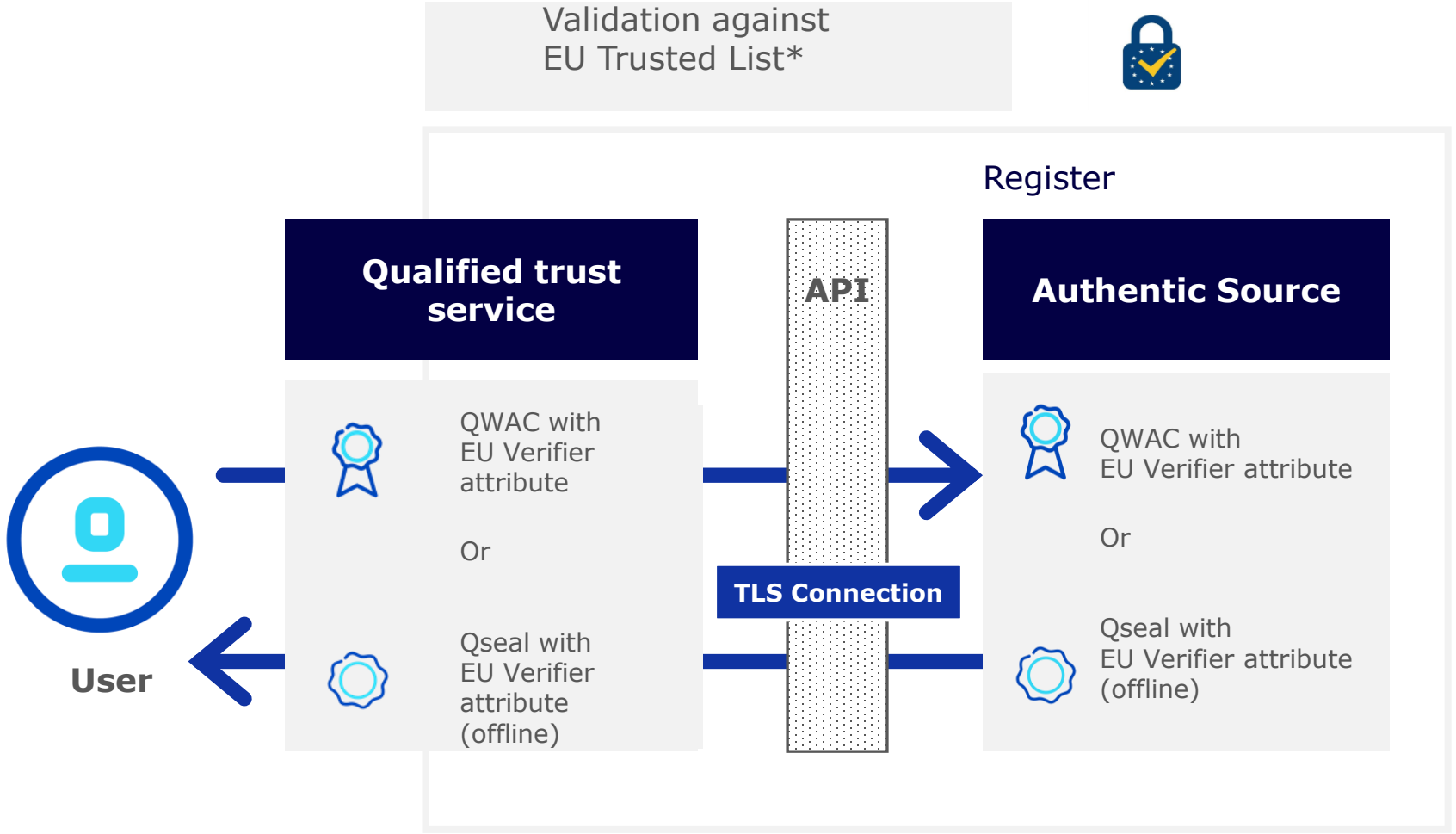
Implementing act EU 2015/1505
ETSI TS 119 612





https://eidas.ec.europa.eu/efda/tl-browser/#/screen/home

PSD2 Model for the Authentic Source API



*European Trust Service List according to Implementing Decision (EU) 2015/1505 (https://webgate.ec.europa.eu/tl-browser)