

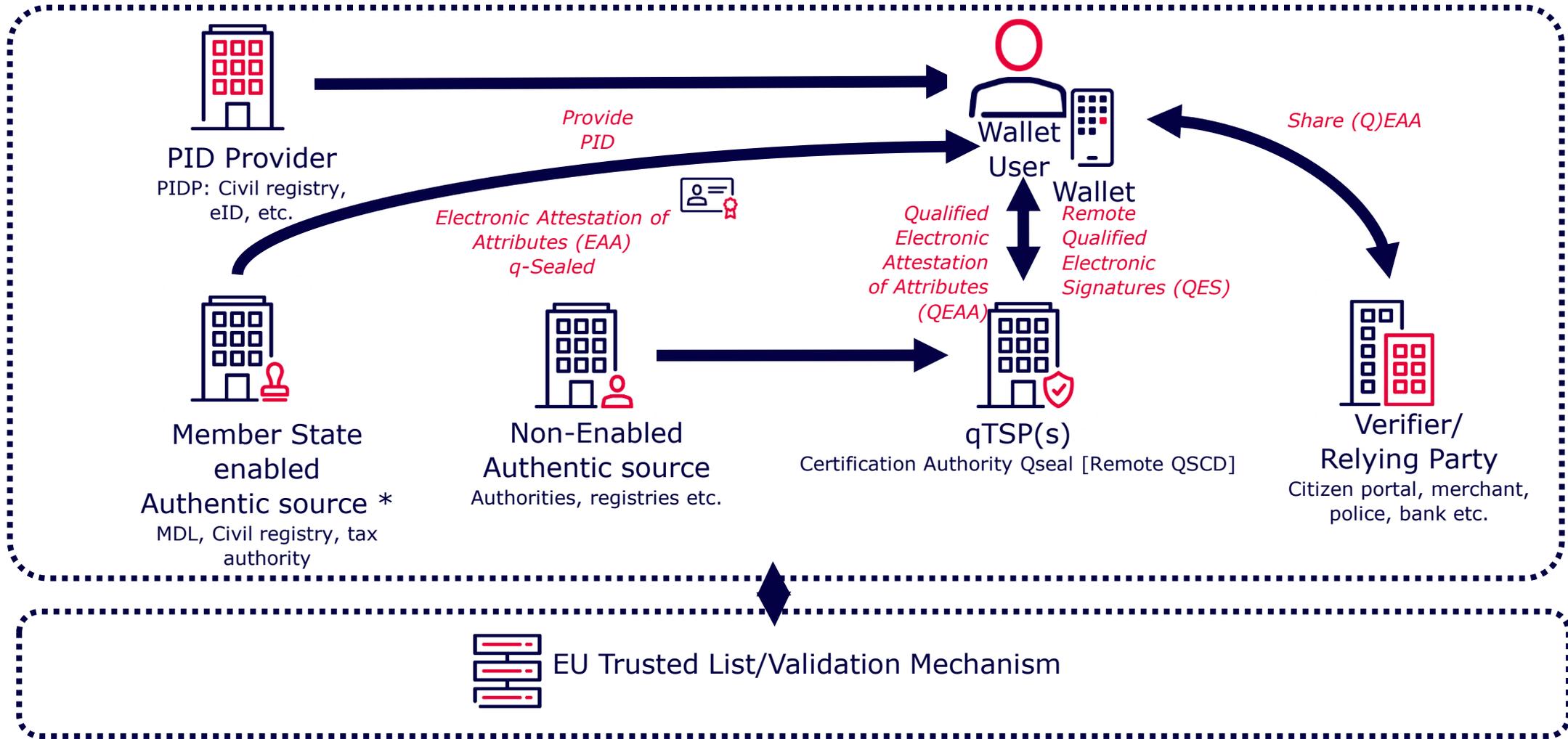


Stimulations from the QTSP

– Trust Framework, Trust Anchor, Formats

Speaker: **Christian Seegebarth**
Business Development
D-Trust/
Place: Heraklion
Date: 26. September 2024

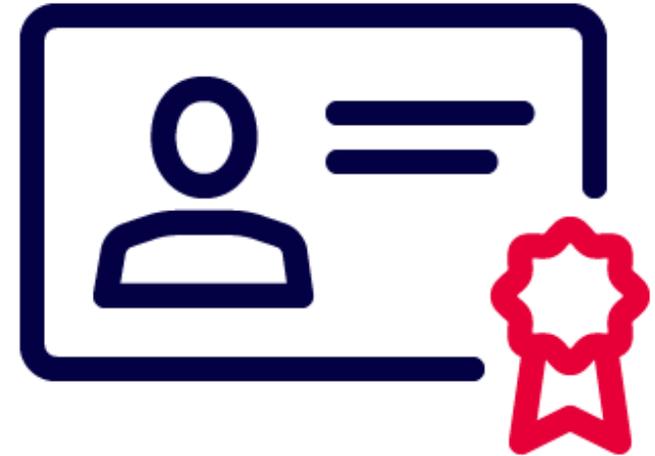
eIDAS 2.0 Architecture Overview – Based on ARF 1.4



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

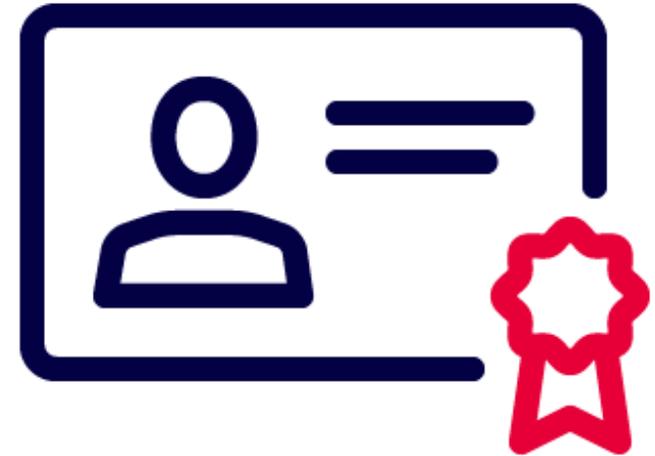
Pub-EAA issued by or on behalf of a public sector body

- eIDAS 2.0 (Art. 45 f)
- EAA with same probative value as physical document
- Examples might be: driver's license, digital travel credential
- Requiements:
 - Meet a level of reliability and trustworthiness equivalent to qualified trust service providers
 - Sealed or signed with a **QES/QSeal**
 - Regularly audited
 - Notification to the commission



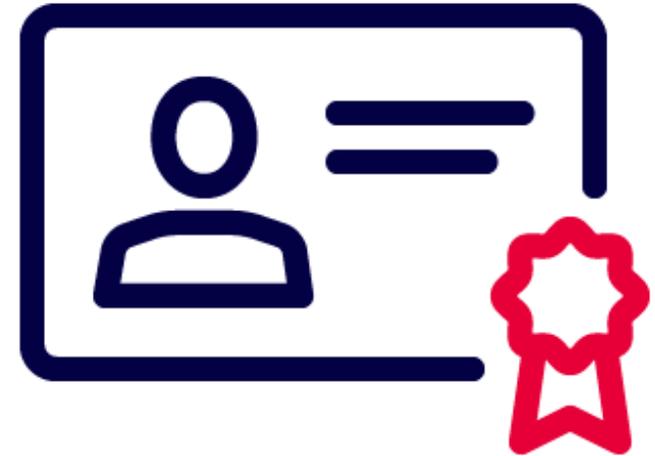
Requirements for a QEAA?

- Can only be issued by a qualified trust service provider(QTSP)
- **Identification** of the user at a qualified level (usually through PID)
- Verified via an interface to the relevant state register - **Obligation of the member state to create the interface**
- Compliance with organizational measures (data separation, separate unit)
- Compliance with **formal requirements** for the data record (user data, issuing QTSP, validity, format, etc.)
- **Qualified sealing** of the data set by a QTSP



EAA

- Only basic requirements for TSP in general (e.g. technical organizational measures)
- Can be issued by anyone, including the users themselves
- No technical requirements or specifications in ARF yet
- Means of protecting the integrity of the data set have not yet been determined. Our wish QSeal/QES
- No validation of the attribute, only self-declaration by the issuer.
- No user identification required
- No special probative value; just cannot be rejected across the board



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



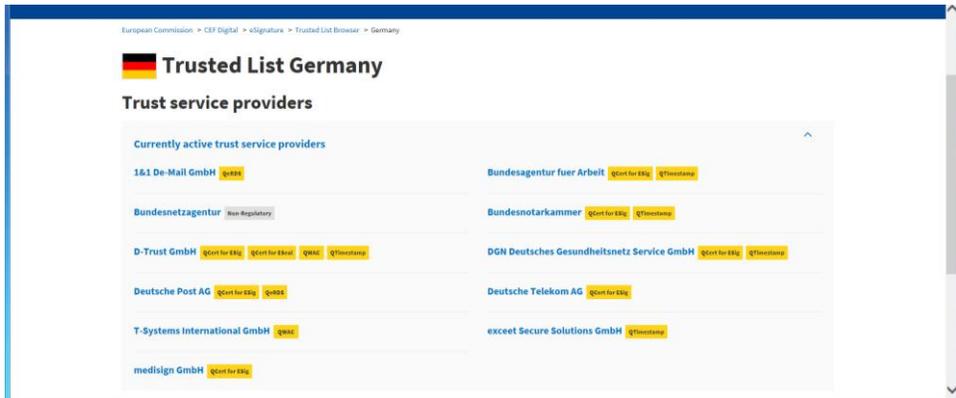
Trusted Lists primarily contain the Trust Anchors of the relevant entities. A Trust Anchor can be represented by a unique identifier and a cryptographic public key which are used to verify signatures or seals issued by that entity. From ARF v1.4 - Annex 2: PID Providers, PuB-EAA Providers, Wallet Providers 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 (-> EU 2015/1505 -> ETSI TS 119 612).

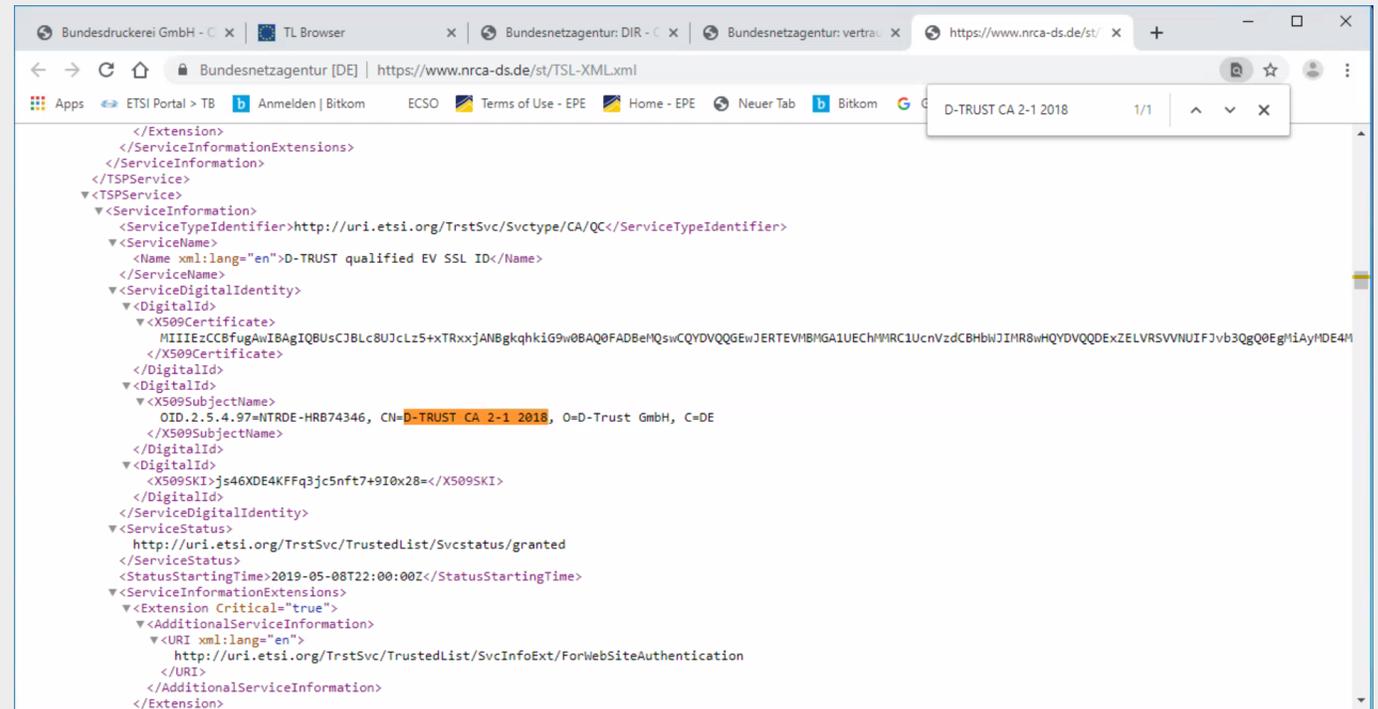
These Trusted Lists may also include non-qualified EAA Providers, but this is not mandatory. Alternatively, domain-specific trusted lists or alternative solutions for managing the trust anchors may be provided for EAA Providers.

Validation against the EU Trusted List

Implementing Decision EU 2015/1505
ETSI TS 119 612



eIDAS Dashboard (europa.eu)



Scheme of a qualified sealed verifiable credential (EAA)

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

Signature JAdES (TS 119 182-1) (here: AdES-BASELINE-B Profile)

Header

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

A seal certificate with the issuer's identity can be verified against the EU Trusted 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

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

Qualified seal of the issuer

European organisational company ID - ORG ID

Payload of a QEAA

```
{
  "iss": "https://d-trust.de",
  "type": "OrgIdentity",
  "cnf": { "jwk": { "kty": "RSA", "n": "0vx7ag", "e": "AQAB" } },
  "credentialSubject": {
    "name": "D-Trust GmbH",
    "regEntry": "DEF1103R.HRB74346B",
    "domain": "example.com",
    "did": "did:indy:idunion:12345",
    "email": "info@dexample.com",
    "address": {
      "street_address": "Kommandantenstrasse 15",
      "locality": "Berlin",
      "country": "DE"
    }
  }
}
```

Already used today in the context of EPREL
(European Product Registry for Energy Labelling)

Definition EUID

Directive EU 2017/1132

Commission Implementing Regulation (EU) 2015/884
of 8 June 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



Stimulations from the QTSP

– QEAA Detail Problems

Speaker:

Andreas Wand

Business Development

D-Trust/

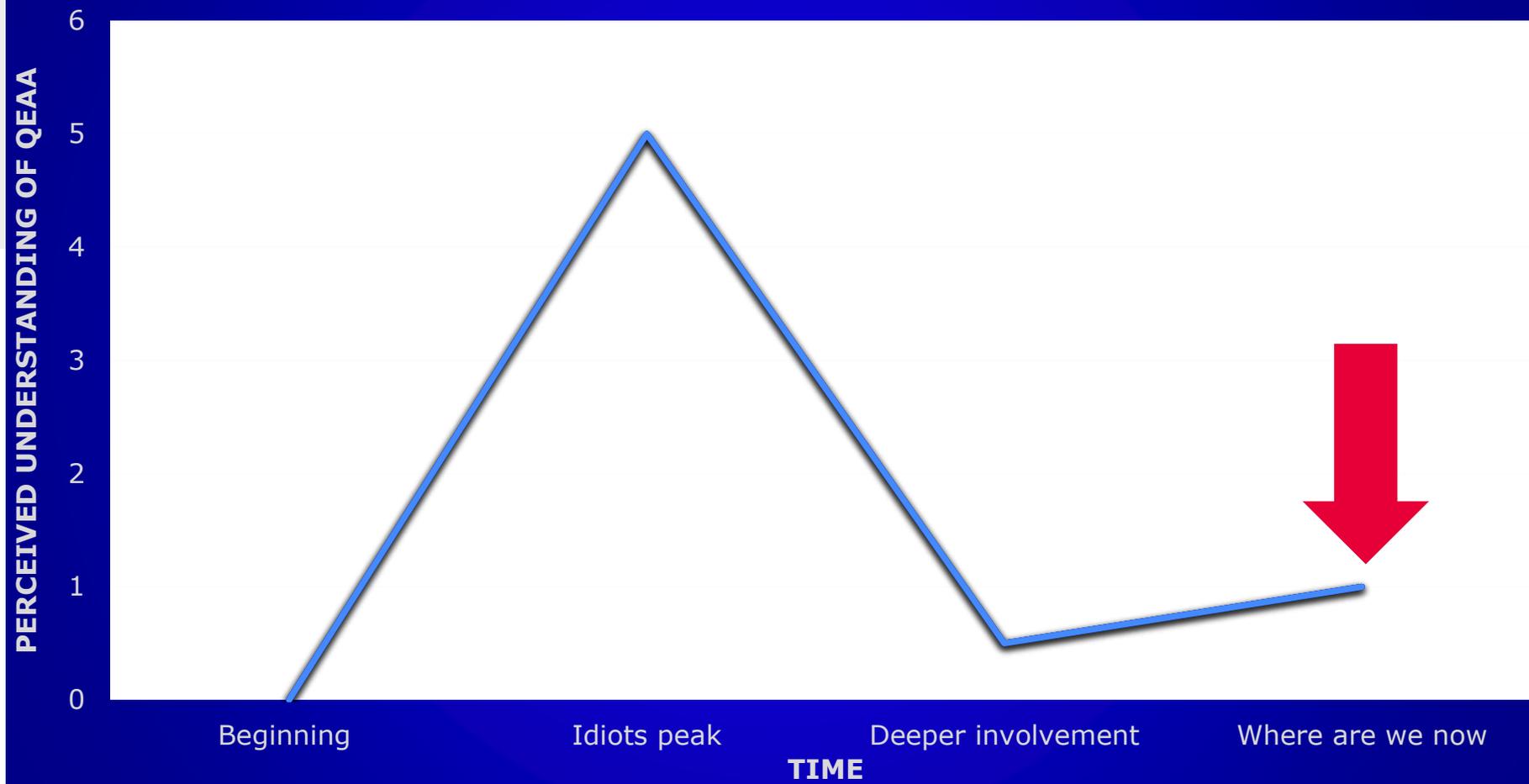
Place:

Heraklion

Date:

26. September 2024

Professional involvement with QEAA



Currently, QEAA seems to be **a projection surface** of concerns, hopes and expectations, which leads to many gaps and different understandings.



1. Problem: How does the QTSP prove the user's authorization to the authentic for issuing the QEAA?

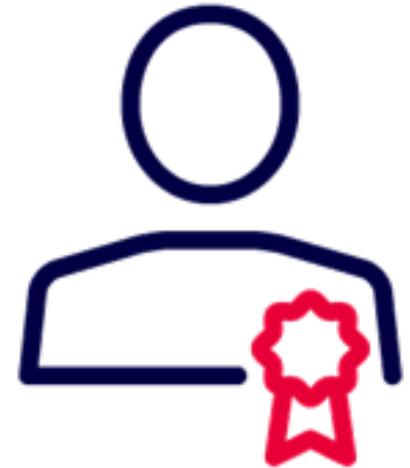
Andreas Wand, LL.M.
Business Development Manager

Potential threat scenario

QTSP requests data from authentic source without authorization from a user with malicious intent

→ General data protection criticism of QEAA, purely organizational measures probably not sufficient

- Possible solutions:
 - Integration at authentic source and collection of consent by authentic source
 - Prior registration of the user at the authentic source and then 2FA
 - Provision of a cryptographic secret → difficult to implement. PID not sufficient
 - ?



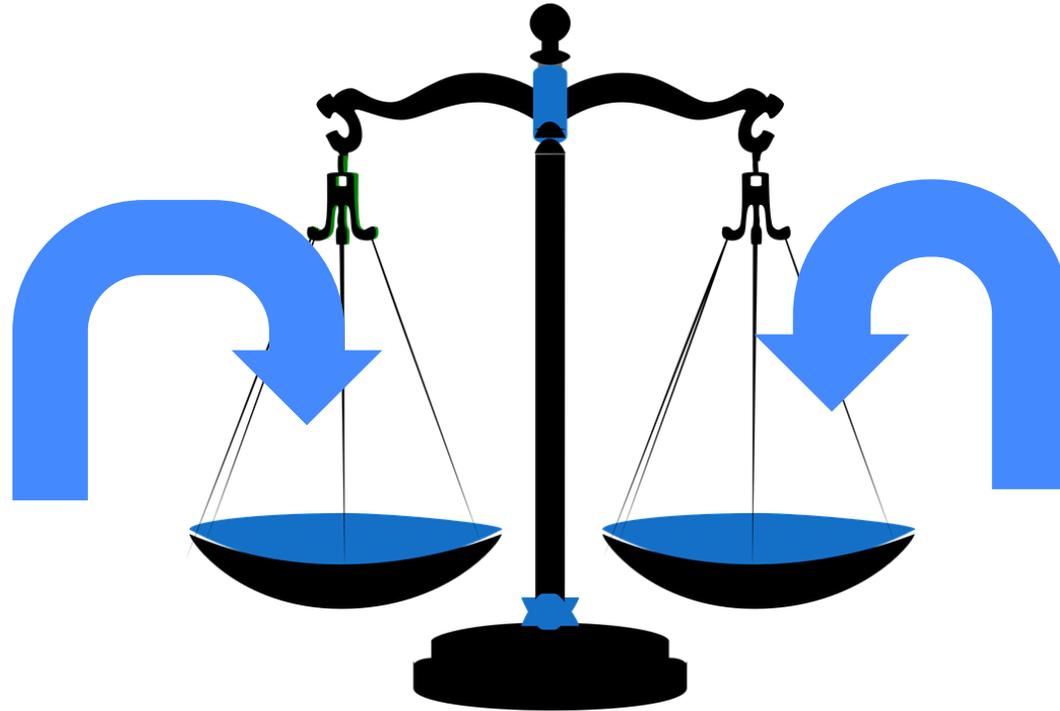
2. Problem: Scheme standardization to enable selective disclosure and zero knowledge proof

Andreas Wand, LL.M.
Business Development Manager

QEAA Scheme

QEAA should (!) be capable of zero knowledge proof, the EUDI shall ensure selective disclosure is generally possible

Selective disclosure and zero knowledge proof only work if QEAA has a precisely defined and standardized structure and designation of the individual data



Overly granular standardization of the QEAA scheme jeopardizes functionality

Schemes are very complex to standardize and implement, also risk that authentic sources do not contain all required data, also translations and restructuring required

- 1. Only basic standardization of the most important QEAA groups, e.g. school certificates, public legal permits, etc.**
- 2. Separation in micro attributes**

3. Problem: Revocation of QEAA when changes within the authentic source

Andreas Wand, LL.M.
Business Development Manager

Changes within authentic sources

Is the QTSP liable if the accuracy of the QEAA changes within the validity period?

→ **Therefore, only short time-QEAA?**

→ If liability is given, how does the QTSP know when something changes?

→ eIDAS does not directly provide a mechanism for it, as

- notification obligation of the authentic source in the event of changes
- renewed automated queries of the QTSP at the authentic source



Christian Seegebarth

Senior Expert Trusted Solutions

E-Mail: christian.seegebarth@bdr.de

Andreas Wand, LL.M.

Business Development Manager

E-Mail: andreas.wand@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

The logo for bdr. consists of the lowercase letters "bdr." in a bold, sans-serif font. The "b" is black, the "d" is red, and the "r" is yellow. A period follows the "r".