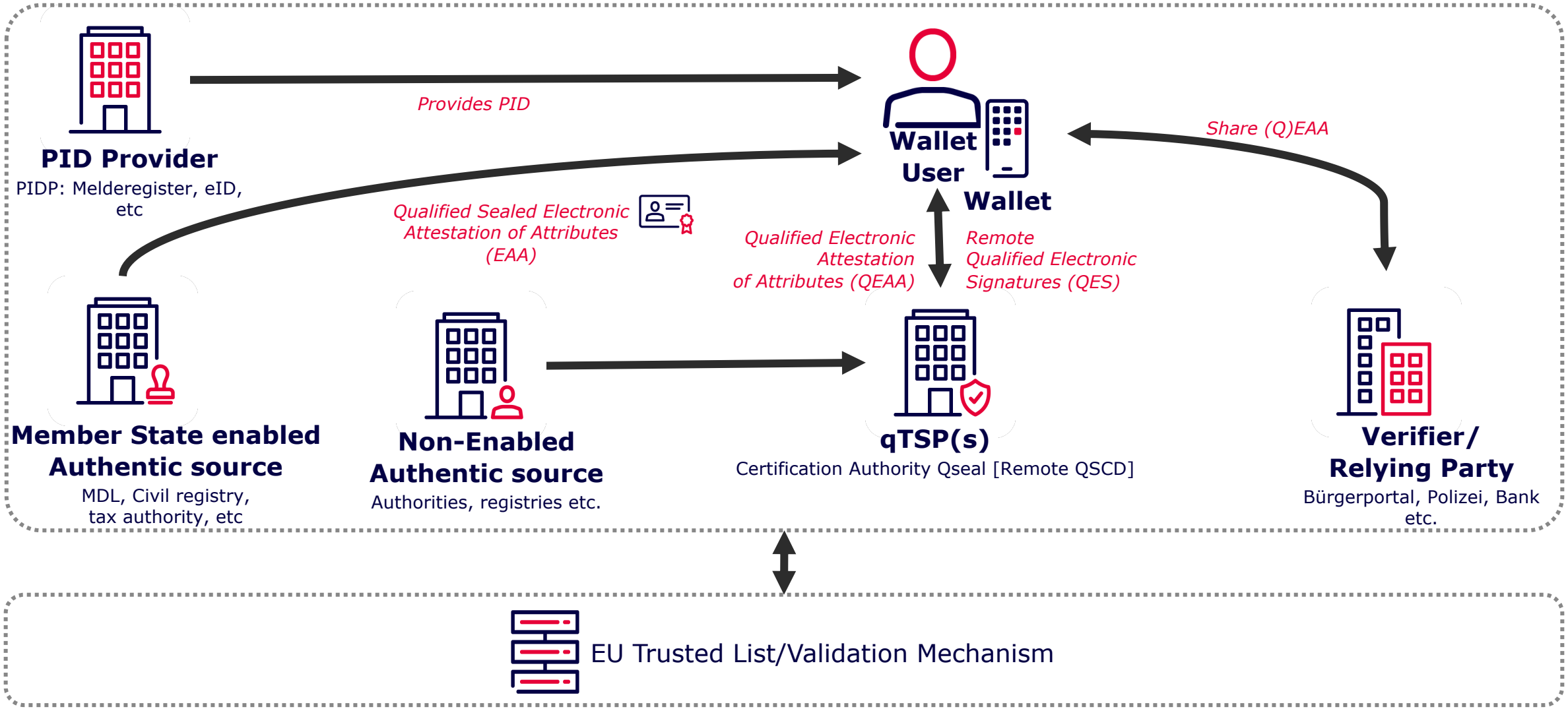
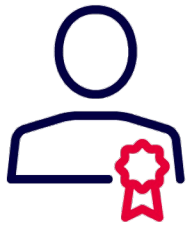
Warum das EUDI-Ökosystem ohne Berücksichtigung von Unternehmens-Wallets scheitern könnte

Datum	23.01.2024
Ort	Omnisecure
Verfasser	Andreas Wand Business Development Manager

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



Warum wird immer nur die natürliche Person in den Fokus genommen?



Nutzer = natürliche Person

(im deutschen Verständnis)

<u>Warum?</u>

- Zersplitterung der Zuständigkeiten
  - nat. Person->BMI
  - jur. Person->BMJ

- Jur. Person muss offenkundig und mit Vertretungsmacht vertreten werden
- Bei W:Enable sind jur. Personen nicht berücksichtigt

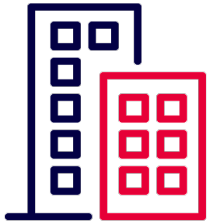
➢ Jur. Person nur als Attribut für (gesetzlicher) Vertreter

Unternehmenswallet vs. Wallets natürlicher Personen

Wallet einer natürlichen Person mit Unternehmens-attributen

- **PID des Mitarbeiters** / Device Binding
    - Delegierte Befähigung zur Vertretung der jur. Person
        - Organschaftliche Vertretung
            - Stammidentität der jur. Person
                - Attribute der jur. Person
                - Zugriff auf Supply-Chain-Systeme, etc.
- (P) Credential-Chaining? Vermutlich wenig Resilienz

vs.



Unternehmens-Wallet

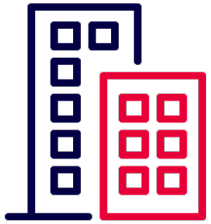
- **Org-ID als PID-Ersatz**
    - Attribute der jur. Person, zB. Erlaubnisse (ZAG, GewO, VAG etc.), Steuernummer, CO2-Daten, Kontonummer, LEI, GS1-Barcodes, Produktpassdaten etc.
    - Internes Rechte- und Rollenmanagement verantwortet durch das Unternehmen
    - Zugriff auf Supply-Chain-, Logistiksysteme
    - Zukunft: Smart Contracts

Unternehmenswallet vs. Wallets natürlicher Personen **– Technische Unterschiede**

Wallet einer natürlichen Person mit Unternehmens-attributen

- „Normale" EUDI Wallet auf dem Device des Mitarbeiters
  - ➢ Risiko: Vermischung berufliche und private Wallet
- Dezentral, keine zentrale Wallet-Instanz
  - ➢ keine zentrale Steuerung des Unternehmens
- Delegation des Vertretungsrecht über Erteilung und Widerruf über des jeweiligen (Q)EAA
  - ➢ Herausforderung: Sperrrecht Dritter
- Gefahr, dass Mechanismen der EUDI den Unternehmen übergestülpt werden

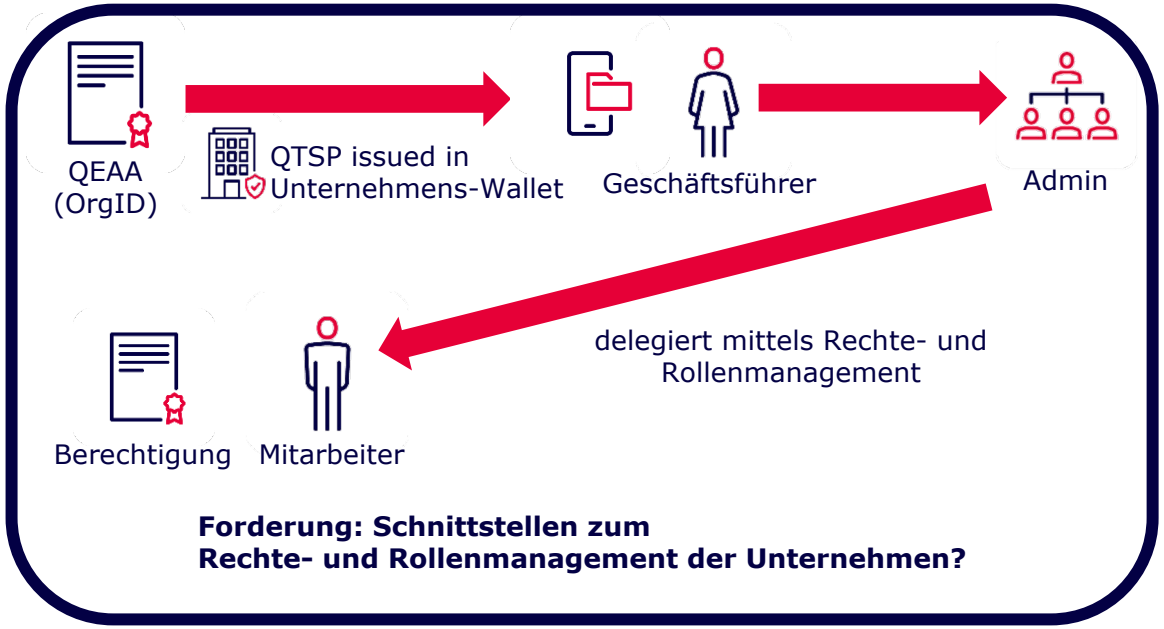
vs.



Unternehmens-Wallet

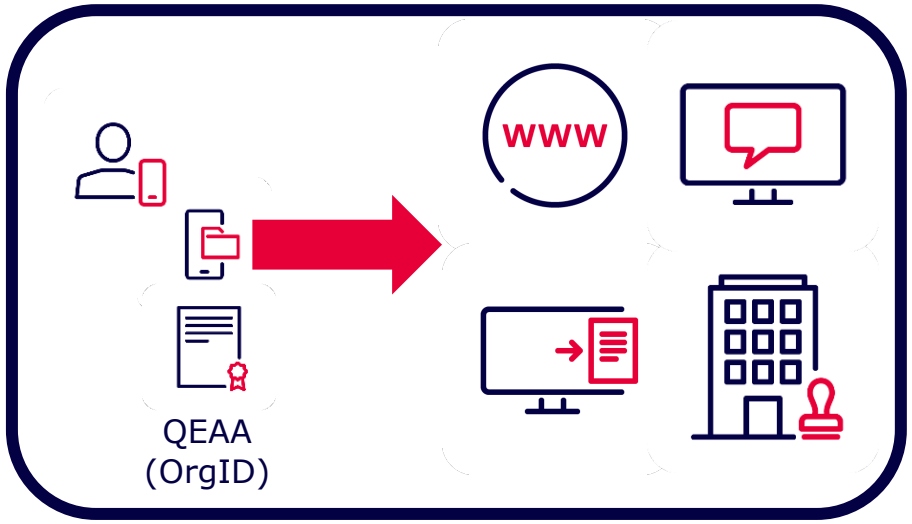
- Zentrale Wallet-Instanz und zentrale Speicherung aller Daten
- Unternehmens-Wallet entweder als eigene EUDI oder als Cloud-Wallet, die EUDI-Wallet als Authenticator bzw. Übertragungsmittel nutzt (Zertifizierung notwendig?)
- Rechte- und Rollenmanagement zentral im Backend durch Admin
- Protokolliert wird der Name des Mitarbeiters
- Interne Unternehmensabläufe sollten größtenteils unangetastet bleiben

Ein Unternehmen lässt sich eine OrgID in die Unternehmens-Wallet ausstellen. Der Geschäftsführer übergibt den Zugang in die Wallet dem Administrator, dieser richtet ein Rechte/Rollenmanagement ein.



Vertretungs-
Berechtigung

Mitarbeiter agiert mittels Unternehmenswallet berechtigt für Unternehmen:



Unternehmenswallet | Internes Rechte und Rollenmanagement delegiert Vertretung intern

1. Unternehmens-Wallet wird eingerichtet;
   Authentifizierungsmittel* wird für GF eingerichtet
2. QTSP stellt eine OrgID aus
3. Geschäftsführer gibt Zugang zur Wallet an Admin weiter
4. Admin richtet Rechte- und Rollenmanagement ein**
5. Delegierte Mitarbeiter richten individuellen Authenticator* ein
6. Mitarbeiter führt mit seinem Zugang Aktionen für das Unternehmen aus, z.B. bei einer Relying Party, Beantragung weiterer QEAA, etc. und übermittelt OrgID, QEAA oder löst QSiegel aus

*Kann EUDI sein, kann aber auch anderes Authentifizierungsmittel sein
** Schnittstelle zu bestehenden Systemen oder eigenes Rechte- und Rollenmanagement der Wallet

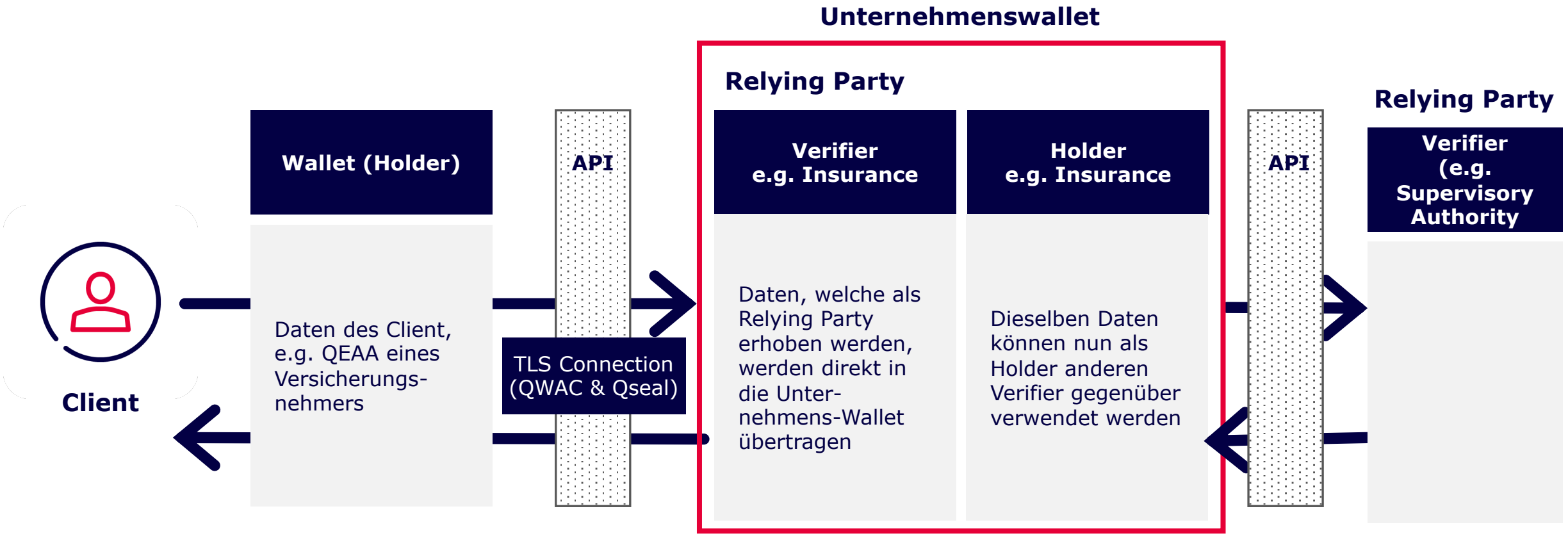
Ablauf der Ausstellung bei Nutzung Mitarbeiter-**Wallet <u>bei nur eingliedriger Unterbeauftragung (!)</u>** (Aus Sicht Sicht des QTSP)

1. Natürliche-Personen-Wallet des Geschäftsführers wird eingerichtet;
   Authentifizierungsmittel wird eingerichtet
2. PID Ausstellung für GF
3. Org-ID Ausstellung durch QTSP;
   Verknüpfung mit GF-Wallet als Attribut der natürlichen Person
4. GF lässt Unterbeauftragung als (Q)EAA ausstellen
5. Mitarbeiter-Wallet wird eingerichtet;
   Authentifizierungsmittel wird eingerichtet
6. PID Ausstellung für Mitarbeiter
7. Verknüpfung des Unterbeauftragungs-(Q)EAA samt der Org-ID als Unterattribut mit Mitarbeiter-Wallet

Für jede Unterbeauftragung jeweils Schritte 4-7

Der Unterschied bei Nutzung als Relying Party

Unternehmenswallet bei Relying Parties (Verifier-Perspektive)



Für den Erfolg der EUDI im B2B- oder B2G-Bereich ist essentiell:

- ✓ OrgID als PID-ähnliche Grundidentität
- ✓ Offenheit des EUDI-Ökosystem für zertifizierte Unternehmenswallets
- ✓ Berücksichtigung von Branchenstandards und Interessen
- ✓ Öffnung der LSP/W:Enable und anderer Beteiligungsprozesse für Unternehmenswallets
- ✓ Keine mandatorische Walletbindung für QEAA, Bindung an die OrgID.

Vielen Dank.

Andreas Wand

D-Trust GmbH
M BD
E-Mail: andreas.wand@d-trust.net
Telefon: +49 (0) 30 25 93 91-0

Teil der Bundesdruckerei-Gruppe