Qualifizierte elektronische Signatur mit der EUDI-Wallet

Omnisecure 2024

Datum	22.01.2024
Ort	Berlin
Verfasser	Dr. Mark Ullmann, D-Trust GmbH

Dr. Mark Ullmann

→ Solution Architect bei der D-Trust GmbH, einer Tochtergesellschaft der Bundesdruckerei GmbH

→ Mitglied im Large Scale Pilot Potential, für den Use Case 5 “Qualifizierte Elektronische Signatur”

Die EUDIW ist eine digitale Version von Ausweis, handschriftlicher Unterschrift, Bescheinigungen

EUDI-Wallet

Identifikation

Ausweis

qualifizierte elektronische Signatur (QES)

Unterschrift

(qualifizierte) elektronische Nachweise (QEAA)

Führerschein
Bescheinigungen

Die EUDIW ist eine digitale Version von Ausweis, handschriftlicher Unterschrift, Bescheinigungen

EUDI-Wallet

qualifizierte elektronische Signatur (QES)

Unterschrift

Identifikation

Ausweis

(qualifizierte) elektronische Nachweise (QEAA)

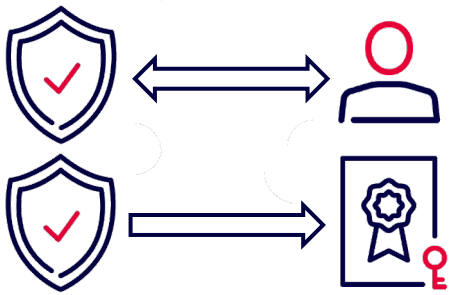
Führerschein
Bescheinigungen

Aussagen dieses Vortrag zur qualifizierten elektronischen Signatur mit der Wallet sind vorläufig, da wir noch in einer frühen Phase des Projekts sind.

Mittels eines Zertifikats wird einem Dokument eine Signatur hinzugefügt.

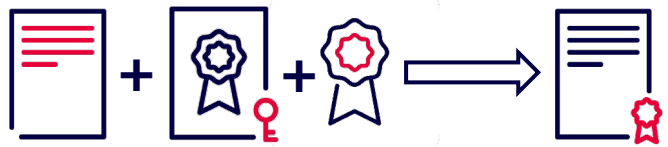
Zertifikat:

Ein **qualifizierter Vertrauensdienste-Anbieter (QVDA)**:
1. **identifiziert** Nutzer
2. stellt **qualifiziertes Zertifikat** aus



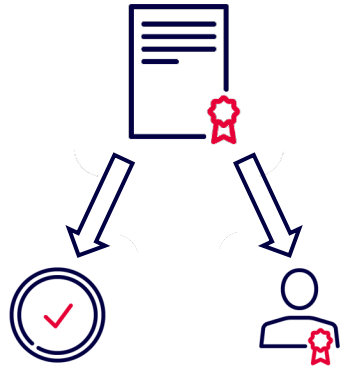
Signiertes Dokument:

besteht aus:
1. Dokument
2. Zertifikat
3. kryptographische Daten („elektronische Signatur“) erzeugt aus Geheimnis des Nutzers



Eine Signatur garantiert:

1. **Integrität** des Dokuments
2. **Absicht** und **Identität** des Unterzeichners



Vier Eigenschaften geben qualifizierten Signaturen die Rechtswirkung

qualifizierte elektronische Signatur (QES)

- Zertifikat ausgestellt durch **qualifizierten Vertrauensdiensteanbieter**
- Signatur wird von einer **qualifizierten Signaturerstellungseinheit** erstellt.
- Quelle der Zertifikatskette (Trust Anchor) steht auf der **EU Trusted List**
- Die kritischen Komponenten zur Erstellung sind **zertifiziert und reguliert**.

Rechtswirkung:
(eIDAS 1, Art. 25 (2))

„Eine qualifizierte elektronische Signatur hat die gleiche Rechtswirkung wie eine handschriftliche Unterschrift."

Qualifizierte Vertrauensdiensteanbieter betreiben hohen technischen und rechtlichen Aufwand, damit ihre Kunden von der Rechtwirkung profitieren!

RP nutzen die Wallet über einen Fernsignaturdienst

Beteiligte Parteien:

- „Relying Party“ (z.B. Bankwebseite)
- Fernsignaturdienst beim Qualifizierten Vertrauensdiensteanbieter (QVDA)
- Nutzer mit EUDI-Wallet

Ablauf aus Nutzersicht:

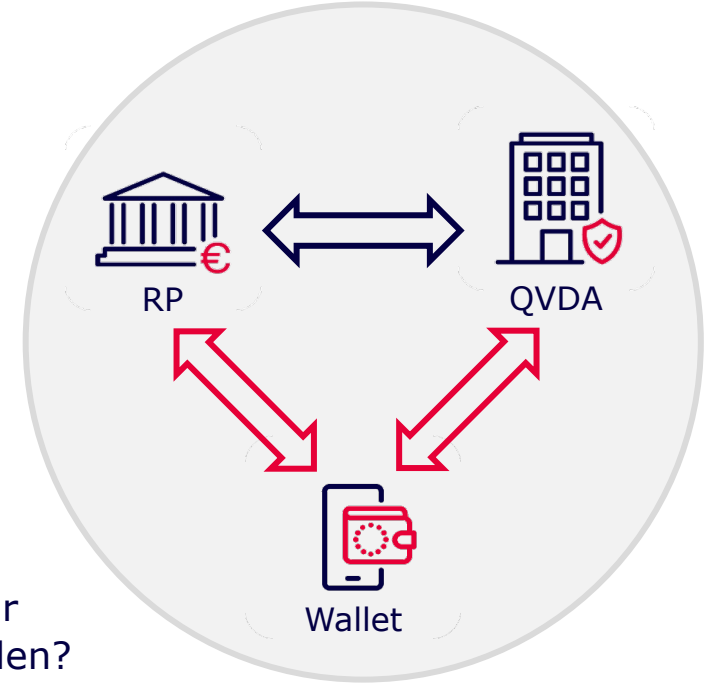
1. Relying Party **fordert Unterzeichnung** eines Dokumentes an.
2. Nutzer **identifiziert** sich oder **authentifiziert** sich beim QVDA.
3. Nutzer **unterzeichnet** das Dokument mittels Wallet.

Ablauf aus Sicht Relying Party:

Relying Party — Anforderung Signatur (die RP ist technisch und vertraglich an den Fernsignaturdienst angebunden) — Fernsignatur-dienst — **Identifizierung** ggf. Authentifizierung / **Freigabe** / Auslösung Signatur — EUDI-Wallet

Das vorgestellte Modell stellt den QVDA in den Mittelpunkt.
- Das entspricht etabliertem Modell der Fernsignatur

Kann die Wallet im Zentrum stehen?



Herausforderungen:

Die EUDI-Wallet ist (wahrscheinlich) **keine zertifizierte Signaturerstellungseinheit.** ⇒ Fernsignatur ist nötig!

Wie ist das **Geschäftsmodell**, wenn kein Vertrag zwischen RP und QVDA existiert? ⇒ RP ist interessiert an Signatur und sollte diese daher bezahlen?

Wie **leichtgewichtig** wird die Wallet? ⇒ Eine Funktionalität muss in **allen nationalen Wallets** vorhanden sein, bevor sie interoperabel benutzbar ist.

Weitere Herausforderungen

Handhabung großer oder vertraulicher Dokumente?

- Lesen langer Dokumente auf dem Smartphone?
- Übertragung großer Dokumente an Smartphone?
- Dürfen **vertrauliche Dokumente** die RP-Umgebung verlassen?
- Kann man Relying Parties bei der **Anzeige vertrauen**, wenn diese nicht vertraglich gebunden sind?

Was sichert das „what you see is what you sign"-Prinzip am besten ab?

Grenzüberschreitende Kompatibilität?

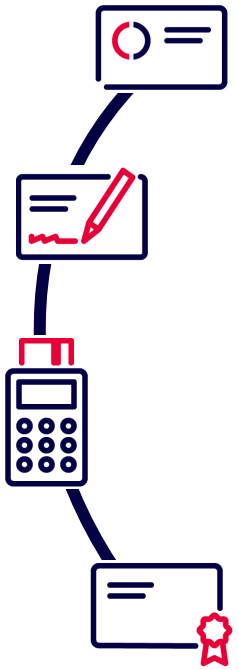
- Jeder QVDA mit jeder Wallet?
- Jede Wallet mit jeder RP?

Berücksichtigung bestehender Modelle der Mitgliedsstaaten?

- Übergang existierender Komponenten zu Wallet-Lösungen?

Ausblick

eIDAS 1-Mittel werden mit der Wallet zugänglicher



Gegenwart (eIDAS 1-Produkte)

- eID-Funktion (AusweisIdent*)
- Signaturkarten*
  Fernsignatur (sign-me*)
- Siegelkarten*
  Fernsiegel (seal-me*)

Entsprechung mit EUDI-Wallet

- Identifikation mit der Wallet
- Fernsignatur mit der Wallet
- Fernsiegel mit der Wallet
- Neu! Qualifizierte elektronische Attribute (QEAA)

*D-Trust Produkte

Mit der zukünftigen EUDI-Wallet…

- … haben wir alle ein **Gerät in der Tasche**, mit dem wir qualifiziert elektronisch unterschreiben können!
- … steht **Relying Parties** in ihren online-Workflows die QES zur breiten Verfügung. Das gibt eine **große Vereinfachung** ihrer Prozesses, auf die sie warten.
- … ergibt sich großes Potential für weitere Anwendungen. („Endlich **papierlos**!“)
- Mit der QES-Funktionalität ergibt sich ein starker Anreiz für die **Nachfrage nach der Wallet!**

Entscheidend: breite und **einfache Verfügbarkeit** der QES-Funktionalität in der Wallet für jeden Bürger.

Vielen Dank.

Dr. Mark Ullmann

Bundesdruckerei GmbH
Solution Architect, D-Trust GmbH
E-Mail: Mark.Ullmann@d-trust.net

Teil der Bundesdruckerei-Gruppe

Anhang

Beispiel signiertes Dokument (Foxit und Acrobat)