

# 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

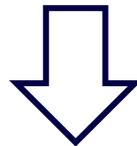
- Solution Architect bei der D-Trust GmbH, einer Tochtergesellschaft der Bundesdruckerei GmbH
- Mitglied im Large Scale Pilot Potential, für den Use Case 5 "Qualifizierte Elektronische Signatur"



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



**EUDI-Wallet**



Identifikation



**Ausweis**

qualifizierte elektronische  
Signatur (QES)



**Unterschrift**



(qualifizierte) elektronische  
Nachweise (QEAA)

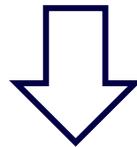


**Führerschein  
Bescheinigungen**

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



**EUDI-Wallet**



qualifizierte elektronische  
Signatur (QES)



**Unterschrift**



(qualifizierte) elektronische  
Nachweise (QEAA)



**Führerschein  
Bescheinigungen**



Identifikation



**Ausweis**

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 Vertrauensdiensteanbieter (QVDA)**:

1. **identifiziert** Nutzer
2. stellt **qualifiziertes Zertifikat** aus



## Signiertes Dokument:

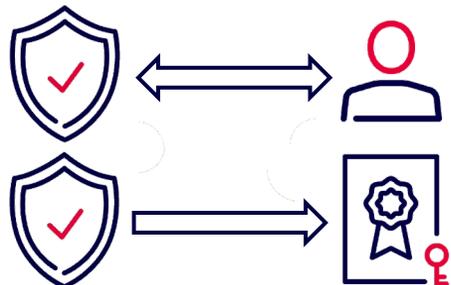
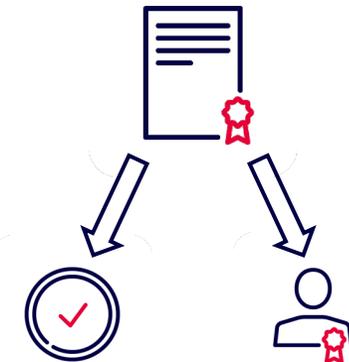
besteht aus:

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 Vertrauensdiensteanbieter betreiben hohen technischen und rechtlichen Aufwand, damit ihre Kunden von der Rechtswirkung 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:

 Relying Party **fordert Unterzeichnung**  
eines Dokumentes an.

Nutzer **identifiziert** sich oder  
**authentifiziert** sich beim QVDA.

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?

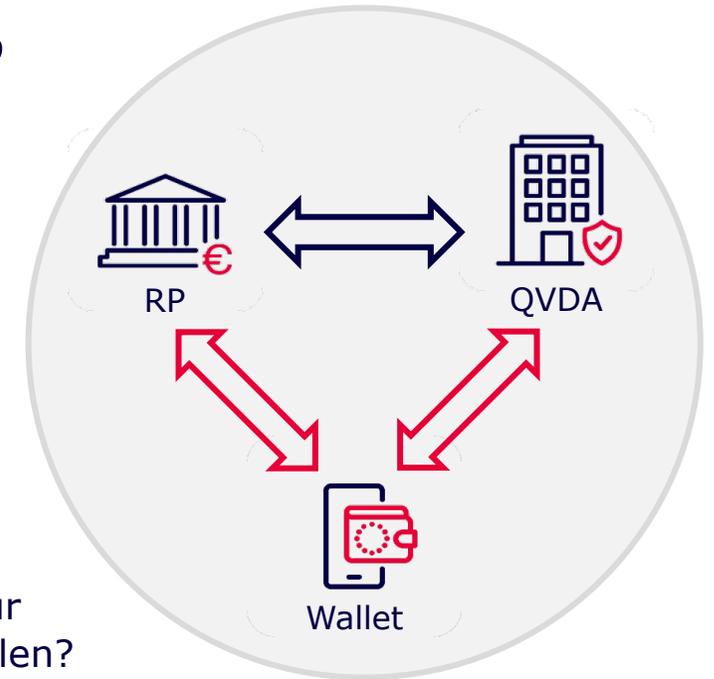


RP ist interessiert an Signatur und sollte diese daher bezahlen?

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\*)



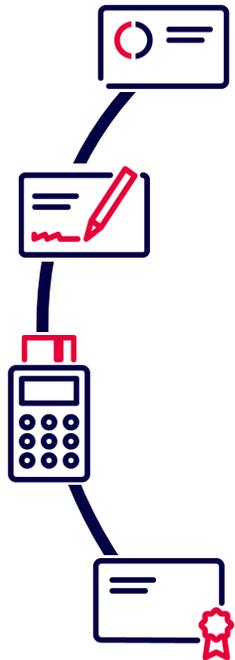
## Entsprechung mit EUDI-Wallet

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](mailto:Mark.Ullmann@d-trust.net)

Hinweis: Diese Präsentation ist Eigentum der Bundesdruckerei GmbH.  
Sämtliche Inhalte – auch auszugsweise – dürfen nicht ohne die Genehmigung der Bundesdruckerei GmbH vervielfältigt, weitergegeben oder veröffentlicht werden.  
© 2024 by Bundesdruckerei GmbH.

Teil der  
Bundesdruckerei-  
Gruppe

The logo for bdr, consisting of the lowercase letters 'bdr' in a bold, sans-serif font. The 'b' is black, the 'd' is red, and the 'r' is black.

# Anhang

# Beispiel signiertes Dokument (Foxit und Acrobat)

The screenshot shows the 'Digital Signatures' panel in Foxit Reader. The main heading is 'Digital Signatures'. Below it, there is a section for 'Rev.1:Signed by MARK ULLMANN'. Under this, there are two sub-sections: 'Signature is valid:' and 'Signature Details'. The 'Signature is valid:' section contains the following text: 'Source of Trust obtained from European Union Trusted Lists (EUTL).', 'This is a Qualified Electronic Signature according to EU Regulation 910/2014', 'The document has not been modified since this signature was applied.', 'The signer's identity is valid.', 'The signature includes an embedded timestamp but it could not be verified.', and 'Signature is LTV enabled'. The 'Signature Details' section contains 'Certificate Details...', 'Last Checked: 2023.12.14 10:40:07+01'00'', 'Field: sign-me-44fd8908e397c828fd9931d5d1141457 on page 1', and 'Click to view this version'. The top of the panel shows a toolbar with icons for Hand, Select, Snapshot, Clipboard, Bookmark, Zoom, Page Fit Option, Reflow, Rotate View, Edit Text, Edit Object, and Typewriter.

The screenshot shows the 'Unterschriften' (Signatures) panel in Adobe Acrobat. At the top, there is a status bar that says 'Unterscriben und alle Unterschriften sind gültig.' Below this, there is a section for 'Unterschriften' with a close button. Underneath, there is a button 'Alle prüfen'. Below that, there is a section for 'Revision 1: Unterscriben von MARK ULLMANN'. This section contains the following text: 'Unterschrift ist gültig:', 'Vertrauensquelle erhalten von European Union Trusted Lists (EUTL).', 'Dies ist eine qualifizierte elektronische Signatur gemäß EU-Verordnung 910/2014.', 'Dokument wurde nach dem Unterscriben nicht mehr geändert.', 'Identität des Unterzeichners ist gültig.', 'Die Signatur ist mit einem eingebetteten Zeitstempel versehen.', and 'Unterschrift ist LTV-fähig'. Below this, there is a section for 'Unterschriftsinformationen' which contains: 'Grund: Test.pdf', 'Ort: SignMeWebApp / www.sign-me.de', 'Zertifikatdetails...', 'Zuletzt geprüft: 2023.12.14 10:45:39 +01'00'', 'Feld: sign-me-44fd8908e397c828fd9931d5d1141457 auf Seite 1', and 'Klicken Sie, um diese Version anzuzeigen.' The top of the panel shows a toolbar with icons for Save, Print, Email, and Search.