

# Wie kann die künftige EU DI Wallet sicher in der öffentlichen Verwaltung angewendet werden?

Omnisecure, Berlin, 22.01.2024

# Gliederung

Wallet-Eigenschaften

ID-Mittel auf VN hoch

QEAA und QES

Sicherheitsfragen

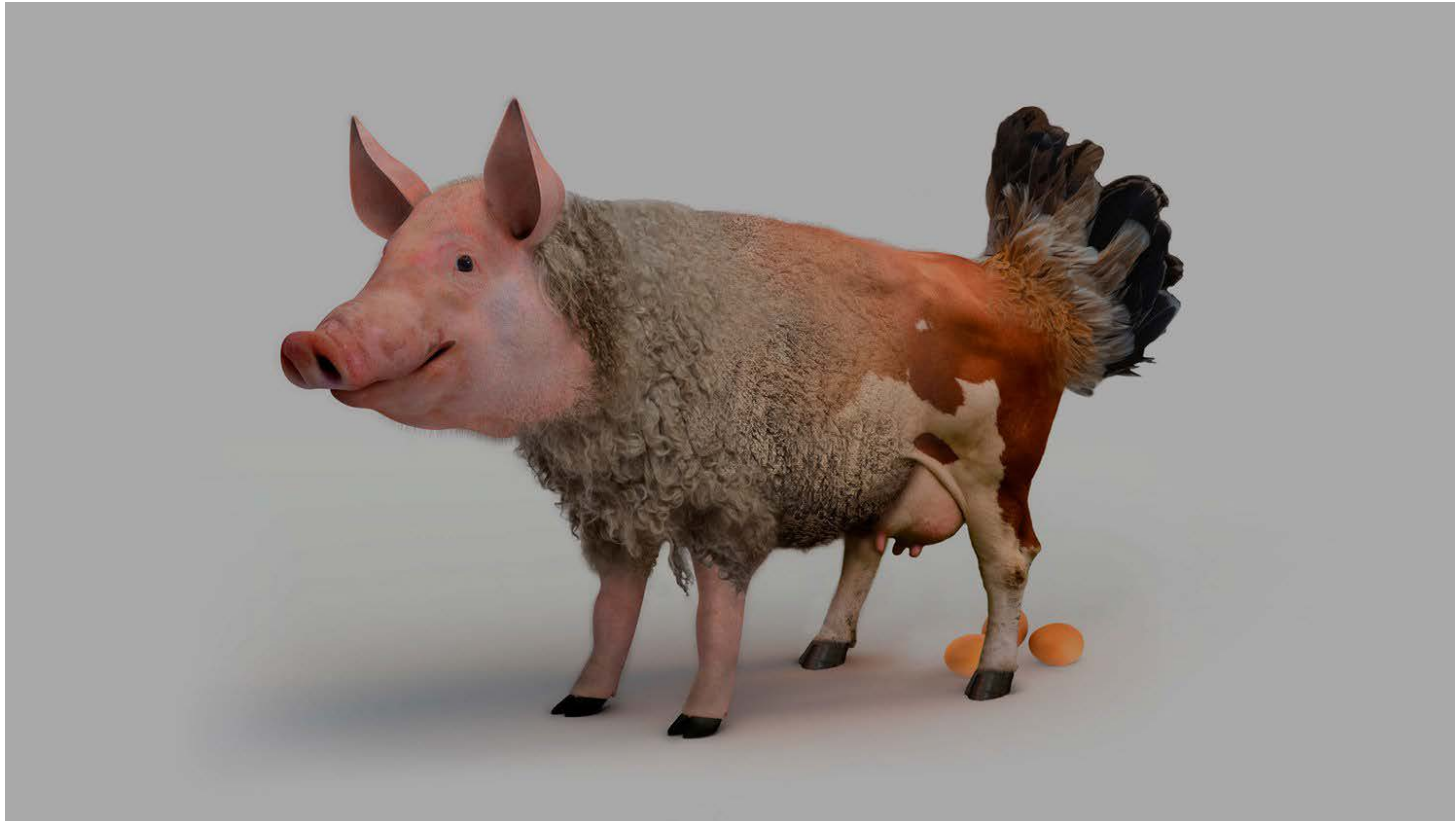
Angestrebte Ergebnisse



## Was wird die EU DI Wallet sein bzw. können?

- Relying on the **level of assurance “high”** (Erwägungsgrund 19, eIDAS-VO 2.0)
- should also allow users to **create and use qualified electronic signatures** and seals (s.o.)
- electronic identification means ... **person identification data** and, where applicable, **in combination with electronic attestations of attributes** (Artikel 6a, Abs. 4 (a) eIDAS-VO 2.0)
- offer the ability to **sign by means of qualified electronic signatures** to all natural persons by default (Artikel 6a, Abs. 4 (e) eIDAS-VO 2.0)
- shall be provided under an electronic identification scheme with assurance level high (Artikel 6a, Abs. 11 eIDAS-VO 2.0)





# Wie wird die EU DI Wallet ein ID-Mittel auf Vertrauensniveau „hoch“?

- Level high = Level substantial, plus:
- 1. The electronic identification means protects against duplication and tampering against attackers with high attack potential.
- Factor-specific examples of protection against tampering and duplication, include:
- Possession-based authentication factors: **embed cryptographic key material in tamper-resistant hardware** that prevents the key from being extracted outside the device either or manipulated in the device through physical or electronic means, hardware security module

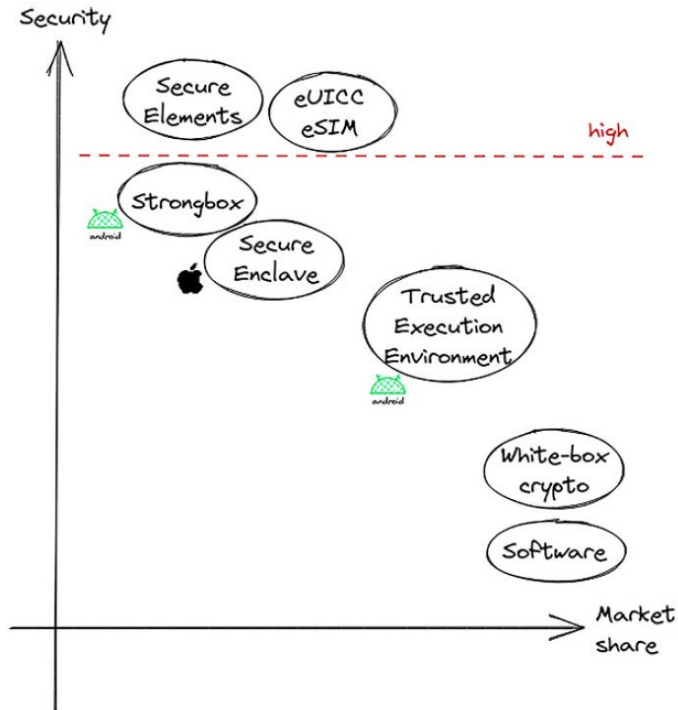
(Guidance for the application of the levels of assurance which support the eIDAS Regulation, 2.2.1 Electronic identification means characteristics and creation)

# Wie wird die EU DI Wallet ein ID-Mittel auf Vertrauensniveau „hoch“?

Dies ergibt sich aus:

- STORK und die **ISO-Norm 29115** beziehen sich unter anderem auf die **Niveaus 2, 3 und 4, die** so weit wie möglich bei der Festlegung technischer Mindestanforderungen, Normen und Verfahren **für die Sicherheitsniveaus „niedrig“, „substanziell“ und „hoch“** im Sinne dieser Verordnung **berücksichtigt werden sollten** (Erwägungsgrund 16, eIDAS-VO 1.0, deutsch)
- **LoA4** is similar to LoA3, but it **adds** the requirements of in-person identity proofing for human entities and **the use of tamper-resistant hardware devices for the storage of all secret or private cryptographic keys** (International Standard ISO/IEC 29115, 2013)

# Wie wird die EU DI Wallet ein ID-Mittel auf Vertrauensniveau „hoch“?



Konzepte für sichere wallets in dezentralen Identitätsökosystemen, Bastian, Kraus, Fischer, Bundesdruckerei GmbH  
HMD Praxis der Wirtschaftsinformatik (2023) 60:381–404

## Wie wird die Vertrauenswürdigkeit von „Qualified electronic attestations of attributes (QEAA)“ sichergestellt?

- When issuing ... a qualified electronic attestation of attributes, a qualified trust service provider **shall verify the identity** and, if applicable, any specific attributes of the **natural ... person**
- The **verification of the identity** referred to in the first subparagraph shall be verified, by appropriate means, by the qualified trust service provider... **based on one of the following methods or on a combination thereof**
- (a) by means of the **European Digital Identity Wallet or a notified electronic identification means** which meets the requirements set out in Article 8 **with regard to the assurance level ‘high’**;  
(c) by using **other identification methods** which ensure the **identification of the person with a high level of confidence**, the conformity of which shall be confirmed by a conformity assessment body;

(Artikel 24, Abs. 1, 1a eIDAS-VO 2.0)



# Wie wird die Vertrauenswürdigkeit von „Qualified electronic attestations of attributes (QEAA)“ sichergestellt?

Requirements for qualified electronic attestation of attributes (Artikel 45d eIDAS-VO 2.0)

- 5. By ... [**6 months after** the date of the entering into force of this amending **Regulation**], the Commission shall, **by means of implementing acts, establish a list of reference standards** and when necessary, **establish specifications and procedures** for qualified electronic attestations of attributes.

# Wie wird die Vertrauenswürdigkeit von „Qualified electronic attestations of attributes (QEAA)“ sichergestellt?

Verification of attributes against authentic sources (Artikel 45e eIDAS-VO 2.0)

- 1. Member States shall ensure within **24 months after** entry into force of the **implementing acts ...** that, at least for the attributes listed in Annex VI, wherever these attributes rely on authentic sources within the public sector, measures are taken to **allow qualified trust service providers of electronic attestations of attributes to verify these attributes by electronic means ...**
- 2. By ... [**6 months after** the date of the entering into force of this amending **Regulation**], the Commission shall, taking into account relevant international standards, **by means of implementing acts, establish a list of reference standards** and when necessary, **establish specifications and procedures** for the catalogue of attributes and schemes for the attestation of attributes and **verification procedures for qualified electronic attestations of attributes.**

## Wie wird die Vertrauenswürdigkeit von „Qualified electronic attestations of attributes (QEAA)“ sichergestellt?

Hierzu gehören nach Annex VI (Minimum List of Attributes) der eIDAS-VO 2.0 u.a.:

- 4. Personenstand;
- 5. Familienzusammensetzung;
- 7. Bildungsabschlüsse, Titel und Lizenzen;
- 8. Berufsqualifikationen, Titel und Lizenzen;
- 9. Befugnisse und Mandate zur Vertretung natürlicher oder juristischer Personen
- 10. Öffentliche Genehmigungen und Lizenzen;

# Wie wird die Vertrauenswürdigkeit von „Qualified electronic attestations of attributes (QEAA)“ sichergestellt?

Hierzu gehören nach Annex VI (Minimum List of Attributes) der eIDAS-VO 2.0 u.a.:

- 4. Personenstand; **4.500 Standesämter in D**
- 5. Familienzusammensetzung;
- 7. Bildungsabschlüsse, Titel und Lizenzen; **422 Hochschulen und über 11.000 weiterführende Schulen in D**
- 8. Berufsqualifikationen, Titel und Lizenzen; **Über 8.000 Berufsschulen in D**
- 9. Befugnisse und Mandate zur Vertretung natürlicher oder juristischer Personen
- 10. Öffentliche Genehmigungen und Lizenzen;

# Wie wird die Vertrauenswürdigkeit von „Qualified electronic attestations of attributes (QEAA)“ sichergestellt?

- Annex V REQUIREMENTS FOR QUALIFIED ELECTRONIC ATTESTATION OF ATTRIBUTES

Qualified electronic attestation of attributes **shall contain:**

(g) the qualified electronic signature or **qualified electronic seal of the issuing qualified trust service provider;**

ANNEX VII REQUIREMENTS FOR ELECTRONIC ATTESTATION OF ATTRIBUTES ISSUED BY OR ON BEHALF OF A PUBLIC BODY RESPONSIBLE FOR AN AUTHENTIC SOURCE

1. An electronic attestation of attributes issued by or on behalf of a public body responsible for an authentic source **shall contain:**

(b) a set of data unambiguously representing the public body issuing the electronic attestation of attributes ...

(g) the qualified electronic signature or **qualified electronic seal of the issuing body;**

(i) the **information** or location of the services that can be used to enquire **about the validity status of the attestation.**



# Wie müssen sich Wallet-Inhaber registrieren, um (remote) qualifiziert signieren zu können?

- 1) When issuing a qualified certificate ..., a **qualified trust service provider shall verify the identity ... of the natural ... person** to whom the qualified certificate ... will be issued.
  - 1a) The **verification of the identity** referred to in the first subparagraph shall be verified, by appropriate means, by the qualified trust service provider... **based on one of the following methods or on a combination thereof ... :**
    - (a) by means of the **European Digital Identity Wallet or a notified electronic identification means** which meets the requirements set out in Article 8 **with regard to the assurance level 'high'**;
    - (c) by using **other identification methods** which ensure the **identification of the person with a high level of confidence**, the conformity of which shall be confirmed by a conformity assessment body;

(Artikel 24 eIDAS-VO 2.0)

# Identifizierungsanforderungen nach Artikel 24 eIDAS-VO alt und neu

<p>(a) by the <b>physical presence</b> of the natural person or of an authorised representative of the legal person; or</p>	<p>(d) through the <b>physical presence</b> of the natural person or of an authorised representative of the legal person by appropriate procedures and in accordance with national laws.</p>
<p>(b) remotely, using electronic identification means, for which prior to the issuance of the qualified certificate, a physical presence of the natural person or of an authorised representative of the legal person was ensured and which <b>meets the requirements</b> set out in Article 8 <b>with regard to the assurance levels 'substantial' or 'high'</b>; or</p>	<p>(a) by means of the European Digital Identity Wallet or a notified electronic identification means which <b>meets the requirements</b> set out in Article 8 <b>with regard to the assurance level 'high'</b>;</p>
<p>(c) by means of a <b>certificate of a qualified electronic signature</b> or of a qualified electronic seal issued <b>in compliance with point (a) or (b)</b>; or</p>	<p>(b) by means of a <b>certificate of a qualified electronic signature</b> or of a qualified electronic seal issued <b>in compliance with point (a), (c) or (d)</b>.</p>
<p>(d) by using other identification methods recognised at national level which provide <b>equivalent assurance in terms of reliability to physical presence</b>. The equivalent assurance shall be confirmed by a conformity assessment body.</p>	<p>(c) by using other identification methods which ensure the <b>identification of the person with a high level of confidence</b>, the conformity of which shall be confirmed by a conformity assessment body;</p>

# Wie könnten Registrierung für und Authentisierung einer remote QES in einem Schritt erfolgen?

Technische Alternative der "On-the-Fly" Signatur mit der Online-Ausweisfunktion als Kombination von Registrierung und Authentisierung in einem Schritt mit den Vorteilen

- keine vorherige Registrierung bei einem Vertrauensdiensteanbieter nötig
- QES-Erstellung ad-hoc möglich

Nähere Informationen unter <https://www.personalausweisportal.de/Webs/PA/DE/wirtschaft/eIDAS-konforme-fernsignatur/eidas-konforme-fernsignatur-node.html;jsessionid=32A04DCAC99DD64ECB571DE29D4C4A61.live882#doc14620566bodyText3>

## Beispiele zu regelnder Fragen mit Bezug zur IT-Sicherheit der Wallet:

- Wie erreicht die EU DI Wallet als ID-Mittel Vertrauensniveau hoch, wenn Secure Elements oder eUICCs noch nicht so weit verbreitet sind? Ausweiskarten-Auslesen per Smartphone wie bislang?
- Wie können die Relying Parties (zB Arbeitgeber, Standesämter) prüfen, dass von QTSPs bereitgestellte und in der Wallet gespeicherte QEAs aus einer authentischen Quelle stammen und valide sind (Artikel 45e, 45f, Annexe V und VII)?
- Müssen die anderen Identifizierungsmethoden zur Personenidentifizierung mit einem „high level of confidence“ den Anforderungen an Wallet oder notifizierten ID-Mitteln (= Vertrauensniveau hoch) entsprechen?
- Wie wird sichergestellt, dass der QES-Ersteller als Wallet-Inhaber auch die Person ist, der die QES zugerechnet werden soll? Muss das Auslösen der QES (Authentisierung) auf dem gleichen Vertrauensniveau wie die Registrierung erfolgen?

## Beteiligung des BSI (Referat DI 15) am LSP, Erkenntnisse für die ÖV

- DI 15 ist im BSI für eID-Lösungen für die digitale Verwaltung zuständig (hierzu gehören nicht nur Empfehlungen für den eID-Einsatz sondern auch zur Anwendung von Vertrauensdiensten)
- European Digital Identity Wallets shall ensure security-by-design (Artikel 6a, Abs. 12 eIDAS-VO 2.0)
- Mitarbeit in den Potential-Use Cases 5 (QES) und 1 (eGovernment Services, angefragt). Rolle hierbei v.a. als Sparringspartner für IT-Sicherheit der Spezifikationsautoren
- Im Ergebnis seiner Mitarbeit, Erstellung eines Handlungsleitfadens für die deutsche öffentliche Verwaltung zur sicheren Anwendung der EU DI Wallet geplant, um damit auch deren künftige sichere Nutzung zu fördern. Beispiele:
  - Verwendung von QEAA (ÖV als Relying Party)
  - Verwendung von EAA anderer ÖVn oder in deren Namen erstellter EAA




# Vielen Dank für Ihre Aufmerksamkeit!

## Kontakt

Michael Klabe  
Referent im Referat DI 15

michael.klabe@bsi.bund.de  
Tel. +49 (0) 228 9582 6089  
Fax +49 (0) 228 10 9582 6089

Bundesamt für Sicherheit in der Informationstechnik (BSI)  
Godesberger Allee 185-189  
53175 Bonn  
[www.bsi.bund.de](http://www.bsi.bund.de)



Das BSI als die Cybersicherheitsbehörde des Bundes gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft.