

Digitale Identitäten und Souveränität – Das neue EUDI-Wallet als Innovation made in the EU?

Simon Tannen, LL.M. (CGSL) **Johannes Noller**
Taylor Wessing CMS Hasche Sigle

Herbstakademie 2026

Die Verwaltung digitaler Identitäten

Heute: für viele Teilidentitäten eigene Verfahren

Künftig: EIN Instrument für viele Nachweise - EUDI-Wallet



Video-Ident



Post-Ident



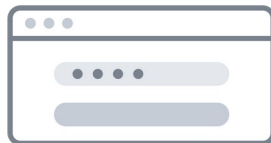
eID mit Lesegerät und PIN



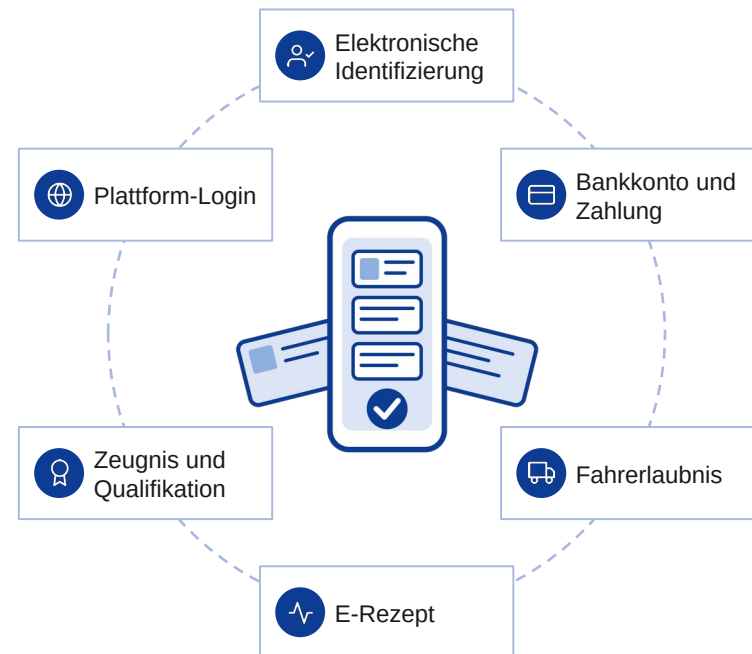
Führerschein in Papierform



Zeugnis per Post



Passwort und Single-Sign-on



Digitale Souveränität und ihre Dimensionen



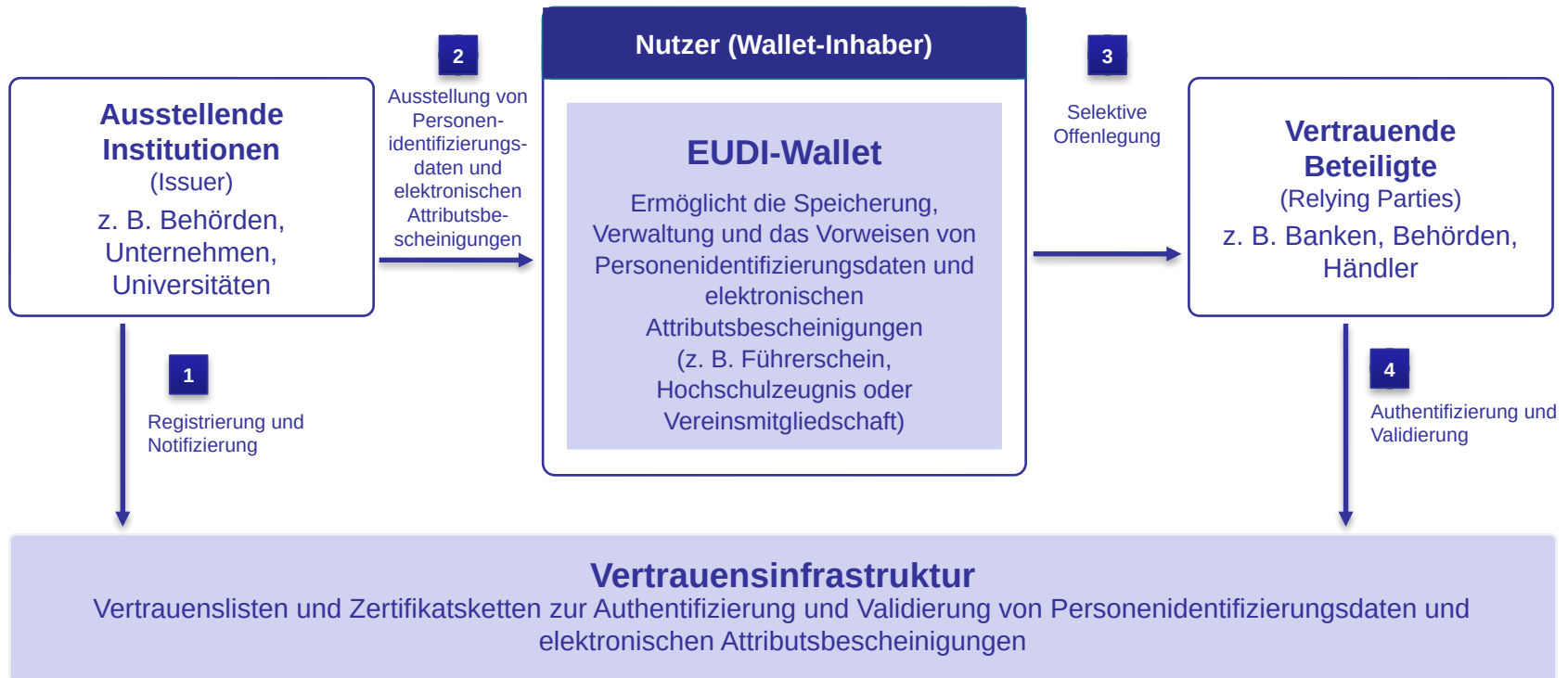
Dimensionen nach Beyerer, Müller-Quade, Reussner, DuD 2018, 277

Agenda

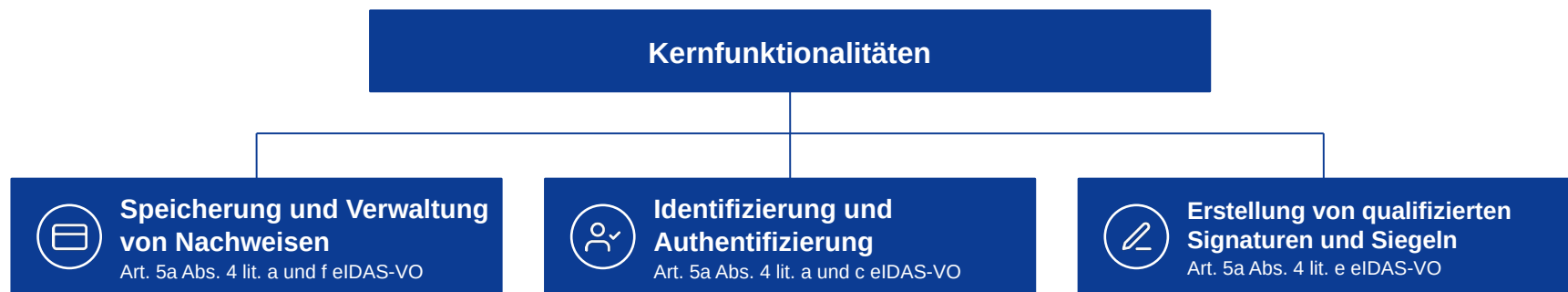
- I. Einleitung: Digitale Identitäten und Souveränität
- II. Europäisches Identitätsökosystem und EUDI-Wallet
 - 1. Anwendungsfelder
 - 2. Ökosystem
 - 3. Funktionalitäten
 - 4. Bereitstellung und Akzeptanzpflichten
 - 5. Vertrauensinfrastruktur
- III. Beispiel: Compliance mit den Jugendschutzvorgaben des DSA
 - 1. Relevanz von Maßnahmen zur Altersfeststellung
 - 2. Pflicht zu Jugendschutzmaßnahmen nach Art. 28 DSA
 - 3. Das EUDI-Wallet als rechtskonforme Technologie zur Altersüberprüfung und neuer Bestandteil des Online-Jugendschutzes
- IV. Fazit

II. Europäisches Identitätsökosystem und EUDI-Wallet

Europäisches Identitätsökosystem



Kernfunktionalitäten des EUDI-Wallets



Das EUDI-Wallet - Beispielhafte Anwendungsfelder



Finanzsektor

- KYC- und AML-Prüfungen
- Identifizierung bei Kontoeröffnung
- Freigabe von Zahlungsvorgängen
- Automatisierte Kreditwürdigkeitsprüfungen



Bildung und Beruf

- Elektronischer Nachweis von Bildungsabschlüssen
- Beschleunigt Bewerbungs-, Onboarding- und Berechtigungsprozesse



Gesundheitssektor

- E-Rezept
- Krankenversicherungskarte und sozialversicherungsrechtliche Nachweise
- Elektronische Patientenakte



Nachweise im B2C-Bereich

- Bahntickets
- Hotelbuchungen
- Fahrerlaubnis für Mietwagenzugang



Behörden und Verwaltung

- Elektronisches Steuerverfahren
- Hochschulbewerbungen
- Nachweis Führerschein bei Verkehrskontrolle



Zugangsmanagement

- Authentifizierung bei physischen Zutrittskontrollen (z.B. Fitnessstudios oder Forschungseinrichtungen)
- Zugriff auf geschützte IT-Systeme



Unternehmensorganisation

- Nachweise von Funktionen und Qualifikationen, Berechtigungen
- Nachweis von Vertretungsbefugnissen



Jugendschutz

- Datensparsame Altersnachweise, die allein die Erfüllung einer Altersschwelle übermitteln



Digitale Rechte- und Zugriffsverwaltung

- Verwaltung und Prüfung von Nutzungs-, Lizenz- und Zugangsrechten an digitalen Inhalten wie E-Books, Musik oder Filmen

Personenidentifizierungsdaten und Attributsbescheinigungen



Personenidentifizierungs- daten (PID) Art. 3 Nr. 3 eIDAS-VO

- **Begriff:** Daten, die im Einklang mit nationalem oder Unionsrecht ausgestellt werden und die Identität einer natürlichen oder juristischen Person eindeutig repräsentieren.
- **Ausstellung:** Durch von den Mitgliedstaaten bestimmte und notifizierte Institutionen (Deutschland über Online-Ausweisfunktion des Personalausweises).
- **Inhalt:** Vor- und Nachname, Geburtsdatum, Geburtsort und Staatsangehörigkeit; für juristische Personen Name und eindeutige Kennung (Anhang Tab. 1 und 3 der DVO (EU) 2024/2977).



Elektronische Attributsbescheinigungen Art. 3 Nr. 43 bis 46 eIDAS-VO



„Einfache“ Attributs- bescheinigungen

- **Aussteller:** nicht-qualifizierte Vertrauensdiensteanbieter
- **Anforderungen:** Geringe Anforderungen
- **Einsatzbsp.:** Mitgliedsausweise, Eintrittskarten, Fahrscheine



Rechts- und Beweiswirkung:
Darf nicht allein wegen elektronischer Form oder fehlender Qualifizierung abgesprochen werden.



Qualifizierte Attributs- bescheinigungen

- **Aussteller:** qualifizierte Vertrauensdiensteanbieter
- **Anforderungen:** Insb. qual. Signatur / Siegel d. Ausstellers sowie Identitäts- und Attributsprüfung
- **Einsatzbsp.:** Vertretungsvollmacht



Rechts- und Beweiswirkung:
Selbe Rechtswirkung wie rechtmäßig ausgestellte Bescheinigungen in Papierform (Art. 45b Abs. 3).



Attributs- bescheinigungen authentischer Quellen

- **Aussteller:** zuständige öffentliche Stelle oder Dritte
- **Einsatzbsp.:** Genehmigungen, Lizenzen, Registerauskünfte



Anforderungen an das EUDI-Wallet

 Nutzungsmodalitäten	Unentgeltlichkeit Für natürliche Personen kostenfrei (Art. 5a Abs. 13); Beschränkung auf nichtgewerbliche Zwecke möglich (Art. 5a Abs. 5 UAbs. 2 eIDAS-VO).	Freiwilligkeit Keine Benachteiligung bei Nichtnutzung; Zugang zu Diensten über alternative Identifizierungsmittel (Art. 5a Abs. 15 eIDAS-VO).
 Transparenz und Kontrolle	Änderungssicheres Dashboard Übersicht über Transaktionen, vertrauende Beteiligte und weitergegebene Informationen (Art. 5a Abs. 4 lit. d eIDAS-VO). Selektive Offenlegung Preisgabe nur zweckerforderlicher Daten (Art. 5a Abs. 4 lit. a, Erwgr. 59).	Betroffenenrechte Datenübertragbarkeit, Löschung (Art. 17 DSGVO) und Meldung an die Aufsichtsbehörde (Art. 5a Abs. 4 lit. d Ziff. ii bis iv, lit. g). Pseudonyme Selbstgewählte Pseudonyme, verschlüsselt lokal gespeichert (Art. 5, Art. 5a Abs. 4 lit. b). Zero-Knowledge-Proofs Binäre Verifikation ohne Datenoffenlegung, Grenze: Identifizierungspflichten (z.B. §11 Abs. 1 GWG).
 Verarbeitung beim Anbieter	Datenminimierung Nutzungsinformationen nur, soweit für die Dienste erforderlich (Art. 5a Abs. 14).	Verknüpfung nur auf Verlangen Kombination mit Daten eigener oder fremder Dienste nur auf ausdrückliches Verlangen des Nutzers (Art. 5a Abs. 14). Logische Trennung Trennung von sonstigen Daten, bei privaten Anbietern.

➔ Beitrag zur Datensouveränität durch selbstbestimmte Verwaltung digitaler Identitäten

Bereitstellung, Zertifizierung und Anerkennung

Bereitstellung des EUDI-Wallets (Art. 5a Abs. 2 eIDAS-VO)



Durch den Mitgliedstaat

Art. 5a Abs. 2 Buchst. a

Der Mitgliedstaat stellt das Wallet selbst bereit.



Im Auftrag des Mitgliedstaats

Art. 5a Abs. 2 Buchst. b

Private Anbieter stellen das Wallet im Auftrag und unter der Verantwortung des Mitgliedstaats bereit.



Private Anbieter

Art. 5a Abs. 2 Buchst. c

Private Anbieter stellen das Wallet unabhängig vom Staat bereit. Erforderlich ist die Anerkennung durch den Mitgliedstaat.

Akzeptanzpflichten

Akzeptanzpflichten nach Art. 5f eIDAS-VO



Öffentliche Stellen Art. 5f Abs. 1 eIDAS-VO

Adressat

Öffentliche Stellen der Mitgliedstaaten.

Auslöser

Soweit für den Zugang zu einem von einer öffentlichen Stelle erbrachten Online-Dienst eine elektronische Identifizierung und Authentifizierung verlangt wird.



Private vertrauende Beteiligte Art. 5f Abs. 2 eIDAS-VO

Adressat

Private vertrauende Beteiligte, ausgenommen Kleinst- und kleine Unternehmen (Empfehlung 2003/361/EG, Art. 2 des Anhangs).

Auslöser

Pflicht zur Online-Identifizierung mit starker Nutzerauthentifizierung (Art. 3 Nr. 51 eIDAS-VO) aus Unionsrecht, nationalem Recht oder vertraglicher Abrede.

Sektoren

Verkehr, Energie, Bankenwesen, Finanzdienstleistungen, soziale Sicherheit, Gesundheit, Trinkwasser, Postdienste, digitale Infrastrukturen, Bildung, Telekommunikation.



Sehr große Online-Plattformen Art. 5f Abs. 3 eIDAS-VO

Adressat

Anbieter sehr großer Online-Plattformen nach Art. 33 DSA (VO (EU) 2022/2065).

Auslöser

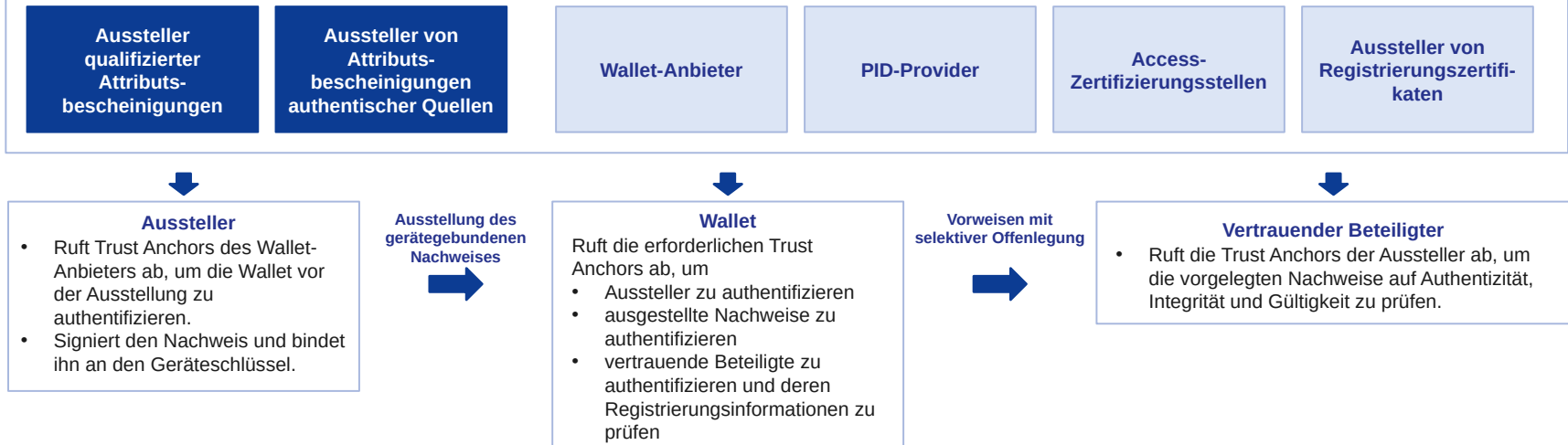
Verlangen einer Nutzerauthentifizierung für den Zugang zu Online-Diensten.

Modalität

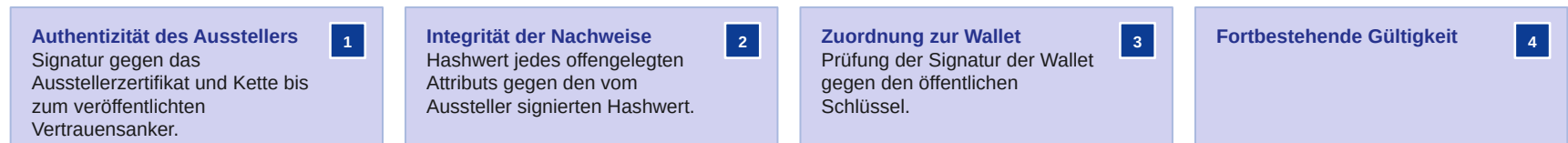
Akzeptieren und erleichtern, nur auf freiwilliges Verlangen des Nutzers und nur mit den Mindestdaten, die für den konkreten Dienst erforderlich sind.

Vertrauensinfrastruktur (stark vereinfacht)

Vertrauenslisten und Listen vertrauenswürdiger Stellen



Prüfung von Nachweisen durch den vertrauenden Beteiligten



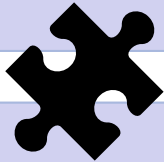
➔ Beitrag zur Infrastruktursouveränität durch europäische Vertrauensinfrastruktur

III. Beispiel: Compliance mit den Jugendschutzvorgaben des DSA

Jugendschutz: Ausgangslage und Pflichtenrahmen



Ausgangslage



Rechtsgrundlagen



Art. 28 Abs. 1 DSA Zentrale Norm

Anbieter von Online-Plattformen, die für Minderjährige zugänglich sind
(P) „geeignete und verhältnismäßige Maßnahmen“



Art. 28b Abs. 3 UAbs. 3 lit. f AVMD-RL Sektorspezifisch

Nennt Altersverifikationsmaßnahmen ausdrücklich; allerdings beschränkt auf Video-Sharing-Plattformen
(P) Überschießende Umsetzung



§ 4 Abs. 2 S. 2 JMStV „Geschlossene Benutzergruppen“

Bei jugendgefährdenden Inhalten (bspw. Pornografie)



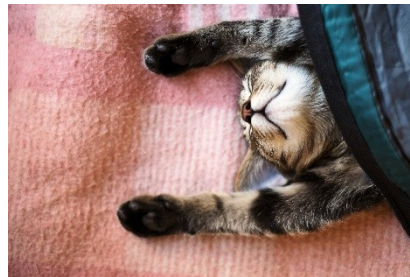
§ 24a Abs. 2 JuSchG Nationale Umsetzung AVMD-RL

Konkurrenzfragen zu Art. 28 DSA und dem Herkunftslandprinzip
(P) Sperrverfügungen // EuGH C-188/24 und C-190/24 (Frankreich)

Art. 28 DSA: sehr weit und auslegungsbedürftig



Anwendungsbereich - weites Verständnis
Art. 3 lit. i, Art. 28 Abs. 1 DSA



„Anbieter von Online-Plattformen, die für Minderjährige zugänglich sind, müssen [...]“

Weites Verständnis: Art. 28 DSA erfasst grundsätzlich alle Plattformen, es sei denn, Minderjährige werden wirksam vom Zugang ausgeschlossen.

Ausschluss in AGB reicht nicht: trotz Erwgr. 71 S. 2 DSA

Folge: Bereits auf Ebene des Anwendungsbereichs Frage nach wirksamen altersbezogenen Zugangsbeschränkungen.



Maßnahmen zum Minderjährigenschutz - offener Pflichtenmaßstab
Risikobasierte und technikoffene Regulierung



„[...] geeignete und verhältnismäßige Maßnahmen ergreifen, um für ein hohes Maß an Privatsphäre, Sicherheit und Schutz von Minderjährigen innerhalb ihres Dienstes zu sorgen.“

Rechtsunsicherheit: wann welche Maßnahme erforderlich vs. Art. 28 Abs. 3 + Erwgr. 71 S. 7 DSA

Spannungsfeld: datenschutzrechtliche Vorgaben, technische Machbarkeit und Nutzerakzeptanz

Folge: Leitlinien der Kommission sehnsüchtig erwartet

Altersfeststellung - nach C 2025/5519 erforderlich?

„Zugangsbeschränkungen auf der Grundlage von Methoden der Altersfeststellung bzw. -überprüfung“

Ob

- Risikobewertung des Anbieters
- Nicht erschöpfender Maßnahmenkatalog (eine von verschiedenen Maßnahmen, Risikobasiert)
- Unter Berücksichtigung allgemeiner Grundsätze (u.a. Wahrung By-Design-Grundsätze)

Wie

- Eigenerklärung
- Altersschätzung
- Altersüberprüfung

Wann ist eine Altersüberprüfung auch Sicht der EU-Kommission „*geeignet und verhältnismäßig*“ (dh erforderlich)?

Inhärent hochriskantes Angebot

Alkohol, Drogen, Glücksspiel, Pornografie - und mildere Maßnahmen reichen nicht aus.

Volljährigkeit nach AGB

Anbieter selbst verlangt in AGB Volljährigkeit der Nutzer.

Anderweitig nicht beherrschbare Risiken

anonymes Messaging, Live-Chat oder Content-Sharing.

Gesetzliches Mindestalter

Für den Zugang zum Dienst oder zum Inhalt besteht Mindestalter (P) Social Media

Von der Übergangslösung zum EUDI-Wallet

Warum bisherige Verfahren nicht tragen:

- Hohe Abbruchquoten bis hin zu offenem Nutzerprotest.
- Aufwand und Kosten je Prüfungsvorgang für Anbieter und Nutzer.
- Offenlegung von über die Altersschwelle hinausgehenden Daten.
- Keine unionsweite, interoperable Lösung (→ Souveränität).



Technologieneutralität: Art. 28 DSA schreibt weder immer Altersüberprüfung noch eine bestimmte Technologie vor
ABER: die Anforderungen der Leitlinien sind durchgängig an den Funktionalitäten des EUDI-Wallets ausgerichtet.

Das EUDI-Wallet als Mittel zur Altersüberprüfung

Anforderung der Leitlinien zur Altersüberprüfung nach Art. 28 DSA



Anonyme Alterstoken und selektive Offenlegung

Keine Offenlegung zusätzlicher
personenbezogener Daten; lediglich
funktionales Ergebnis („über/unter 18“)



Robustheit

Methode zur Altersfeststellung muss
robust und nicht leicht zu umgehen sein.



Wahlfreiheit und Akzeptanzpflichten

Es muss stets mehr als eine Methode zur
Altersfeststellung angeboten werden.



Datentrennung und -minimierung

Eigenständiger, von sonstigen
Datenerhebungen getrennter Vorgang;
keine Speicherung über Altersgruppe hinaus.

Entsprechung im EUDI-Wallet (eIDAS-VO)

Selektive Offenlegung als tragender Grundsatz des Wallets
sowie datenschutzfreundliche kryptographische Verfahren
(bspw. *Zero-Knowledge-Proofs*)

Art. 5a Abs. 4 lit. a eIDAS-VO, Erwgr. 14, 59 ÄndVO (EU) 2024/1183

Sicherheitsniveau „hoch“ des notifizierten Identifizierungssystems,
Aufbau auf **Vertrauensankern** und Zertifikatsketten sowie
Anknüpfung an die **staatlich abgesicherte Identität**.

Art. 5a Abs. 11 eIDAS-VO

Freiwilligkeit der Wallet-Nutzung, keine Nachteile bei Nichtnutzung, Zugang
auch über andere Identifizierungsmittel.

Akzeptanzpflichten (auf Verlangen des Nutzers) für sehr große Online-
Plattformen

Art. 5a Abs. 15, Art. 5f Abs. 3 eIDAS-VO

Verknüpfungsverbot für Wallet-Anbieter sowie

Bindung vertrauende Beteiligte an bei Registrierung angegebene
Datenkategorien.

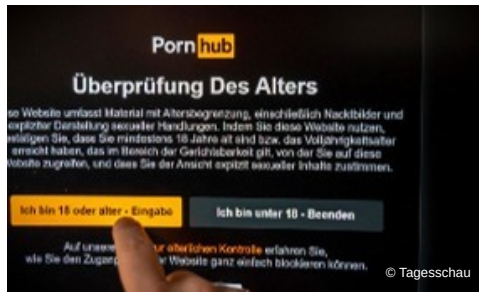
Art. 5a Abs. 14, Art. 5b Abs. 2 lit. c, Abs. 3 eIDAS-VO

Jugendschutz bald mit bissfesten Zähnen?

Rechtssichere, datenschutzkonforme und europäisch-souveräne Lösung zur Altersüberprüfung



„Pflicht“ zur Altersüberprüfung Klarstellende Leitlinien



Steigender Druck Gedanke „Europäische Souveränität“

← Post



Ursula von der Leyen
@vonderleyen

We need age-appropriate restrictions on platforms.

This is not about whether children can access social media.

It is about when social media can access our children.

© X



Teils verpflichtende Akzeptanz VLOPs

ChatGPT, Reddit, Roblox to adhere to EU's "very large platform" rules

By Reuters

August 31, 2026 12:02 PM GMT+2 · Updated 8 hours ago

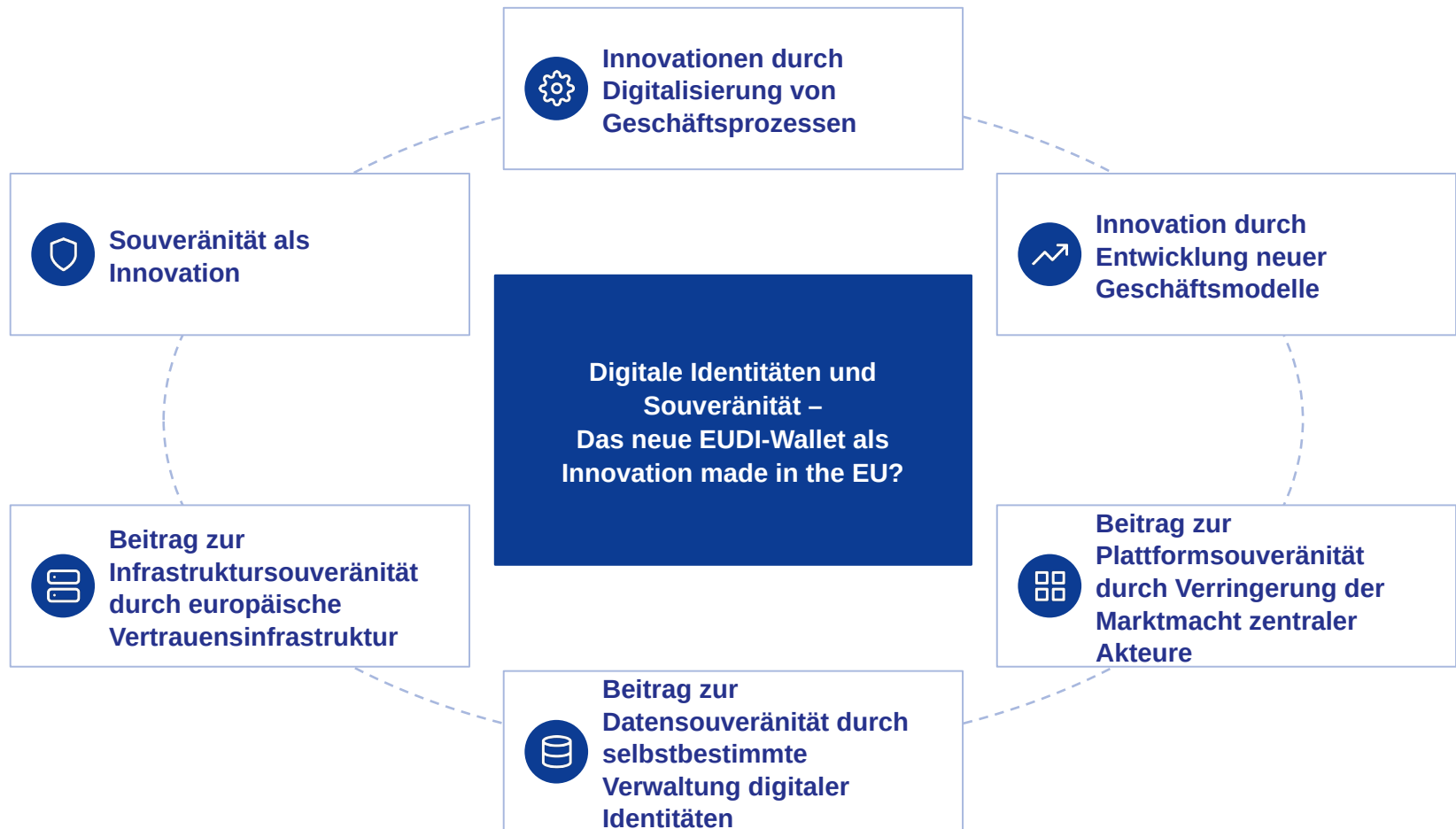


Fazit: Das EUDI-Wallet kann - je nach Umsetzung - einen Beitrag dazu leisten, die Lücke zwischen regulatorischem Anspruch und praktischer Umsetzbarkeit des Online-Jugendschutzes zu schließen.

Handlungsempfehlung: Anbieter sollten sich bereits jetzt auf die - teils verpflichtende - Akzeptanz des EUDI-Wallets sowie auf die damit verbundene Registrierung als vertrauende Beteiligte im Identitätsökosystem vorbereiten.

IV. Fazit

Fazit: Guter Baustein, aber die Umsetzung ist entscheidend



Herzlichen Dank für die Aufmerksamkeit!



Simon Tannen, LL.M. (CGSL)

Rechtsanwalt

Direct +49 40 36803-470

Mobile +49 1756355035

E-Mail s.tannen@taylorwessing.com

Taylor Wessing Partnerschaftsgesellschaft mbB

Am Sandtorkai 41

20457 Hamburg

Tel +49 40 36803-0

Fax +49 40 36803-280

www.taylorwessing.com



Johannes Noller

Rechtsanwalt | Associate

T +49 89 23807 182

M +49 175 9442447

F +49 89 23807 40682

E johannes.noller@cms-hs.com



Weitere Informationen

Noller/Tannen: Digitale Identitäten und
EUDI-Wallet,
in: Tann/Ruttloff/Wagner/Scherenberg,
Rechtshandbuch Web3

