



Ausschussdrucksache 21(23)104
vom 4. Oktober 2026

Schriftliche Stellungnahme

des Sachverständigen Prof. Dr.-Ing. habil. Jürgen Anke
Hochschule für Technik und Wirtschaft Dresden

Öffentliche Anhörung am 6. Oktober 2026

zu dem Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Durchführung der unionsrechtlichen Vorschriften über
die Europäische Briefftasche für die Digitale Identität sowie zur Änderung anderer
Rechtsvorschriften

BT-Drs. 21/7408

Stellungnahme zum Entwurf des Digitale Identitätengesetz (DIdG)

03.10.2026

Prof. Dr.-Ing. habil. Jürgen Anke
Professor für Softwaretechnologie und Informationssysteme
Hochschule für Technik und Wirtschaft (HTW) Dresden

Zur Person: Jürgen Anke ist Wirtschaftsinformatiker mit langjähriger Erfahrung in Forschungs- und Entwicklungsprojekten zum praktischen Einsatz digitaler Identitäten, verifizierbarer Nachweise und Wallet-Infrastrukturen. Er war wissenschaftlicher Leiter des BMWi-Schaufensterprojekts „ID-Ideal“. Weiterhin ist er Mitherausgeber des Buches „Digitale Identitäten und Nachweise“ (Springer, 2025) sowie Organisator der Konferenzreihe „authenticon – Vertrauen in der digitalen Gesellschaft“. Seine Arbeit befasst sich insbesondere mit der Gestaltung und Erprobung organisationsübergreifender Identitäts-ökosysteme, deren technischer und organisatorischer Interoperabilität sowie der Integration digitaler Nachweise in reale Verwaltungs- und Geschäftsprozesse.

1 Perspektive der Stellungnahme und zentrale Thesen

Die Einführung der Europäischen Brieftasche für die Digitale Identität (EUDI-Wallet) bietet die Chance, Bürgerinnen und Bürger zu befähigen, sich im digitalen Raum sicher und selbstbestimmt auszuweisen, vertrauenswürdige digitale Nachweise zu verwenden und damit digitale Prozesse ohne Medienbrüche durchzuführen.

Die vorliegende Stellungnahme erfolgt aus der Perspektive der Wirtschaftsinformatik. Sie betrachtet die EUDI-Wallet als Bestandteil eines soziotechnischen Systems, in dem digitale Technologie, Menschen, Organisationen und institutionelle Rahmenbedingungen zusammenwirken. Im Kern steht die Frage, unter welchen technisch-organisatorischen Bedingungen der Gesetzentwurf die Entstehung eines funktionsfähigen und skalierbaren digitalen Identitätsökosystems unterstützt. Eine technisch funktionsfähige Wallet allein reicht dafür nicht aus. Ihr praktischer Nutzen hängt davon ab,

- ob relevante Nachweise verfügbar sind,
- ob öffentliche und private Stellen diese ausstellen und akzeptieren,
- ob die beteiligten Systeme interoperabel zusammenarbeiten und
- ob die Prozesse für Bürgerinnen und Bürger verständlich und einfach nutzbar sind.

Solche digitalen Nachweise entfalten ihren besonderen Nutzen organisations- und sektorübergreifend. Ein privatwirtschaftlicher Prozess kann beispielsweise Nachweise aus Verwaltung, Finanzwesen oder anderen Vertrauensdomänen benötigen. Erst technische, semantische und organisatorische Interoperabilität ermöglicht es, solche Nachweise wiederzuverwenden und Medienbrüche zu vermeiden (vgl. Anke, Richter & Seiffert 2025; Granc, Peters & Fiedler 2025).

Um die Voraussetzungen für die Verbreitung digitaler Identitäten und Nachweise zu analysieren, lassen sich Identitätsökosysteme als mehrseitige Märkte betrachten. Diese sind von Netzwerkeffekten geprägt: Je mehr relevante Dienste und Nachweise verfügbar sind, desto attraktiver wird die Wallet für Nutzende; mit zunehmender Verbreitung steigt wiederum der Anreiz für weitere Organisationen, die Wallet zu unterstützen (vgl. Kubach 2025).

Vor diesem Hintergrund wird der Gesetzentwurf entlang der folgenden fünf Thesen beurteilt:

1. Der praktische Nutzen der EUDI-Wallet hängt wesentlich von einem breiten und interoperablen Angebot an elektronischen Nachweisen ab.
2. Interoperabilität muss Ende-zu-Ende betrachtet werden. Technische Konnektivität zwischen Wallet, BundID, NOOTS und Fachverfahren ist notwendig, reicht jedoch ohne syntaktische, semantische und organisatorische Interoperabilität nicht aus.
3. Registrierung und Lifecycle-Management von Relying Parties müssen auf breite Skalierung sowie auf Transparenz und Vertrauensbildung für Nutzende ausgelegt sein.
4. Digitale Vertretung erfordert interoperable Modelle für Erteilung, Nachweis, Änderung, Widerruf und Prüfung von Vertretungs- und Handlungsbefugnissen.
5. Ein Multi-Wallet-Ökosystem benötigt Wechselfähigkeit, Betriebskontinuität und verlässliche Rahmenbedingungen. Technische und regulatorische Flexibilität sollte deshalb mit einer transparenten Roadmap für die Umsetzung sowie angemessenen Planungshorizonten für die beteiligten öffentlichen und privaten Akteure einhergehen.

Auf diese Thesen wird nachfolgend mit Bezug auf den Entwurf des DIdG eingegangen.

2 Der Nutzen der Wallet entsteht durch Nachweise

Durch die Personenidentifizierungsdaten (PID) kann die EUDI-Wallet als elektronisches Identifizierungsmittel eingesetzt werden. § 15 Abs. 1 und 2 EBDIG-E erweitert die Akzeptanz der EUDI-Wallet auf rein nationale Sachverhalte und ermöglicht ihren Einsatz grundsätzlich auch dort, wo deutsches Recht einen elektronischen Identitätsnachweis nach Personalausweisgesetz, eID-Karte-Gesetz oder Aufenthaltsgesetz vorsieht. Bei einer ausschließlich Nutzung zur Identifikation bleibt der zusätzliche Nutzen gegenüber der bisherigen Online-Ausweisfunktion jedoch begrenzt. Der Gesetzentwurf selbst hebt als Mehrwert insbesondere die funktionale Kombination von digitaler Identität, Nachweisen sowie Signatur- und Siegelfunktionen hervor (vgl. § 15 Abs. 1 und 2 EBDIG-E; BT-Drs. 21/7408, S. 2).

Das besondere Nutzenpotenzial der EUDI-Wallet entsteht durch die Möglichkeit, Identität mit elektronischen Attributsbescheinigungen (EAA, QEAA, Pub-EAA) gemeinsam zu verwalten und in unterschiedlichen Kontexten wiederzuverwenden (vgl. Art. 5a Abs. 4 Buchst. a eIDAS-VO). Für zahlreiche Alltagsprozesse werden über die Identität einer Person hinaus noch Informationen zu Eigenschaften, Qualifikationen oder Berechtigungen benötigt. Dazu gehören Fahrerlaubnisse, Bildungs- und Berufsqualifikationen, Beschäftigungsnachweise, Mitgliedschaften oder andere fachliche Berechtigungen.

Für die praktische Wirkung der EUDI-Wallet ist § 16 EBDIG-E besonders relevant. Er verpflichtet Behörden des Bundes, nach Ablauf von 24 Monaten nach Verkündung nach Bundesrecht ausgestellte Dokumente auf Verlangen zusätzlich als elektronische Attributsbescheinigungen bereitzustellen. Damit adressiert der Gesetzentwurf einen zentralen Erfolgsfaktor. Die Reichweite bleibt jedoch begrenzt, da zahlreiche im Alltag relevante Nachweise von Ländern, Kommunen, Kammern, Bildungseinrichtungen oder privaten Organisationen ausgestellt werden.

Die Verwaltung spielt für den Aufbau des EUDI-Ökosystems eine zentrale Rolle. Staatlich ausgestellte Nachweise werden nicht nur in Verwaltungsverfahren, sondern auch in privatwirtschaftlichen Prozessen benötigt, z.B. bei der Autovermietung. Die Befähigung öffentlicher Stellen zur standardisierten Ausstellung elektronischer Nachweise kann deshalb über die Verwaltungsdigitalisierung hinaus privatwirtschaftliche und sektorübergreifende Anwendungsfälle mit hoher Alltagsrelevanz ermöglichen.

Der Aufbau des EUDI-Ökosystems sollte zudem unter dem Gesichtspunkt positiver Netzwerkeffekte betrachtet werden. Relevant ist nicht nur, wie viele Wallets installiert oder aktiviert werden, sondern auch, welche praktisch relevanten Nachweise verfügbar sind und in wie vielen Diensten sie tatsächlich eingesetzt werden können.

Empfehlung: Die Evaluation nach § 24 EBDIG-E sollte über ihren derzeitigen, auf die Wirksamkeit der in §§ 9 und 10 getroffenen Festlegungen zu mehreren authentischen Quellen fokussierten Gegenstand hinaus, um die Entwicklung des Nachweisökosystems ergänzt werden. Geeignete Indikatoren wären insbesondere die Zahl produktiver Nachweistypen, registrierter Herausgeber und Relying Parties, tatsächliche Nutzung sowie der Anteil medienbruchfrei verarbeiteter Nachweise. Ergänzend erscheint eine öffentliche Roadmap für prioritäre Nachweise und zentrale Infrastrukturkomponenten sinnvoll.

3 Interoperabilität muss Ende-zu-Ende betrachtet werden

§ 12 EBDIG-E sieht die Interoperabilität der EUDI-Wallet mit Nutzerkonten nach dem Onlinezugangsgesetz und mit dem Nationalen Once-Only-Technical-System (NOOTS) vor. Als mögliche Ziele nennt die Vorschrift unter anderem den Login mittels EUDI-Wallet, die vereinfachte Erstellung eines Nutzerkontos sowie die Übertragung von Nachweisen und Daten. Diese Verknüpfung ist sinnvoll, weil bestehende Infrastrukturen genutzt werden können und die Wallet nicht als isoliertes System eingeführt werden muss.

Insbesondere die vom IT-Planungsrat ausdrücklich vorgesehene mittelbare Anbindung über die BundID kann kurzfristig die Identifizierung und Authentifizierung mittels EUDI-Wallet für bereits an die BundID angebundene Verwaltungsleistungen ermöglichen; daneben soll auch die direkte Anbindung vorangetrieben werden (IT-Planungsrat 2026a, Ziff. 3). Dadurch allein entsteht jedoch noch kein verbesserter digitaler Prozess. Wenn das jeweilige Antrags- oder Fachverfahren elektronische Nachweise weder ausstellen noch entgegennehmen und automatisiert verarbeiten kann, bleibt der zusätzliche Nutzen begrenzt.

Für die weitere Umsetzung sollte deshalb ein mehrstufiger Interoperabilitätsbegriff zugrunde gelegt werden. Granc, Peters und Fiedler (2025) unterscheiden vier Ebenen:

1. strukturelle Interoperabilität: Systeme können über definierte Anschlüsse und Protokolle Daten austauschen;
2. syntaktische Interoperabilität: die übertragenen Daten folgen gemeinsamen Formaten;
3. semantische Interoperabilität: die beteiligten Systeme interpretieren die Daten fachlich gleich;
4. organisatorische Interoperabilität: Prozesse, Zuständigkeiten und Governance ermöglichen ein organisationsübergreifendes Zusammenwirken.

Diese Unterscheidung ist für die EUDI-Wallet unmittelbar relevant. Eine technische Schnittstelle oder ein Connector deckt nur einen Teil der erforderlichen Interoperabilität ab. Das Ziel muss sein, dass ein Nachweis vom ausstellenden Fachverfahren über die Wallet bis zum Fachverfahren der empfangenden Stelle ohne unnötige manuelle Transformation verarbeitet werden kann. Hierfür müssen unter anderem gemeinsame Datenmodelle und Semantik, geeignete Mechanismen für Gültigkeit und Status, Fehlerbehandlung sowie die Zuordnung zum fachlichen Vorgang funktionieren.

Ein zentraler NOOTS-Anschluss kann den technischen Integrationsaufwand, insbesondere für föderal verteilte Register, reduzieren. Der Gesetzentwurf sieht hierfür die Interoperabilität mit NOOTS und den Aufbau eines zentralen Dienstes zum Abruf von Daten über NOOTS für die EUDI-Wallet vor (vgl. § 12 EBDIG-E; BT-Drs. 21/7408, S. 3). Er ersetzt jedoch nicht die notwendige semantische und organisatorische Abstimmung. Gleiches gilt für eine indirekte Anbindung über die BundID oder über zentrale Basisdienste. Diese können einen sinnvollen Übergang und eine erhebliche Vereinfachung darstellen, dürfen aber nicht mit vollständiger Ende-zu-Ende-Interoperabilität gleichgesetzt werden.

Empfehlung: Bei der Umsetzung des § 12 EBDIG-E, bei der Nutzung der Verordnungsermächtigung für technische Einzelheiten nach § 22 Abs. 2 Nr. 6 EBDIG-E sowie im Rahmen der Experimentiermöglichkeiten nach § 23 Abs. 2 Nr. 6 und 8 EBDIG-E sollte Ende-zu-Ende-Interoperabilität als Gestaltungsziel berücksichtigt werden. Bewertet werden sollte nicht nur, ob Systeme technisch miteinander kommunizieren, sondern ob fachlich relevante Nachweise vom Herausgeber bis zum empfangenden Fachverfahren korrekt und automatisiert verarbeitet werden können. Eine entsprechende Erweiterung der Erfolgsevaluation sollte geprüft werden.

4 Registrierung von Relying Parties muss skalierbar und vertrauensbildend sein

§ 10 EBDIG-E bestimmt die zentrale deutsche Registrierungsstelle für vertrauende Beteiligte (Relying Parties) und setzt damit die unionsrechtlich vorgegebene Registrierung nach Art. 5b eIDAS-VO und der Durchführungsverordnung (EU) 2025/848 national um. Die Registrierung schafft Transparenz darüber, welche Organisationen Daten aus EUDI-Wallets anfordern, und ist trägt damit zur Vertrauensbildung bei den Nutzenden bei.

Der Gesetzentwurf setzt in seiner modellhaften Erfüllungsaufwandsberechnung für die erstmalige Registrierung eines Unternehmens einen durchschnittlichen Zeitaufwand von rund 40 Arbeitsstunden an; für die Einführungsphase werden modellhaft rund 4.200 Unternehmen angesetzt. Diese Werte sind keine empirisch gemessenen Prozesszeiten, sondern Annahmen der Folgenabschätzung und können mit der tatsächlichen Marktentwicklung variieren (BT-Drs. 21/7408, S. 54 f.). Soll die EUDI-Wallet zu einer horizontalen Infrastruktur für zahlreiche öffentliche und private Dienste werden, muss das Verfahren auch bei deutlich höheren Teilnehmerzahlen effizient funktionieren.

Dies betrifft nicht nur die technische Kapazität der Registrierungsstelle, sondern auch den gesamten Transaktionsaufwand des Onboarding- und Lifecycle-Prozesses. Neben der Erstregistrierung sind Änderungen an Anwendungsfällen und Datenanforderungen, Zertifikatswechsel, organisatorische Änderungen sowie gegebenenfalls Suspendierung und Aufhebung von Registrierungen zu berücksichtigen. Auch Intermediäre sind zu berücksichtigen. Sie handeln im Namen von Relying Parties und gelten nach Art. 5b Abs. 10 eIDAS-VO selbst als Relying Parties. Bei der Registrierung soll die Vertretungsbefugnis eines handelnden Vertreters nach Möglichkeit automatisiert geprüft werden (Art. 6 Abs. 3 Buchst. b DVO (EU) 2025/848). Weitere Betrachtungen zu Vertretungsbefugnissen finden sich unter Punkt 5.

Bestehende Register und authentische Quellen sollten deshalb so weit wie möglich genutzt werden, um Unternehmensdaten automatisiert zu übernehmen und wiederholte manuelle Prüfungen zu vermeiden. Die ab 24. Dezember 2026 anwendbare DVO (EU) 2025/848 verlangt hierfür benutzerfreundliche elektronische und, soweit möglich, automatisierte Registrierungsprozesse. Die Registrierungsregeln sollen zudem festlegen, auf welche authentischen Quellen oder sonstigen amtlichen elektronischen Register zurückgegriffen werden kann.

Die Registrierung erfüllt zugleich eine wichtige Vertrauensfunktion gegenüber den Nutzenden. Relying Parties müssen den beabsichtigten Verwendungszweck und die dafür angeforderten Daten im Registrierungsprozess angeben und dürfen keine anderen Daten als die für diesen Zweck registrierten anfordern (Art. 5b Abs. 2 und 3 eIDAS-VO). Nach der aktuellen Fassung der DVO (EU) 2025/848 müssen Registrierungszertifikate den Verwendungszweck abbilden; Wallet-Anbieter müssen Nutzende informieren, wenn eine Relying Party Daten anfordert, die nicht im Registrierungszertifikat angegeben sind (Art. 8 Abs. 2 Buchst. b bis d DVO (EU) 2025/848).

Die praktische Wirksamkeit dieses Mechanismus hängt jedoch von seiner Umsetzung ab. Eine formell korrekte Registrierung genügt nicht, wenn Nutzende nicht nachvollziehen können, welche Daten zu welchem Zweck angefragt werden. Sicherheit, Datenschutz und User Experience müssen deshalb gemeinsam betrachtet werden; insbesondere müssen Nutzende bei informierten Entscheidungen über die Weitergabe ihrer Daten unterstützt werden (vgl. Sauer et al. 2025, S. 393–409).

Auch eine Anfrage von unnötigen Daten („Überidentifizierung“) sollte vermieden werden. Der europäische Rechtsrahmen unterstützt hierzu selektive Offenlegung und Pseudonyme: Die Wallet muss selektive Offenlegung von Attributen unterstützen und Pseudonyme erzeugen können; Relying Parties dürfen Pseudonyme nicht zurückweisen, wenn die Identifizierung des Nutzers unions- oder nationalrechtlich nicht erforderlich ist (Art. 5a Abs. 4 Buchst. a und b sowie Art. 5b Abs. 9 eIDAS-VO; Art. 14 DVO (EU) 2024/2979). Die Herausforderung besteht damit wesentlich in der konkreten Gestaltung der Anwendungsfälle.

Empfehlung: Für die Evaluation sollten Indikatoren für die Skalierung und das Vertrauen entwickelt werden, z.B. Registrierungsdauer, Aufwand für Antragsteller, Anteil automatisierter Prüfungen, Änderungsaufwand sowie die Zahl und Bearbeitung von Beanstandungen wegen übermäßiger oder nicht registrierter Datenanforderungen.

5 Digitale Vertretung erfordert Delegations- und Berechtigungsmodelle

Vertretungs- und Handlungsbefugnisse sind für natürliche wie juristische Personen von großer praktischer Bedeutung. Die Bandbreite reicht von einfachen Vollmachten bis zu komplexen Unternehmensvertretungen oder gemeinschaftlich auszuübenden Berechtigungen.

§ 15 Abs. 3 EBDIG-E adressiert diesen Sachverhalt. Die Vorschrift ordnet die Verwaltung von Vertretungsbefugnissen grundsätzlich den natürlichen und juristischen Personen selbst zu und regelt, wie Nachweise von Vertretungs- und Handlungsbefugnissen aus authentischen Quellen mit Personenidentifizierungsdaten über elektronische Attributsbescheinigungen verknüpft werden können. Auch Anhang VI Nr. 9 eIDAS-VO nennt Befugnisse und Mandate zur Vertretung natürlicher oder juristischer Personen als relevante Attribute (vgl. § 15 Abs. 3 EBDIG-E). Für die technische Gestaltung ist folgende Unterscheidung erforderlich:

- Identität: Wer ist die handelnde Person A?
- Vertretungsbezug: Für welche Person oder Organisation B handelt A?
- Berechtigungsnachweis: Aufgrund welcher Befugnis darf A für B handeln, wer durfte diese Befugnis erteilen bzw. bescheinigen, und ist sie noch gültig?
- Autorisierungsentscheidung: Reicht die nachgewiesene Befugnis für den konkreten Vorgang aus?

Die elektronische Attributsbescheinigung ist dabei nicht mit der Vertretungsmacht selbst gleichzusetzen. Sie kann vielmehr als maschinenprüfbarer Nachweis einer nach dem jeweils einschlägigen Recht bestehenden Befugnis dienen. Die Gesetzesbegründung stellt klar, dass § 15 Abs. 3 EBDIG-E weder die wirksame Entstehung noch den Bestand, Beschränkungen oder Rechtsscheinwirkungen von Vertretungsbefugnissen regelt; diese richten sich nach dem materiellen Recht (BT-Drs. 21/7408, Begründung zu § 15 Abs. 3, S. 75 f.).

Die Forschung zu digitalen Organisationsidentitäten stellt heraus, dass neben der Identität einer Organisation beziehungsweise Person insbesondere geklärt werden muss, ob eine konkrete Person tatsächlich berechtigt ist, im Namen einer Organisation zu handeln. Organisations-Wallets wie die geplante „EU-Business Wallet“ erfordern deshalb Rollen- und Berechtigungskonzepte. Für komplexe organisatorische Konstellationen werden auch Mehrparteien- beziehungsweise Multi-Signature-Mechanismen diskutiert (vgl. Bochnia 2025; Schaarschmidt 2025).

Praktisch lassen sich mindestens drei Situationen unterscheiden.

- Vorab eingeräumte Vertretung: Person A verfügt bereits über einen geeigneten elektronischen Nachweis, dass sie für B in einem bestimmten Umfang handeln darf.
- Ad-hoc erteilte Vertretung: Eine Berechtigung liegt zu Beginn eines Vorgangs noch nicht vor. Eine hierzu autorisierte Person oder Stelle C wird in den laufenden Vorgang einbezogen und erteilt eine konkrete, gegebenenfalls kurzfristige oder transaktionsgebundene Freigabe.
- Komplexe oder gemeinschaftliche Vertretung: Die Befugnis hängt von mehreren Voraussetzungen oder mehreren Berechtigten ab. Auch die Frage, wer eine Vertretung erteilen darf, kann selbst eine weitere Berechtigungs- und Vertrauenskette erfordern.

Für die digitale Vertretung sind daher Mechanismen für Geltungsbereich, zeitliche Befristung, Änderung, Widerruf, Delegation und gegebenenfalls gemeinschaftliche Entscheidungen erforderlich. Die Wallet muss dabei nur geeignete Vertretungs-Nachweise sicher verwalten und präsentieren. Die fachliche Entscheidung, ob die nachgewiesene Befugnis für einen konkreten Vorgang ausreicht, verbleibt beim jeweiligen Dienst oder Fachverfahren. Die Gesetzesbegründung lässt hierfür unterschiedliche technische Ansätze bis hin zu strukturierten Daten und organisationsweiten Funktionen zur Verwaltung von Vertretungsbefugnissen offen (BT-Drs. 21/7408, Begründung zu § 15 Abs. 3, S. 75 f.).

Empfehlung: Bei der weiteren technischen Ausgestaltung sollten interoperable Modelle für Erteilung, Delegation, Statusprüfung, Widerruf sowie gegebenenfalls transaktionsbezogene Freigaben berücksichtigt werden. Dabei sollte bewusst offengehalten werden, ob ein konkreter Fall über eine längerfristig nutzbare elektronische Attributsbescheinigung, einen kurzlebigen oder transaktionsgebundenen Berechtigungsnachweis oder einen anderen geeigneten Mechanismus umgesetzt wird.

6 Multi-Wallet-Ökosysteme benötigen Wechselbarkeit und planbare Rahmenbedingungen

Die §§ 3 bis 6 EBDIG-E ermöglichen die drei unionsrechtlich vorgesehenen Bereitstellungsmodelle: unmittelbar staatlich, im staatlichen Auftrag sowie unabhängig angeboten und staatlich anerkannt; § 7 EBDIG-E ergänzt Informationspflichten zur Verfügbarkeit der Wallets. Damit kann ein Multi-Wallet-Ökosystem entstehen. Dieses kann Wettbewerb und Innovation fördern, stellt aber zusätzliche Anforderungen an Interoperabilität, Anbieterwechsel und Betriebskontinuität (vgl. §§ 3–7 EBDIG-E; Art. 5a Abs. 2 eIDAS-VO).

Daneben ist die Planungssicherheit für öffentliche und private Akteure zu berücksichtigen. § 22 EBDIG-E eröffnet bewusst Spielraum für spätere Rechtsverordnungen, insbesondere für zusätzliche Anforderungen an die Anerkennung unabhängiger Wallet-Anbieter (§ 22 Abs. 2 Nr. 3 EBDIG-E) sowie für technische Einzelheiten (§ 22 Abs. 2 Nr. 6 EBDIG-E). Diese Flexibilität ist angesichts der technischen Entwicklungen grundsätzlich sinnvoll.

In einem Multi-Wallet-Ökosystem ist zwischen Datenportabilität und funktionaler Wechselbarkeit zu unterscheiden. Das Unionsrecht enthält bereits eine Portabilitätsvorgabe für den Anbieterwechsel: Wallet-Einheiten müssen, soweit technisch machbar und mit Ausnahme kritischer Assets, den sicheren Export und die Portabilität personenbezogener Daten ermöglichen, um einen Wechsel zu einer anderen Wallet-Lösung unter Wahrung des Vertrauensniveaus „hoch“ zu unterstützen (Art. 13 DVO (EU) 2024/2979). Für die Betriebskontinuität bleibt praktisch zu klären, wie Nutzende bei einem Anbieterwechsel oder der Einstellung eines Angebots ihre digitale Handlungsfähigkeit zuverlässig wiederherstellen können, insbesondere wenn einzelne Nachweise oder kryptographische Schlüssel nicht unmittelbar übertragbar sind. Je nach Nachweistyp kann hierfür eine erneute Ausstellung erforderlich sein.

Neben der Frage der Bereitstellung von Wallets für die Bürger ist auch die technische Befähigung öffentlicher Stellen zur Teilnahme am EUDI-Ökosystem hochgradig relevant. Der IT-Planungsrat hat mit Beschluss B-2026/19-IT den Bund gebeten, einen zentralen Issuer- und Verifier-Dienst zur Nachnutzung durch Länder und Kommunen bereitzustellen. Zugleich soll der Bund möglichst bis Ende 2026 einen Vorschlag für eine Verwaltungsvereinbarung einschließlich der Finanzierung vorlegen (IT-Planungsrat 2026a, Ziff. 1). Solche zentralen Komponenten können den Integrationsaufwand erheblich reduzieren.

Daraus entsteht für Länder, Kommunen und Unternehmen ein Planungsbedarf. Kommunen und Länder arbeiten mit Haushalts-, Vergabe- und Entwicklungszyklen; Unternehmen treffen Investitions- und Produktentscheidungen häufig lange vor der Markteinführung. Sie müssen daher frühzeitig wissen, welche zentralen Dienste bereitstehen, welche zusätzlichen nationalen Anerkennungsbedingungen gelten und welche technischen Anforderungen als stabil gelten. Dies gilt insbesondere für zentrale Komponenten wie Issuer- und Verifier-Dienste sowie für weitere Funktionen, die durch Rechtsverordnungen konkretisiert werden sollen. Für die technische Ausstattung öffentlicher Stellen müssen

Leistungsumfang, Betriebsmodell, Zugangsbedingungen, Finanzierung und Verfügbarkeit zentraler Dienste frühzeitig bekanntgegeben werden.

Empfehlung: Die Flexibilität des § 22 EBDIG-E sollte durch eine transparente Roadmap begleitet werden. Diese sollte unter anderem ausstehende Entscheidungen und deren Zeitpunkte, zentrale Dienste und deren Leistungsumfänge, stabile technische Rahmenbedingungen sowie Übergangs- und Migrationsfristen enthalten. Der IT-Planungsrat fordert für den D-Stack bereits eine verbindliche Meilensteinplanung, damit Länder Integration und Investitionen zuverlässig planen können (IT-Planungsrat 2026b, Ziff. 1 und 6). Fachexpertise aus Wirtschaft, Verwaltung, Wissenschaft und Zivilgesellschaft sollte bei wesentlichen Entscheidungen frühzeitig eingebunden werden.

7 Schlussfolgerung

Der DIdG-Entwurf schafft zentrale nationale Voraussetzungen für die Einführung der EUDI-Wallet. Der langfristige Erfolg sollte daran gemessen werden, ob ein funktionierendes Ökosystem entsteht, in dem öffentliche und private Stellen relevante Nachweise ausstellen und akzeptieren, Nutzende einen erkennbaren Alltagsnutzen erfahren und digitale Nachweise organisationsübergreifend ohne Medienbrüche automatisiert verarbeitet werden können. Die Herausforderung der kommenden Jahre liegt damit in der koordinierten Entwicklung des gesamten EUDI-Ökosystems, in dem die Ziele von Bürgerinnen und Bürgern, der öffentlichen Verwaltung und der Privatwirtschaft gleichermaßen berücksichtigt werden.

Quellen

Anke, J.; Richter, D.; Seiffert, M. (2025): *Grundlagen, Entwicklungslinien und Perspektiven Digitaler Identitäten und Nachweise*. In: Anke, J.; Kubach, M.; Sürmeli, J. (Hrsg.): *Digitale Identitäten und Nachweise*. Springer Vieweg, Wiesbaden.

Bochnia, R. (2025): *Von Identifikatoren zu Wallets: Die Zukunft digitaler Organisationsidentitäten*. In: Anke, J.; Kubach, M.; Sürmeli, J. (Hrsg.): *Digitale Identitäten und Nachweise*. Springer Vieweg, Wiesbaden.

Granc, F.; Peters, R.; Fiedler, A. (2025): *Entwicklung neuer Standards für Interoperabilität im europäischen Identitätsökosystem: Beiträge aus dem Schaufensterprogramm Sichere digitale Identitäten*. In: Anke, J.; Kubach, M.; Sürmeli, J. (Hrsg.): *Digitale Identitäten und Nachweise*. Springer Vieweg, Wiesbaden.

Kubach, M. (2025): *Ökonomisch tragfähige Identitätsökosysteme: Wertschöpfung und Marktstrategien*. In: Anke, J.; Kubach, M.; Sürmeli, J. (Hrsg.): *Digitale Identitäten und Nachweise*. Springer Vieweg, Wiesbaden.

Sauer, M.; Lenski, N.; Ebert, S.; Krauß, A.-M.; Pfeifer, S. (2025): *Benutzbare Sicherheit und Benutzbarer Datenschutz von Wallets: Anforderungen und Bewertungsmethodik*. In: Anke, J.; Kubach, M.; Sürmeli, J. (Hrsg.): *Digitale Identitäten und Nachweise*. Springer Vieweg, Wiesbaden.

Schaarschmidt, K. (2025): *Digitale Unternehmensidentitäten: Herausforderungen, Lösungen und Handlungsempfehlungen*. In: Anke, J.; Kubach, M.; Sürmeli, J. (Hrsg.): *Digitale Identitäten und Nachweise*. Springer Vieweg, Wiesbaden.