

Stellungnahme

Juli 2026

Bitkom-Stellungnahme zum Regierungsentwurf eines Digitale Identitäten-Gesetzes

Zusammenfassung

Bitkom begrüßt den Regierungsentwurf als wichtigen Schritt zur nationalen Umsetzung der EUDI-Wallet und zur Schaffung eines rechtlichen Rahmens für digitale Identitäten in Deutschland. Damit die EUDI-Wallet ihr Potenzial in der Praxis entfalten kann, braucht es jedoch an mehreren Stellen weitere Konkretisierungen. Dies betrifft insbesondere die frühzeitige Bereitstellung elektronischer Attributsbescheinigungen, die verlässliche Abdeckung aller relevanten Akteure beim Bezug von Personenidentifizierungsdaten, die klare Bestimmung der hierfür maßgeblichen authentischen Quellen sowie die technologieoffene Ausgestaltung des PID-Onboardings. Zudem sollten zentrale Prozesse wie der zentrale Issuing Dienst, die Abbildung von Vertretungs- und Handlungsbefugnissen sowie die Rolle und Verantwortlichkeit des Brieftaschenanbieters klarer geregelt werden. Insgesamt sollte der Rechtsrahmen weiter präzisiert werden, um die breite Nutzbarkeit der Wallet für Bürgerinnen und Bürger, Unternehmen und Verwaltung sicherzustellen.

Übergangsfrist von 24 Monaten für die Ausstellung elektronischer Attributsbescheinigungen durch Bundesbehörden – Art. 1, § 16 Abs. 1 EBDIG

Problembeschreibung

Eine Übergangsfrist von 24 Monaten für die Ausstellung elektronischer Attributsbescheinigungen durch Bundesbehörden ist kritisch, weil zentrale Nachweise damit voraussichtlich erst deutlich nach dem Start der EUDI-Wallet verfügbar wären. Gerade in der Einführungsphase droht dadurch ein begrenzter praktischer Nutzen der Wallet. Ohne früh verfügbare elektronische Attributsbescheinigungen fehlen wichtige Anwendungsfälle, die für Akzeptanz und Nutzung der Wallet entscheidend sind.

Lösungsvorschlag

Die vorgesehene Übergangsfrist von 24 Monaten für die Ausstellung elektronischer Attributsbescheinigungen durch Bundesbehörden sollte überprüft werden. Um frühzeitig einen praktischen Mehrwert der EUDI-Wallet zu schaffen, sollten besonders relevante Attributsbescheinigungen identifiziert, priorisiert und gestuft bereitgestellt werden. Hierbei sollte die Mindestattributsliste aus Art. 45e Abs. 1 eIDAS-Verordnung i. V. m. Anhang VI der eIDAS-Verordnung berücksichtigt werden, da es sich insoweit um eine unionsrechtliche Vorgabe handelt, die innerhalb der in der eIDAS-Verordnung vorgesehenen Frist umzusetzen ist.

Zugleich sollte die Regelung nicht isoliert im EBDIG verortet bleiben, sondern im Rahmen einer abgestimmten Gesetzgebung von Bund und Ländern in die einschlägigen Verwaltungsverfahrensgesetze und Prozessordnungen integriert werden. Da Bundesgesetze häufig durch Länder und Kommunen ausgeführt werden und viele relevante Verwaltungsleistungen nicht von Bundesbehörden erbracht werden, ist eine stärkere Einbindung von Ländern und Kommunen erforderlich, um Fragmentierung zu vermeiden und einen breiten praktischen Anwendungsbereich sicherzustellen.

Beschränkung des Schriftformersatzes auf Behörden des Bundes – Art. 1, § 16 Abs. 2 EBDIG

Problembeschreibung

Der Regierungsentwurf erkennt elektronische Attributsbescheinigungen als Schriftformersatz nur gegenüber Behörden des Bundes an. Für Länder und Kommunen enthält der Entwurf keine entsprechende allgemeine Regelung. Da viele Verwaltungsverfahren auf Landes- oder kommunaler Ebene stattfinden, kann dies zu unterschiedlichen Regelungen je nach Bundesland führen und die einheitliche Nutzung der EUDI-Wallet

erschweren. Zudem stellt sich in der Zusammenschau aller Limitationen des § 16 Abs. 2 EBDIG die entscheidende Frage, welche Anwendungsfälle tatsächlich noch verbleiben. Ohne einen tatsächlichen praktischen Nutzen kann auf die Rechtsvorschrift auch verzichtet werden.

Lösungsvorschlag

Der Gesetzgeber sollte daher vor der Verabschiedung dieser Rechtsvorschrift evaluieren, welche Anwendungsfälle bei einer derart restriktiven Formulierung verbleiben. Da bei Antragsverfahren, welche ausnahmsweise die Schriftform vorsehen, typischerweise eine Unterschrift zu leisten ist, wird wohl regelmäßig zumindest eine qualifizierte elektronische Signatur für rein elektronische Verfahren vorausgesetzt sein. Es ist jedenfalls nicht ohne Weiteres erkennbar, welche praxisrelevanten Fälle verbleiben.

Wir raten weiterhin dazu, mit den Ländern die Gesetzgebung abzustimmen und diese zu motivieren, eigene entsprechende Regelungen zum Schriftformersatz für ihre Verwaltungen zu erlassen.

Darüber hinaus sollte geprüft werden, ob und in welchem Umfang elektronische Attributsbescheinigungen auch in gerichtlichen Verfahren nutzbar gemacht und in den einschlägigen Gerichtsordnungen, unter anderem der Zivilprozessordnung (ZPO) und der Verwaltungsgerichtsordnung (VwGO), berücksichtigt werden sollten. Soweit hierfür Anpassungen der bestehenden Rechtsgrundlagen erforderlich sind, sollten diese frühzeitig in die weitere Gesetzgebungsabstimmung einbezogen werden.

Regelung zu Personenidentifizierungsdaten und authentischen Quellen – Art. 1, § 9 EBDIG

Problembeschreibung

Die Regelung zu Personenidentifizierungsdaten wirft Fragen hinsichtlich Wortlaut und Systematik auf. Unklar bleibt insbesondere das Verhältnis zwischen Personenidentifizierungsdaten, authentischen Quellen und elektronischen Attributsbescheinigungen.

Zudem wird für wirtschaftlich tätige natürliche Personen, die nicht im Handelsregister geführt werden, keine eigenständige berufliche Identität mit geeigneter authentischer Quelle vorgesehen. Dies führt zu einer sachlich nicht gerechtfertigten Ungleichbehandlung gegenüber im Handelsregister eingetragenen wirtschaftlich tätigen natürlichen Personen und kann dazu führen, dass berufliche und private Nutzung der Wallet nicht ausreichend getrennt werden können.

Für die eintragungsfähigen, aber nicht eingetragenen GbRs sowie für die nicht von § 9 Abs. 2 EBDIG erfassten Unternehmen sollte ausdrücklich geregelt werden, ob und welche authentischen Quellen für Personenidentifizierungsdaten und die hierfür erforderlichen Berechtigungsprüfungen herangezogen werden können. Andernfalls kann nicht verlässlich geprüft werden, ob eine Person berechtigt ist, Personenidentifizierungsdaten für das jeweilige Unternehmen zu erhalten.

Lösungsvorschlag

§ 9 EBDIG sollte so angepasst werden, dass für alle nicht durch Justizregister abgedeckten Unternehmen im Sinne des § 3 Abs. 1 UBRegG, insbesondere für bislang nicht ausreichend erfasste wirtschaftlich tätige natürliche Personen, eindeutig geregelt wird, aus welchen authentischen Quellen Personenidentifizierungsdaten bezogen werden können.

Für GbR sollte klargestellt werden, unter welchen Voraussetzungen Personenidentifizierungsdaten bezogen werden können. Dabei ist zu berücksichtigen, dass eGbR im Gesellschaftsregister geführt werden und eintragungsfähige GbR die Möglichkeit der Eintragung haben, aber auch ohne Eintragung rechtsfähig sind. Zugleich sollten unklare Zugangsvoraussetzungen in der Praxis vermieden werden.

Zudem sollte sichergestellt werden, dass die Berechtigung zur Beantragung und Nutzung von Personenidentifizierungsdaten verlässlich geprüft werden kann. Hierfür sollte der Gesetzgeber klarstellen, aus welchen authentischen Quellen die jeweils erforderlichen Vertretungsinformationen und Berechtigungsnachweise bezogen werden können. Dies gilt vor allem für die Fälle des § 9 Abs. 3 EBDIG.

Anbindung weiterer Quell- und angebundener Register und Anpassungsbedarf des UBRegG – Art. 1, § 9 EBDIG und Art. 13

Problembeschreibung

Für eine praxistaugliche Nutzung des Unternehmensbasisdatenregisters bedarf es einer ausreichenden Datengrundlage. Hierfür sollten weitere geeignete Quell- und angebundene Register einbezogen werden, soweit die erforderlichen Daten nicht bereits über bestehende authentische Quellen abgedeckt sind oder eine technische Anbindung an diese Quellen erforderlich ist. Gleichzeitig zeigt sich Anpassungsbedarf im UBRegG, da zahlreiche Vorschriften bislang auf die bestehenden Register nach §§ 4 ff. UBRegG zugeschnitten sind und später über die UBRegV eingebundene Register nicht ausdrücklich berücksichtigen.

Lösungsvorschlag

Weitere geeignete Quell- und angebundene Register sollten über eine Anpassung der UBRegV an das Unternehmensbasisdatenregister angebunden beziehungsweise über dieses nutzbar gemacht werden, soweit dadurch bislang nicht abgedeckte Fälle erfasst werden. Zugleich sollte das UBRegG um geeignete Öffnungstatbestände ergänzt werden, damit neu angebundene Register und die dort erfassten Einheiten rechtssicher berücksichtigt werden können und keine rechtlichen Anschlusslücken entstehen.

Zur konkreten Umsetzung schlagen wir vor, § 3 Abs. 1 UBRegG um einen entsprechenden Öffnungstatbestand zu ergänzen:

»§ 3 Absatz 1 wird wie folgt geändert:

a) In Nummer 7 wird der Punkt am Ende durch ein Komma ersetzt.

b) Nach Nummer 7 wird folgende Nummer eingefügt:

8. weitere Einheiten, welche in einer nach § 10 Satz 1 Nummer 6 erlassenen Rechtsverordnung bestimmt werden.«

Zulässigkeit technologieoffener Remote-Identifizierungsverfahren beim PID-Onboarding – Art. 1, § 20 EBDIG, im Zusammenhang mit § 9 EBDIG

Problembeschreibung

Die Regelung zu Personenidentifizierungsdaten berücksichtigt bislang nicht ausreichend die zwischenzeitlich konkretisierten europäischen Vorgaben zum Wallet-Onboarding. Mit der Durchführungsverordnung (EU) 2026/798 wird klargestellt, dass das Vertrauensniveau »hoch« auch durch die Kombination von Identifizierungsmitteln mit dem Sicherheitsniveau »substanziell« und zusätzlichen Remote-Onboarding-Verfahren erreicht werden kann. Zudem werden dokumentenbasierte Verfahren (z. B. NFC-basierte Ausweisprüfung) als gleichwertige Use Cases zur eID-Authentifizierung anerkannt. Ohne diese Klarstellung besteht das Risiko einer faktischen Einschränkung auf einzelne Identifizierungsmittel und damit verbundene Nutzungshürden.

Lösungsvorschlag

Klarstellung im Gesetz oder in der Begründung, dass für das PID-Onboarding neben der Online-Ausweisfunktion auch eIDAS-konforme Remote-Identifizierungsverfahren nach Art. 24 zulässig sind. Dies umfasst insbesondere dokumentenzentrierter Verfahren sowie nicht notifizierte, zertifizierte Identifizierungsmittel, sofern sie den Vorgaben der Durchführungsverordnung (EU) 2026/798 entsprechen, das erforderliche Vertrauensniveau erreicht und die Integrität der Personenidentifizierungsdaten (PID) jederzeit gewährleistet wird.

Weitere Regelungen zum zentralen Issuing Dienst (zID) – Art. 1, § 12 EBDIG

Problembeschreibung

Nach § 12 EBDIG i. V. m. der Gesetzesbegründung soll ein zentraler Issuing-Dienst (zID) eingeführt werden, sodass öffentliche Stellen bei Anbindung an das NOOTS elektronische Attributsbescheinigungen ausstellen können.

Lösungsvorschlag

Mit Blick auf die Ausstrahlungswirkung gegenüber öffentlichen Stellen sollen Detailregelungen zum zID bereits getroffen werden:

- Wer ist die für den zID zuständige Stelle?
- Welche Art von elektronischer Attributsbescheinigung wird verwendet (PuB-EAA oder QEAA)?
- Welche Kosten entstehen für öffentliche Stellen, welche den zID nutzen?
- Treten die öffentlichen Stellen als Aussteller auf oder nur der Betreiber des zID?
- Wie wird die Ausstellung und der Widerruf der ausgestellten Attributsbescheinigungen sichergestellt?
- Wie stellt der zID die inhaltliche Richtigkeit der ausgestellten Attribute sicher? Sofern es die beauftragende Behörde ist: Wie stellt diese sicher, dass die Attributsbescheinigung nur in die richtige Wallet ausgestellt wird?

Vertretungs- und Handlungsbefugnisse – Art. 1, § 15 Abs. 3 EBDIG

Problembeschreibung

Die Regelung zu Vertretungs- und Handlungsbefugnissen lässt offen, ob auch qualifizierte elektronische Attributsbescheinigungen erfasst sind und wie rechtsgeschäftliche Vertretungsmacht berücksichtigt werden kann. Zudem bleibt unklar, welche Rolle gesetzlich geregelte Vollmachtsdatenbanken künftig im Wallet-Ökosystem einnehmen sollen und aus welchen authentischen Quellen gesetzliche und rechtsgeschäftliche Vertretungs- und Handlungsbefugnisse jeweils abgeleitet werden können.

Lösungsvorschlag

§ 15 Abs. 3 EBDIG sollte klarstellen, dass auch qualifizierte elektronische Attributsbescheinigungen erfasst sind und rechtsgeschäftliche Vertretungsmacht berücksichtigt werden kann. Zudem sollten gesetzlich geregelte Vollmachtsdatenbanken bei der Ausgestaltung berücksichtigt werden, soweit sie insbesondere für den Nachweis rechtsgeschäftlicher Vertretungsmacht als geeignete authentische Quellen in Betracht kommen. Für gesetzliche Vertretungsinformationen und sonstige Handlungsbefugnisse sollte der Gesetzgeber klar bestimmen, welche authentischen Quellen jeweils zuständig sind. Soweit die erforderlichen Informationen bereits in bestehenden authentischen Quellen verfügbar sind, sollten diese unmittelbar genutzt werden; unnötige Datenkopien sowie zusätzliche Pflege- und Validierungsaufwände sollten vermieden werden.

Verbindliche Überführung von Pilotverfahren in den Regelbetrieb – Art. 1, § 21 EBDIG

Problembeschreibung

Die Experimentierklausel ist ein zentrales Instrument zur Erprobung neuer Verfahren. Der Entwurf enthält jedoch keine klare Perspektive für die Überführung erfolgreicher Pilotverfahren in den Regelbetrieb, insbesondere im Bereich digitaler Identifizierungsverfahren.

Lösungsvorschlag

Ergänzung, dass erfolgreiche Pilotverfahren – insbesondere im Bereich eIDAS-konformer Remote-Onboarding-Verfahren – systematisch evaluiert und bei Erfolg in den Regelbetrieb überführt werden.

Klarstellung des Begriffes »Brieftaschenanbieters« – Art. 1, § 19 EBDIG

Problembeschreibung

Der Gesetzentwurf verwendet den Begriff des »Brieftaschenanbieters« an mehreren Stellen – insbesondere in § 19 (Datenverarbeitung) und § 20 Abs. 3 (Trennungsgebot) – ohne ihn im Gesetzentwurf selbst zu definieren. Der Begriff ist jedoch unionsrechtlich zumindest in den einschlägigen Durchführungsverordnungen definiert; so bestimmt etwa Art. 2 Nr. 9 der Durchführungsverordnung (EU) 2024/2977, dass »Brieftaschenanbieter« eine natürliche oder juristische Person ist, die Brieftaschenlösungen bereitstellt. Der Begriff wird im Gesetzentwurf vielmehr funktional abgeleitet und als Oberbegriff für private Anbieter oder öffentliche Stellen verwendet, die eine Europäische Brieftasche im Sinne des Art. 3 Nr. 42 der Verordnung (EU) Nr. 910/2014 gegenüber den Nutzern (gem. §§ 4, 5 oder 6) bereitstellen und hierfür die Gesamtverantwortung tragen.

Eine entsprechende Klarstellung und ein Verweis auf die unionsrechtliche Begriffsbestimmung sollte in der Begründung vorgenommen werden, um Unklarheiten für alle Beteiligten zu vermeiden, wie etwa in Bezug auf die Frage, wie weit das Trennungsgebot des § 20 Abs. 3 reicht.

Lösungsvorschlag

Nachfolgende Klarstellung im Begründungstext zu § 19 Abs. 1 vornehmen:

»Die Vorschrift legt fest, dass die Verarbeitung personenbezogener Daten zulässig ist, soweit dies zur Gewährleistung der Funktionalität und Integrität der Brieftasche sowie der damit verbundenen Dienste erforderlich ist. Hintergrund der Regelung ist, dass

nach Erwägungsgrund Nummer 9 der Verordnung (EU) 2024/1183 die Datenschutz-Grundverordnung und gegebenenfalls die Richtlinie 2002/58/EG für jede Verarbeitung personenbezogener Daten gemäß der Verordnung (EU) Nr. 910/2014 gelten. Die Verarbeitung personenbezogener Daten im Anwendungsbereich dieses Gesetzes unterliegt demnach der unmittelbar geltenden Datenschutz-Grundverordnung. Mithin bedarf jede Verarbeitung personenbezogener Daten gemäß Art. 6 Abs. 1 Unterabs. 1 der Datenschutz-Grundverordnung einer gültigen Rechtsgrundlage. Die gesetzliche Vorschrift schafft eine entsprechende Rechtsgrundlage für die Datenverarbeitung durch den Brieffaschenanbieter, der unionsrechtlich zumindest in Art. 2 Nr. 9 der Durchführungsverordnung (EU) 2024/2977 als natürliche oder juristische Person definiert ist oder der nach § 5 und § 6 eine Europäische Brieffasche im Sinne des Art. 3 Nr. 42 der Verordnung (EU) Nr. 910/2014 gegenüber den Nutzenden bereitstellt und hierfür die Gesamtverantwortung trägt. Klarstellend erfasst sind nach dem Wortlaut auch mit der Bereitstellung verbundene Dienste«.

Ermöglichung des Identitätsnachweises mittels Europäischer Brieffasche vor praktischer Implementierungsfähigkeit – Art. 1 § 15 Abs. 2 EBDIG

Problembeschreibung

Nach dieser Regelung gilt die Europäische Brieffasche bereits mit Inkrafttreten des Gesetzes (Verkündung) als Identifizierungsmittel (z. B. bei § 172 TKG). Dies ist jedoch praktisch nicht umsetzbar, da die erforderlichen technischen, organisatorischen und regulatorischen Voraussetzungen auf Unternehmensseite noch nicht vorliegen und die Brieffasche selbst erst schrittweise ab 2027 verfügbar und funktionsfähig sein wird. Ohne eine entsprechende Klarstellung entsteht daher ein Widerspruch zwischen der gesetzlichen Ausgestaltung und der tatsächlichen Umsetzbarkeit sowie erhebliche Rechtsunsicherheit für betroffene Unternehmen.

Lösungsvorschlag

Zur Vermeidung dieser Unsicherheiten sollte das Gesetz klarstellen, dass die Europäische Brieffasche für digitale Identität zwar entsprechend Anwendung als zulässiges Identifizierungsmittel findet, eine verpflichtende Nutzung bzw. Akzeptanz jedoch erst ab einem späteren, klar definierten Zeitpunkt greift. Naheliegend ist hierbei eine Anknüpfung an die Systematik des Art. 5f Abs. 2 der eIDAS-Verordnung. Ergänzend sollte zwischen der bloßen Zulässigkeit und der verpflichtenden Akzeptanz differenziert sowie sichergestellt werden, dass eine mögliche Verpflichtung erst greift, wenn die notwendigen technischen und infrastrukturellen Voraussetzungen tatsächlich vorhanden sind. Hierzu sollte § 15 Abs. 2 EBDIG um folgenden Satz ergänzt werden: »Unbeschadet der Regelung in Absatz 1 begründet Satz 1 keine Verpflichtung zur Akzeptanz der Europäischen Brieffasche für die Digitale Identität.«.

Reduktion von Zugangshürden durch digitale PIN-Rücksetzung

Problembeschreibung

Der Zugang zur eID ist eine zentrale Voraussetzung für das Wallet-Onboarding. Die bisherige Ausgestaltung über physische Briefprozesse weist jedoch deutliche Einschränkungen hinsichtlich Nutzung, Kosten und Skalierbarkeit auf und führt zu Medienbrüchen.

Lösungsvorschlag

Ergänzung in der Begründung, dass der PIN-Rücksetzdienst perspektivisch um digitale, eIDAS-konforme Identifizierungsverfahren nach Art. 24 ergänzt werden sollte, um vollständig digitale und nutzerfreundliche Prozesse zu ermöglichen.

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber

Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartnerin

Lorène Slous | Referentin Vertrauensdienste & Digitale Identitäten
T 030 27576-157 | l.slous@bitkom.org

Verantwortliches Bitkom-Gremium

AK Anwendung elektronischer Vertrauensdienste
AK Digitale Identitäten

Copyright

Bitkom 2026

Diese Publikation stellt eine allgemeine unverbindliche Information dar. Die Inhalte spiegeln die Auffassung im Bitkom zum Zeitpunkt der Veröffentlichung wider. Obwohl die Informationen mit größtmöglicher Sorgfalt erstellt wurden, besteht kein Anspruch auf sachliche Richtigkeit, Vollständigkeit und/oder Aktualität, insbesondere kann diese Publikation nicht den besonderen Umständen des Einzelfalles Rechnung tragen. Eine Verwendung liegt daher in der eigenen Verantwortung des Lesers. Jegliche Haftung wird ausgeschlossen. Alle Rechte, auch der auszugsweisen Vervielfältigung, liegen beim Bitkom oder den jeweiligen Rechteinhabern.