



Ausschussdrucksache 21(23)105
vom 4. Oktober 2026

Schriftliche Stellungnahme

der Sachverständigen Bianca Kastl
Innovationsverbund Öffentliche Gesundheit e.V.

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

Bianca Kastl, Innovationsverbund Öffentliche Gesundheit e. V. (InÖG)

04.10.2026

Kurzfassung.....	1
Vorbemerkung.....	2
Verbesserungsbedarfe der Gesetzgebung.....	2
Registrierung und Kontrolle von Diensteanbietern.....	2
Freiwilligkeit und diskriminierungsfreier Zugang.....	3
Gesetzlich verankertes Recht auf Opt-out aus biometrischen Lichtbildern in der Wallet.....	4
Schutz von Betroffenen vor Missbrauch von Identitätsdaten und Überidentifizierung.....	5
Festlegung einer geeigneten Schwelle zur Notifizierung.....	5
Mängel der bisherigen Umsetzung.....	6
Widersprüche hinsichtlich der Responsibilisierung des Individuums.....	6
Fehlende Datenschutzfunktionen und Funktionen für eine datensparsame Nutzung.....	7
Fehlen eines vertrauenswürdigen Entstehungsprozesses.....	7
Erhöhung des Schadensausmaßes durch aktuelle Technikgestaltung.....	9
Erschwerung robuster Wallet-Funktionen durch Technikgestaltung.....	10
Umsetzung auf weiteren Plattformen.....	11
Unklarer Anspruch an die Barrierefreiheit der Umsetzung.....	11
Ausblick und generelle Empfehlung.....	12
Bezug der Sachverständigen zum Themengebiet.....	14
Über den Innovationsverbund Öffentliche Gesundheit e. V.....	14

Kurzfassung

Rechtlicher Rahmen: Der Entwurf des Digitalen Identitätengesetzes (DIdG) lässt wesentliche Schutzmaßnahmen vermissen. Durch unzureichende Kontrollen und vage Rechtsgrundlage bei der Registrierung von Diensteanbietern droht ein „Cookie-Banner 2.0“ mit übergriffigen Datenabfragen. Zudem fehlt ein gesetzliches Opt-out für biometrische Lichtbilder sowie ein klarer Rechtsrahmen für die Sanktionierung von Datenmissbrauch und die dauerhafte Finanzierung notwendiger Dienste wie des PIN-Rücksetzprozesses.

Technische Umsetzung: Die technische Realisierung weist kritische Mängel auf. Es fehlen essenzielle Privacy-by-Design-Funktionen wie Pseudonyme und Funktionen zur Wahrnehmung von Datenschutzrechten. Die gewählte Cloud-Architektur schafft einen zentralen „Single Point of Failure“ und erhöht das Schadensausmaß bei Datenabflüssen massiv. Zudem mangelt es dem Entwicklungsprozess an Transparenz und Offenheit, die für eine vertrauenswürdige Umsetzung notwendig wären. Ein Go-Live zum geplanten Termin im Januar 2027 erscheint aufgrund dieser tiefgreifenden Defizite kaum realisierbar.

Vorbemerkung

Bei kritisch-konstruktiver Analyse von Digitalvorhaben im politischen Raum in Deutschland wird oftmals der Vorwurf laut, „gegen Digitalisierung zu sein“. Im Kontext der deutschen Umsetzung der European Digital Identity Wallet (im Folgenden kurz Wallet, Bezeichnung der Bundesregierung: d-you) wurden Vorwürfe – gegen „die Wallet“ zu sein – nach Kritik an der Umsetzung auch in der Presse geäußert. Deutschland müsse jetzt „mutig digitalisieren“. Es sei in diesem Zuge darauf hingewiesen, dass solche öffentlichen Aussagen allein nichts an der Güte der finalen Umsetzung dieses für die gesamte Bevölkerung relevanten Themas verbessern werden.

Eine menschenzentrierte, zugängliche und die Bevölkerung befähigende Umsetzung der Thematik der digitalen Identitäten wird nur dann möglich werden, wenn bei der Umsetzung digitaler Identitäten Kritik als konstruktives Element für bessere digitale Lösungen für uns alle aufgenommen wird. Andernfalls drohen digitale Lösungen, die uns allen schaden und das Vertrauen in die staatliche Handlungsfähigkeit weiter erodieren.

Verbesserungsbedarfe der Gesetzgebung

In dieser Anhörung wird primär der „Entwurf eines Gesetzes zur Durchführung der unionsrechtlichen Vorschriften über die Europäische Brieftasche für die Digitale Identität sowie zur Änderung anderer Rechtsvorschriften (Digitale Identitätengesetz – DIdG)“ (BT-Drs. 21/7408) diskutiert, der die novellierte EU-Verordnung **eIDAS 2.0** (Verordnung (EU) 2024/1183) in nationales Recht überführen soll. Die nationale Umsetzung ist an einen europäischen Rahmen gebunden, kann aber national entsprechend der gesetzlichen Möglichkeiten ausgestaltet werden. Nicht alle Mängel und Herausforderungen der Umsetzung zu eIDAS 2.0 / zur Wallet in Deutschland sind rein gesetzlicher Natur, der zu schaffende gesetzliche Rahmen bildet aber die Grundlage, um die bislang nicht hinreichende Technikgestaltung mit möglichen negativen Folgen entsprechend abzumildern. Die Empfehlungen stellen nur eine Minimalforderung an möglichen Anpassungen dar.

Registrierung und Kontrolle von Diensteanbietern

Die in § 10 EBDIG vorgesehene Registrierung von vertrauenden Beteiligten (Diensteanbietern) lässt im Vergleich zu ähnlich gelagerten Registrierungen bei Identitätsdiensten in Deutschland Schutzmaßnahmen vor Missbrauch vermissen. Solche möglichen Begrenzungen ex ante sind etwa im Kontext der Berechtigungszertifikate des Personalausweisgesetzes (§ 21 PAuswG) klarer umrissen. Aktuell sind Abfragen über Berechtigungszertifikate in der eID-Infrastruktur beispielsweise auf drei Jahre beschränkt und enthalten bei Missbrauch bereits entsprechende Bußgeldvorschriften (§ 32 PAuswG). Im Kontext der geplanten Gesetzgebung fehlen diese aber (vgl. Stellungnahme von epicenter.works).

Ebenso enthält die Registrierung keine Begrenzung der abgefragten Daten aufgrund eines gesetzlichen Rahmens nach eIDAS (vgl. Stellungnahme vom VZBV). Die Bundesregierung hält das nach Antwort in kleiner Anfrage (Drucksache 21/7319) nicht für leistbar, aber: Auch hier gibt es

bereits Anbindungsprozesse in der Verwaltungsdigitalisierung, welche hier als Orientierung dienen könnten: Im Kontext des National Once Only Technical Systems wird technisch schon in der Vermittlungsstelle in Kombination mit dem Datenmanagementsystem eine abstrakte Berechtigungsprüfung durchgeführt, ob eine bestimmte Abfrage rechtlich überhaupt zulässig sein kann. *(Der Hinweis auf das NOOTS heißt nicht, dass alles an der Umsetzung am NOOTS gut ist. Aspekte wie eindeutige Personenkennziffern und Weiteres sind hier überaus kritisch zu sehen.)* Für eine abstrakte Berechtigungsprüfung wäre bei der Registrierung mindestens die Abfrage des Rechtsrahmens notwendig, die bisher nicht stattfindet.

Damit stellt der aktuelle gesetzliche Rahmen eine Verschlechterung für Bürger*innen dar.

Damit werden Szenarien wiederholter Datenanfragen ermöglicht, die bei Betroffenen ähnlich wie bei bisherigen Einwilligungsmechanismen zu einer stärkeren Weitergabe von personenbezogenen Daten führen können, als eigentlich persönlich intendiert („**Cookie-Banner 2.0**“). Eine staatliche Wallet, wie d-you, kann zu einer weiteren Legitimation solcher übergreifenden Anfragen führen, weil deren staatliche Vertrauensstellung Anfragen legitimer erscheinen lassen kann. Gerade deshalb ist eine tiefergehende Prüfung der möglichen Datenanfragen von Anbietern sinnvoll. Hier kann eine nach dem Schutzbedarf der abgefragten Daten **abgestufte Prüfung von Diensteanbietern stattfinden**, etwa durch Unterstützung des BfDI oder bereits erwähnte etablierte Prozesse im Bundesverwaltungsamt.

Im Sinne von Bürokratieabbau könnten bei der Registrierung weniger stark invasive Datenabfragen (etwa von pseudonymen oder anonymen Daten) über einfachere und damit schnellere Registrierungsverfahren ermöglicht werden. Damit würde die Prozessgestaltung der Registrierung selbst zu einer datensparsameren und bewussteren Abfrage von Daten durch Diensteanbieter beitragen.

Empfehlung: Einführung eines risikobasierten Registrierungsverfahrens, Ergänzung von Schutzmaßnahmen ex ante wie Fristen und Prüfung der Angemessenheit bei der Registrierung, mindestens Plausibilisierung des Rechtsrahmens zu Datenabfragen, nachdem Diensteanbieter Daten anfragen

Freiwilligkeit und diskriminierungsfreier Zugang

Die Nutzung einer Wallet ist nach Art. 5a Abs. 15 eIDAS 2.0 freiwillig. **In der praktischen Realität wird eine De-facto-Nutzungspflicht aber durch Unternehmen, die Verwaltung und durch große Online-Dienste bestimmt.**

Integrieren diese Anbieter Wallet-Funktionen in ihre digitalen Anwendungen, kann es wegen einer versprochenen Bequemlichkeit durch die Nutzung der Funktionen der Wallet zu einem De-facto-Nutzungszwang der Wallet kommen. Darin liegt ein immenses Risiko, wie der Paritätische Gesamtverband feststellt: „**Die EUDI-Wallet darf nicht als vorgeschaltete Zugangshürde für staatliche oder soziale Leistungen wirken.**“ Der regulatorische Hebel gegen eine solche Entwicklung liegt bei der Registrierung der Diensteanbieter nach § 10 EBDIG. Bei der Registrierung sollten hier schon entsprechende diskriminierungsfreie Alternativen (z. B. direkte

Nutzung der eID-Funktionen und analoge Ersatzverfahren) bei der Registrierung abgefragt werden. Ebenso sollte entsprechendes Wissen, wie alternative, diskriminierungsfreie Wege ausgestaltet werden, aufgebaut werden.

Aufseiten der betroffenen Personen ist eine Anlaufstelle, wie von epicenter.works ebenfalls gefordert, ratsam, um **diskriminierungsfreie Zugangswege gegenüber Diensteanbietern durchsetzen zu können**. Ebenso wichtig sind in der Folge mögliche Sanktionsverfahren gegen Diensteanbieter.

Unabhängig von der Seite der Diensteanbieter ist für Personen, welche die Wallet nutzen wollen, dauerhaft ein diskriminierungsfreier Zugang zur digitalen Identifizierung notwendig. **Das Nadelöhr zur digitalen Identifikation ist dabei in Deutschland traditionell die (Suche nach der) PIN des Personalausweises**. Hier hat die Bundesregierung mit dem PIN-Rücksetzdienst inzwischen wieder eine kostenfreie Möglichkeit zum Onboarding geschaffen. Allerdings wurde der PIN-Rücksetzdienst wegen der nicht sichergestellten Finanzierung immer wieder ausgesetzt. Hier sollte in der Gesetzgebung evaluiert werden, ob hier ein Rechtsrahmen zur dauerhaften Finanzierung des PIN-Rücksetzdiensts geschaffen werden kann.

Empfehlung: Prüfung von Zugangsalternativen bei der Registrierung von Diensteanbietern, Schaffung einer Anlaufstelle für Betroffene gegen Diskriminierung im Zugang, dauerhafte Finanzierung des PIN-Rücksetzdiensts

Gesetzlich verankertes Recht auf Opt-out aus biometrischen Lichtbildern in der Wallet

Nach § 20 des EBDIG wird in der Gesetzgebung bisher kein Gebrauch vom europäischen Rechtsrahmen gemacht, der es Mitgliedstaaten ermöglicht, biometrische Lichtbilder optional zu erheben (nach Tabelle 1 Annex des Durchführungsrechtsakts 5a zur eIDAS-Verordnung). **Damit werden alle Nutzer*innen dazu verpflichtet, ein biometrisches Lichtbild in der Wallet zu hinterlegen, ohne Möglichkeit zum Opt-out.**

Hiermit betreibt die Bundesregierung weitere Maßnahmen zur Zentralisierung und weiteren Nutzung digitaler biometrischer Daten, welche durch die Nutzung von signierten Daten in der aktuellen deutschen Implementierung weiter verschärft werden. **In Kombination mit der Freiheit der Diensteanbieter, gewissermaßen alle beliebigen Daten abzufragen, wird das „Cookie-Banner 2.0“ weiter verschärft** und übertrifft damit die Warnungen von CCC und FiFF aus dem Jahr 2021 deutlich. Solche Bestände biometrischer Daten bedeuten immer immense Machtzuwächse und sind in freiheitlichen Demokratien stets begründungspflichtig, mindestens hinsichtlich der Erforderlichkeit oder Verhältnismäßigkeit. Ebenso entstehen durch schlecht gesicherte Übertragungssysteme einerseits sowie durch den zentralisierten Datenbestand andererseits gefährliche Einfallstore für Kriminelle oder andere unbefugte Dritte.

Empfehlung: Aufnahme eines Opt-out-Rechts zur Speicherung eines biometrischen Lichtbilds in die Wallet, Absicherung von Diensteanbietern bei Abfrage des biometrischen Lichtbilds

Schutz von Betroffenen vor Missbrauch von Identitätsdaten und Überidentifizierung

Inzwischen liegt leider jeder massenhaften Verarbeitung von personenbezogenen Daten ein hohes Missbrauchspotential inne, auch wenn technische Maßnahmen und rechtliche Vorgaben da einzudämmen scheinen. Im Kontext der Recherchen zu den Databroker-Files werden immer wieder Szenarien deutlich, wie allein durch Metadaten umfassende, standortgenau aufgelöste Profile von Personen geschaffen werden können. **Die massenhafte Bereitstellung von Wallets mit staatlich verifizierten und technisch signierten Informationen droht, dieses Szenario in Kombination mit der schon beschriebenen Gefahr eines „Cookie-Banner 2.0“ weiter zu verschärfen.**

Datenhändler, die im Kontext von eIDAS durch Datenhehlerei und Verkettung von Daten im Hintergrund auffallen (Erzeugung von Schattenprofilen), müssen hier scharf sanktioniert werden können. Eine mögliche rechtliche Referenz könnte hier § 202d StGB sein.

Für Betroffene wird im Kontext der europäischen Umsetzung gerade an einer Referenzimplementierung von Datenschutzfunktionen gearbeitet, wie einem Datenschutz-Dashboard, aber auch der Möglichkeit, verdächtige Anfragen digital melden zu können. Hier sollte ins Gesetz eine digitale, medienbruchfreie Regelung aufgenommen werden, die eine Verarbeitung solcher Anfragen schnell und unbürokratisch ermöglicht (vgl. Stellungnahme von epicenter.works).

Empfehlung: Evaluierung der Erweiterung der Gesetzgebung auf das Szenario Datenhehlerei bei Schattenprofilierung, Ergänzung der Gesetzesgrundlage um einen digitalen Meldeweg bei Datenmissbrauch oder verdächtigen Anfragen

Festlegung einer geeigneten Schwelle zur Notifizierung

Nach Aussage der Bundesregierung wurde die Wallet bisher nur durch eine beschleunigte Sicherheitszertifizierung (BSZ) geprüft (vgl. kleine Anfrage (Drucksache 21/7319)). Nach Artikel 7 der eIDAS-Verordnung sind entsprechende Sicherheitsniveaus sicherzustellen. Dies kann rein praktisch erst dann erfolgen, wenn der volle Funktionsausbau und **eine neutrale, gewissenhafte und vollständige Zertifizierung** erfolgt sind (vgl. epicenter.works oder BAG Selbsthilfe).

Empfehlung: Festlegung einer geeigneten Schwelle zur Notifizierung, die auf dem vollen Funktionsumfang sowie einer vollständigen Zertifizierung basiert

Mängel der bisherigen Umsetzung

Als Vorbemerkung zur Umsetzung muss ergänzt werden, dass im parlamentarischen Prozess weniger als drei Monate vor dem geplanten Go-Live der Wallet am 02. Januar 2027 noch der Rechtsrahmen diskutiert wird. **Es erscheint überaus ambitioniert, die substanziellen Änderungen aufgrund rechtlicher Anpassungen, welche anzuraten sind, zum Start der Wallet funktional und sicher umsetzen zu können.** Üblicherweise liegt zwischen Verabschiedung des rechtlichen Rahmens und dem Go-Live einer darauf aufbauenden Umsetzung mindestens ein Jahr.

Widersprüche hinsichtlich der Responsibilisierung des Individuums

Eine wesentliche Säule bei der Umsetzung der Wallet ist das Konzept der selbstbestimmten Identität (Self Sovereign Identity). Dabei wird die volle Datenkontrolle dem Individuum übertragen, so auch Aussagen auf der Webseite zur Wallet. Für die Freigabe und Kontrolle einer Datenanfrage ist am Ende also die betroffene Person selbst verantwortlich. Im Wesentlichen kommt dann dem Individuum selbst die Aufgabe zu, die Weitergabe von Daten feingranular zu beeinflussen.

In Hinblick auf andere Digitalvorhaben der Bundesregierung aus den vorherigen Legislaturen ergibt sich hier allerdings ein Widerspruch. Im Kontext der elektronischen Patientenakte gilt aktuell, dass ähnlich gelagerte Freigabeprozesse bestimmter Daten an bestimmte anfragende Stellen aus Sicht der Benutzungsfreundlichkeit nicht zumutbar seien, vgl. Antwort auf eine kleine Anfrage (Drucksache 21/2238) zur elektronischen Patientenakte.

Im Kontext der Wallet wird nun aber im Gesundheitsbereich bald eine auf der Wallet basierende GesundheitsID mit dem Kontext von SSI und selektiver Freigabe für den Zugang verwendet werden. Um einen Zugang zu Daten einer elektronischen Patientenakte zu bekommen, bei dem ein ähnlich kompliziertes feingranuläres Rechtemanagement wiederum nicht zumutbar sei. Das erscheint hochgradig widersprüchlich und ist in einem Ende-zu-Ende-Benutzungsszenario konzeptionell kaum nachzuvollziehen und der Bevölkerung kaum verständlich zu vermitteln. **Hier wäre eine ressortübergreifende Abstimmung anzuraten, welche Freiheitsgrade bei Datenfreigaben der Bevölkerung in der Breite zumutbar sein sollen und ob die zugemuteten Freiheitsgrade auch im Kontext SSI als Teil einer Datenschutz- und Sicherheitsarchitektur anzusehen sind.**

Empfehlung: Prüfung, inwieweit das Konzept von SSI konzeptionell in Einklang mit den Möglichkeiten von Datenfreigabe bei anderen Digitalvorhaben steht

Fehlende Datenschutzfunktionen und Funktionen für eine datensparsame Nutzung

Für die Umsetzung der Wallet stehen aktuell wesentliche datensparsame Funktionsprimitive nicht zur Verfügung, etwa Pseudonyme. Gute eID-Systeme, so schreibt auch der BfDI in seinem Tätigkeitsbericht 2023, sollten „Selective Disclosure und Zero-Knowledge-Proofs beherrschen“.

Die Umsetzung von selektiver Freigabe bestimmter Daten über SD-JWT ist aktuell laut Codestand vom Anfang Oktober blockiert und aktuell bis jetzt nicht nutzbar, weil der europäische Rahmen fehlt.

Durch das Fehlen der Möglichkeit von Pseudonymen steht die Umsetzung in Konflikt mit Artikel 5 der eIDAS-Verordnung, welche aussagt, dass **die Benutzung von vom Nutzer gewählten Pseudonymen ohne Einschränkung ermöglicht werden muss** (sofern keine anderen rechtlichen Gründe dagegen sprechen).

Bei der aktuellen Umsetzung der Wallet kann nicht von einer Privacy-by-Design-Umsetzung gesprochen werden, weil wesentliche Funktionen nicht vorliegen, die bei einer privatsphäreschonenden Umsetzung der notwendige Ausgangspunkt gewesen wären, um von dort schrittweise mehr persönliche Daten freizugeben. Dies ist nicht allein ein Mangel der deutschen Umsetzung, allerdings sind entsprechende Meilensteine oder eine Höherpriorisierung in der deutschen Umsetzung ebenfalls nicht erkennbar.

Ein Start mit einer nicht datensparsam nutzbaren Wallet stellt einen erheblichen Mangel dar, weil damit nicht datensparsame Funktionen zum De-facto-Standard werden, mangels nutzbarer Funktionsalternativen. Eine ähnliche Forderung findet sich in der Stellungnahme des VZBV.

Für die Nutzung einer Wallet in einer datenschutzkonformen Art und Weise ist darüber hinaus das Vorliegen der gerade als Referenzimplementierung entwickelten Datenschutzfunktionen wie eines Datenschutzdashboards, Löschanfragen sowie die Meldung verdächtiger Anfragen.

Empfehlung: Klare Priorisierung von Funktionen zur datensparsamen Nutzung, Start der Wallet erst mit allen datensparsamen Funktionen von Beginn an, Start der Wallet nur mit Datenschutzfunktionen wie Dashboard, Löschanfragen sowie Meldung verdächtiger Anfragen

Fehlen eines vertrauenswürdigen Entstehungsprozesses

Vertrauenswürdige digitale Infrastrukturen können nur entstehen, wenn der Entstehungsprozess selbst Vertrauen ermöglicht. In der Genese der Wallet ist hier aber bereits viel Vertrauen verschenkt worden.

Zu Beginn der Entwicklung der Wallet wurde mittels eines offenen Konsultationsprozesses für die Architektur versucht, transparent und offen die Entwicklung der Wallet nachvollziehbar zu machen. Im Jahr 2023 wurde dieser Prozess hoffnungsvoll erwartet.

In der weiteren Entwicklung der Wallet haben sich Beteiligungsprozesse aber als „Fishing-for-Compliments“-Versuche herausgestellt, die keine echte kritische Beteiligung ermöglichen sollten.

Ein paar Beispiele für Mängel an der Vertrauenswürdigkeit des Prozesses:

- Im Austausch mit der SPRIND kam es zur Androhung einer Verleumdungsklage gegenüber dem InÖG bei Öffentlichmachung der Interessenkonflikte des Projektteams bei der Entwicklung der Wallet, welche zwischenzeitlich öffentlich wurden.
- Die Sandbox zur Anbindung der Relying Parties unterliegt seit Anbeginn einer Vertraulichkeitsklausel, sodass ein Austausch über technische Details im Vorfeld des Go-Live verhindert wird. Nach Aussage des BMDS sei dies zum Schutz von Geschäftsgeheimnissen gedacht, es schürt aber den Eindruck einer bewusst intransparenten Entwicklung.
- Anfragen nach dem Informationsfreiheitsgesetz zur Wallet wurden seitens des BSI seit Dezember 2025 nicht beantwortet.
- Die relevante technische Richtlinie TR 03189 ist nicht öffentlich einsehbar (bzw. noch nicht final?) und ermöglicht drei Monate vor Go-Live kein neutrales Nachvollziehen der Sicherheitseigenschaften der Wallet.
- Es fehlt das Bekenntnis zu einer Datenschutz-Zertifizierung oder mindestens die Veröffentlichung einer Datenschutzfolgeabschätzung (vgl. epicenter.works).
- Der Source Code wurde erst sehr spät im Entwicklungsprozess veröffentlicht (Anfang September 2026 bei Entwicklungsbeginn wohl im Jahr 2025). Mit dem Source Code, etwa der Apps, lassen sich keine reproduzierbaren Builds erzeugen. Eine tiefergehende neutrale Prüfung durch Dritte ist so nicht möglich.
- Die aktuelle Security Policy ermöglicht nur Meldungen anhand des veröffentlichten Produkts. Damit werden Meldungen von Sicherheitslücken auf den spätestmöglichen Zeitpunkt hinausgeschoben – wohl nach dem Chaos Communication Congress Ende 2026. Damit wird ein sicherheitstechnisch anzustrebendes Shift-Left-Vorgehen erschwert. Positiv zu erwähnen ist der Versuch einer Safe Harbor Regelung für verantwortungsvolle Sicherheitsforschung. Ob dieser am Ende rechtlich bindend ist, ist angesichts der immer noch stockenden Überarbeitung des Computerstrafrechts nicht vollständig klar.
- In der kleinen Anfrage (Drucksache 21/7319) an die Bundesregierung wird von einer Beteiligung des Chaos Computer Clubs an einem Datenschutzworkshop 2024 gesprochen. Eine solche Beteiligung hat nach Angaben des CCC selbst nie stattgefunden.
- Wiederum nicht aufgeführt bei Terminen mit der Zivilgesellschaft ist beispielsweise der InÖG

mit der Teilnahme an diversen Terminen, wie etwa Workshops zu Use Cases, Geschäftsmodellen, Datenschutz & Sparsamkeit, der “Ecosystem Governance and Operating Models Working” Group nicht benannt.

- Ein öffentlicher Architekturworkshop zur Konsultation der Architektur mit Stakeholdern hat – trotz Ankündigung – nicht stattgefunden. Es gab damit also keine dedizierte Konsultation zur Architektur
- Die FAQ auf der Webseite spricht davon, dass bereits die Architektur bewusst so gestaltet sei, dass keine zentrale Stelle die Nutzung nachvollziehen kann. Das ist wegen eines zentrale Cloud-Sicherheitsankers ein architektonisches Paradoxon. (Diese Kritik wurde 2025 auf dem Chaos Communication Congress geäußert, netzpolitik hat darüber berichtet).
- In der kleinen Anfrage (Drucksache 21/7319) wird dazu behauptet, dass “bei der Nutzung eines authentifizierten Kanals wäre der Aussteller der PID in jeden Nutzungsvorgang einer PID involviert und würde damit die Person und den Nutzungszeitpunkt erfahren”. Das ist falsch, weil der Aussteller der PID in einer eID-Kommunikation gar nicht involviert ist. Allein im Gesundheitswesen gibt es sehr viele eID-Server, etwa voneinander getrennt bei der AOK, TK, DAK, BKK, Barmer, HEK, Knappschaft... Es gibt in Deutschland mindestens drei öffentlich gelistete eID-Serverbetreiber, die noch weitaus mehr eID-Server betreiben können.

In Summe kann daher wegen solcher wiederholter Intransparenz und Fehlern bei einem solchen Prozesses der Entwicklung eines Produkts, dem die ganze Bevölkerung vertrauen können soll, bislang kein Vertrauen ausgesprochen werden. Ein vertrauenswürdiger Entstehungsprozess ist die Basis eines vertrauenswürdigen digitalen Produkts.

Empfehlung: Etablierung eines konsequenten Open Development-Prozesses, Veröffentlichung zurückgehaltener Dokumente und Richtlinien, Reflexion von Vertraulichkeitsklauseln, Verifizierung der Kommunikation auf Korrektheit und Ehrlichkeit

Erhöhung des Schadensausmaßes durch aktuelle Technikgestaltung

Bei der Entwicklung der Wallet wurde im Rahmen des ARF eine Architekturvariante gewählt, die als C' bezeichnet wird (Signed Credential with Cloud Support (C')). Dabei wird die Präsentation von personenbezogenen Identitätsdaten (PID) mittels eines Sicherheitsankers in der Cloud (RWSCD - Remote Wallet Secure Cryptographic Device) unterstützt. Die gewählte Entscheidung erhöht zwei Risiken beträchtlich:

- Ein Ausfall des Cloud-Sicherheitsankers führt kurzfristig zu einem Ausfall von Funktionen der gesamten nationalen digitalen Identitätsinfrastruktur. Dabei ist keine Ausstellung von PID-Daten mehr möglich. Die Präsentation von PID gegenüber Diensteanbietern ist nicht mehr möglich. **Der Cloud-Sicherheitsanker ist in dem Fall ein nationaler Single Point of Failure.** Nicht alle Funktionen der Wallet können durch andere Ersatzsysteme (wie die eID-Infrastruktur) aufgefangen werden, weil bestimmte Abfragen nur mittels der

Walletinfrastruktur möglich sein werden.

- **Durch die Verwendung von signierten Daten als Absicherung der Integrität der übermittelten Daten wiegen Datenabflüsse schwerer, weil abgeflossene Daten als garantiert echt bewiesen werden können.** Dieses Risiko ist an allen Punkten der digitalen Identitätsinfrastruktur höher, also auch bei allen Diensteanbietern.

Diese Entscheidung fällt in folgende Gesamt-Cybersicherheitslage: Im Mai 2026 wurde seitens des BSI eine neue Zeitrechnung der Cybersicherheit deklariert in Folge des Aufkommens von KI-Modellen mit Fähigkeiten, Sicherheitslücken eigenständig zu entdecken und teilweise selbstständig auszunutzen.

Im Jahr 2022 wurde noch seitens des BSI die Variante signierter Daten als Variante beschrieben, **die nicht verwendet werden sollte** – zugunsten der Variante eines authentifizierten Kanals.

Die gewählte Architektur widerspricht dem Prinzip von Security by Design und hat per Design eine große öffentlich erreichbare Angriffsfläche. Das Schadensausmaß wird durch das Design nicht reduziert, es wird sogar erhöht. Die vermeintlichen Mehrwerte an Robustheit durch signierte Daten werden durch die Gefahr eines Totalausfalls egalisiert.

Empfehlung: Architekturentscheidung C' überdenken, weitere Schutzmaßnahmen andenken im Falle der Weiternutzung von C'

Erschwerung robuster Wallet-Funktionen durch Technikgestaltung

Die Entscheidung für signierte Daten wurde auch mit einer besseren Offline-Verfügbarkeit begründet. In der aktuell vorliegenden Umsetzung ist eine Offlinefähigkeit nicht vorhanden.

Durch den Sicherheitsanker in der Cloud ist bei fast allen Interaktionen mit der Wallet eine Onlineverbindung notwendig, etwa bei der Ausstellung von persönlich identifizierenden Daten (PID), aber auch bei der Präsentation dieser Daten. "Für die Nutzung der sicheren Wallet-Ausweisfunktion (PID) ist in der aktuellen Architektur eine Internetverbindung erforderlich, da die Prüfung über serverbasierte Sicherheitsmechanismen erfolgt.", so die FAQ zur Wallet.

Bisher ist nur die Verfügbarkeit von lokal gespeicherten Nachweisen (z. B. digitaler Führerschein) auch offline anzunehmen. Im europäischen Rahmen definierte Wallet-zu-Wallet Use Cases (Proximity) sind noch nicht definiert.

Grundsätzlich ist mit der aktuellen Umsetzung zwar möglich, den Vorgaben (z. B. Art. 5a(5)(a)(iii)) und Erwägungsgründen von eIDAS gerecht zu werden, allerdings dürfte die praktische Nutzungserfahrung immer wieder etwas haken.

Der technische Rahmen des ARF würde eine Online-Verbindung für die Attestierung zwar mindestens alle 24 Stunden erfordern, bei der Ausgestaltung der Funktionen selbst existiert aber Handlungsspielraum für eine bessere Nutzbarkeit in wechselnden Onlineverfügbarkeiten wie in Deutschland (immer mal wieder, immer noch).

Empfehlung: Architekturentscheidung C' überdenken

Umsetzung auf weiteren Plattformen

Die Wallet wird bislang nur über die offiziellen App-Stores von Google (Play Store) und Apple (App Store) für Android und iOS angeboten. Nach [FAQ](#) ist hierfür zwar kein Account notwendig, es werden in der Praxis zur Verteilung der Apps allerdings die offiziellen App-Stores genutzt, womit doch wieder eine Nutzung von offiziellen App-Stores von Google und Apple notwendig ist, die nicht vollständig europäisch kontrolliert werden können.

Um einem möglichen Wegfall der App-Verteilung über offizielle App-Stores aufgrund von geopolitischen Spannungen vorzubeugen, würde es helfen, **frühzeitig Versionen der Wallet für GrapheneOS** anzustoßen, welche nach Architecture Reference Framework (ARF) explizit möglich wären. Ein Sideloadung, also eine Verteilung der Apps über weitere herstellerunabhängige App-Stores, wäre dann später durchführbar und trägt so zur Resilienz der Walletinfrastruktur bei.

Weitere Android-Varianten außer GrapheneOS verfügen allerdings nicht über Möglichkeiten zur Hardware-Attestierung und sind damit nach dem aktuellen ARF nicht geeignet.

Kritisch im Kontext der Umsetzung bleibt die Kontrolle der Anbieter offizieller App Stores über die Sperrung von Apps oder App Updates (wie etwa bei der Ablehnung eines Updates von Spotify 2024) oder individuelle Accounts (wie im Falle des internationalen Gerichtshofes). Eine Folge einer solchen Sperre wäre auch der Verlust von Sicherheitsfunktionen, die für die Attestierung der Wallet für deren Benutzung notwendig wären. Daher ist es zu empfehlen, weitere Attestierungsverfahren zu evaluieren.

Empfehlung: Etablierung von Wallet-Versionen für weitere Betriebssysteme und App-Stores, Evaluation von weiteren Attestierungsverfahren

Unklarer Anspruch an die Barrierefreiheit der Umsetzung

In der Kommunikation um die Wallet wird ein unterschiedlicher Anspruch an die Barrierefreiheit kommuniziert. Aufseiten des BMDS wird von barrierearm gesprochen. Auf der Informationsseite zur Wallet selbst von barrierefrei. Es sei an dieser Stelle darauf hingewiesen, dass **nur eine vollständig barrierefreie Wallet** rechtlich nach Behindertengleichstellungsgesetz (BGG) und BITV 2.0 für öffentliche Stellen vorgeschrieben ist. Entsprechende Regelungen fehlen auch im DIdG, wie auch die BAG Selbsthilfe anmahnt.

Empfehlung: Präzisierung der Anspruchshaltung zur Umsetzung der Barrierefreiheit in der Kommunikation um die Wallet, Nachweis der vollständigen Barrierefreiheit durch Offenlegung der relevanten Zertifizierungen (z. B. BIK BITV für Apps)

Ausblick und generelle Empfehlung

Es ist im Kern generell begrüßenswert, dass sich Europa und in nationaler Umsetzung die Bundesregierung dem Aspekt digitaler Identitäten umfänglich annehmen, um hier einen europäisch harmonisierten Rechts- und Funktionsrahmen für die Digitalisierung zu schaffen.

Gerade das Fehlen sicherer und gut verfügbarer digitaler Identitäten hat zuletzt in diversen Bereichen der Digitalisierung Probleme verursacht.

Der aktuelle Gesetzentwurf enthält aber noch große Baustellen und ungeklärte Fragen. Die Bundesregierung sollte tunlichst vermeiden, dass:

- einer Wallet offiziell als bereit deklariert wird, die elementare Funktionen zur datensparsamen Nutzung vermissen lässt: Pseudonyme, Zero-Knowledge-Proof, Datenschutzübersichten und die Möglichkeit, Datenschutzrechte nahtlos digital auszuüben.
- einer Wallet als fertig deklariert wird, die durch Architekturentscheidungen erhebliche Defizite bei der Eindämmung des potenziellen Schadensausmaßes und der Funktion ohne Internetverbindung hat.
- eine Gesetzgebung verabschiedet wird, die für den Schutz der Bürger*innen-Rechte einen Rückschritt bedeuten würde („Cookie-Banner 2.0“), weil kaum sinnvolle Auflagen für Diensteanbieter existieren.

Es muss stark infrage gestellt werden, ob die beschriebenen Mängel zum 02. Januar 2027 sinnvoll behoben werden können.

Sofern etwas Erfreuliches in der zu erwartenden Entwicklung zu sehen sein soll, muss man es mit Thomas Jarzombek, Parlamentarischem Staatssekretär beim Bundesminister für Digitales und Staatsmodernisierung, halten:

„Wir werden sicherlich das Highlight werden irgendwann auf dem CCC Jahrestreffen. Da gehen wir fest von aus.“

Diese Stellungnahme endet mit zwei kaum veränderten Zitaten aus einem offenen Brief zur elektronischen Patientenakte von 2023 und einer Stellungnahme von CCC und FiFF von 2021, die in Verkettung kaum verändert so stehen können:

Die Politik geht ansonsten Risiken ein, die am Ende von den Individuen getragen werden müssen. Sie reichen von Gefahren für die individuelle Privatsphäre, Ausfall von Systemen oder Manipulation von Daten – diese Risiken tragen am Ende die Bürger*innen persönlich.

Auch wenn sichere digitale Identitäten auf mobilen Endgeräten *in Form einer europaweit interoperablen Wallet* grundsätzlich begrüßenswert wären: Im Falle des vorliegenden

Gesetzentwurfes und der aktuell vorliegenden Umsetzung wurden die – *besonders für die Bevölkerung negativen* – Erfahrungen aus den vorherigen Digitalvorhaben und Regelungen leider schlicht ignoriert.

Bezug der Sachverständigen zum Themengebiet

Bianca Kastl ist 1. Vorsitzende des Innovationsverbunds Öffentliche Gesundheit und engagiert sich für eine bessere Digitalisierung von Verwaltung und Gesundheitswesen in Deutschland.

Ihr fachlicher Schwerpunkt sind skalierende, sichere digitale Infrastrukturen, Systemarchitekturen, Cloud-native Anwendungen, IT-Security mit dem Fokus auf Zero-Trust-Prinzipien, Privacy sowie Barrierefreiheit und User Experience, seit Jahren in Open Source.

Beruflich ist sie als Tech Lead und Chief Product Owner im Öffentlichen Dienst tätig und entwickelt mehrfach ausgezeichnete, vernetzte Anwendungsplattformen nach Stand der Technik.

Über den Innovationsverbund Öffentliche Gesundheit e. V.

Der Innovationsverbund Öffentliche Gesundheit (InÖG) e. V. entwickelt und begleitet als gemeinnütziger Verein langfristig innovative Civic-Tech- und eGovernment-Lösungen im Bereich des digitalen Gesundheitswesens und der öffentlichen Verwaltung. Er begleitet das Thema digitale Identitäten seit 2021. Seine Mitglieder waren seit August 2022 Teil der zivilgesellschaftlichen Vertreter im interministeriellen Laborformat für Digitale Identitäten GovLabDE Digitale Identitäten (GovLabDE DI).

Der InÖG agiert überparteilich sowie unabhängig von Unternehmen und Verbänden.

Eintrag im Lobbyregister