

Frequently Asked Questions

HINWEIS: Dieses Dokument wurde im Nachgang der BAGFW-Infoveranstaltung am 30.01.2026 als Ergänzungsmaterial bereitgestellt. Es beantwortet Fragen, die während der Veranstaltung von Teilnehmenden im Chat geäußert wurden.

Die Antworten auf die folgenden Fragen sind zum Stand vom 18.02.2026 korrekt und können sich im Laufe der Projektentwicklung sowie bei der Ankündigung neuer Funktionen oder Pläne ändern.

1. Grundsätzliche Informationen

- **Was ist die EUDI-Wallet?**

Die EUDI-Wallet ist die digitale Brieftasche für alle Bürger:innen und Einwohner:innen der EU. Sie ermöglicht das sichere Speichern und Nutzen von Ausweisen und Nachweisen wie Personalausweis, Führerschein, Hochschulzeugnis oder das Deutschlandticket direkt auf dem Smartphone. EUDI-Wallets basieren auf einheitlichen technischen Standards, werden aber durch jeden Mitgliedstaat der EU eigenständig bereitgestellt. Die Nutzung erfolgt unter Einhaltung der höchsten Sicherheits- und Datenschutzstandards sowie europäischer und nationaler Vorgaben und ist für Nutzer:innen kostenfrei und freiwillig.

Nach der novellierten eIDAS-Verordnung haben EUDI-Wallets perspektivisch die folgenden Kernfunktionen:

1. Sichere Identifizierung auf hohem Vertrauensniveau mittels elektronischem Personalausweis und Aufenthaltstitel (eAT);
2. Speichern und Nutzen digitaler Nachweise;
3. Elektronisches Unterschreiben (mit sogenannten qualifizierten elektronischen Signaturen (QES));
4. Pseudonymisierung (Schutz von persönlichen Daten durch pseudonymes Login);
5. Bestätigung von Zahlungen mit der Wallet.

Bei der ersten Iteration der EUDI-Wallet liegt der Fokus auf der Umsetzung der Ausweis- und Nachweisfunktionen (Punkte 1 und 2).

- **Was sind „digitale Nachweise“ konkret?**

„Digitale Nachweise“ sind digital signierte Bescheinigungen über bestimmte Eigenschaften, Berechtigungen oder Qualifikationen einer Person, die maschinell verarbeitet werden können. Eine digitale Signatur schützt einen Nachweis kryptografisch gegen Manipulation. Der Empfänger eines Nachweises kann damit automatisch prüfen, ob eine Bescheinigung echt ist, was beispielsweise bei Fotos von Ausweisen nicht möglich ist. Beispiele sind: Führerscheine, Ausbildungs- oder Hochschulzeugnisse und E-Rezepte. Mit digitalen Nachweisen können Nutzer:innen bestimmte Attribute (wie Name, Geburtsdatum, Adresse, Berechtigungen etc.) sicher, standardisiert und europaweit rechtsverbindlich nachweisen – online und vor Ort.

- **Was ist der aktuelle Umsetzungsstand in Deutschland?**

Deutschland entwickelt eine staatliche EUDI-Wallet, die Anfang 2027 als App erscheinen soll. Zum Start bietet sie die Möglichkeit, digitale Nachweise zu verwalten und zu nutzen, online wie auch vor Ort. Erste unterstützte Nachweise werden der elektronische Personalausweis und Aufenthaltstitel (eAT) sowie

Frequently Asked Questions

voraussichtlich der digitale Führerschein, der Sozialpass und der Rentenausweis sein. Weitere Nachweise folgen schrittweise – die Anzahl und Vielfalt dieser Nachweise hängt von der Mitwirkung der zukünftigen Aussteller (“Issuer”) im EUDI-Ökosystem ab. Wir suchen kontinuierlich und aktiv nach solchen Ausstellern. Falls Ihre Organisation zukünftig digitale Nachweise ausstellen möchte, finden Sie [hier weitere Informationen](#).

Seit Dezember 2025 steht die offizielle deutsche “EUDI-Wallet Sandbox” bereit. Die Sandbox ist eine nationale Testumgebung, in der Organisationen ihre Anwendungsfälle (“Use Cases”) und Integrationen mit der staatlichen EUDI-Wallet testen können, ausschließlich mit Testdaten. Die Sandbox ist das Einstiegstor ins nationale und europäische EUDI-Ökosystem. Derzeit wird die Wallet-Ausweisfunktion mittel aus elektronischem Personalausweis und Aufenthaltstitel (eAT) generierten Personenidentifizierungsdaten (oft als “PID” abgekürzt) unterstützt. Zeitnah werden weitere Nachweise unterstützt.

Die Entwicklung der staatlichen EUDI-Wallet erfolgt schrittweise, begleitet durch IT-Architekturarbeit, Pilotierungen und den SPRIND-Prototypenprozess. Neben der staatlichen Lösung werden zukünftig auch nicht-staatliche EUDI-Wallet Anbieter die Möglichkeit haben, ihre Produkte als EUDI-Wallet zertifizieren zu lassen. Alle Aktivitäten des deutschen EUDI-Wallet-Projekts sind über OpenCoDE, die Open-Source-Plattform für digitale Souveränität in Deutschland, öffentlich und transparent dokumentiert: <https://gitlab.opencode.de/bmi/eudi-wallet>.

- **Was ist das langfristige Ziel?**

Das langfristige Ziel der EUDI-Wallet ist der Aufbau einer europaweit einheitlichen und interoperablen digitalen Infrastruktur, mit der Menschen in der EU digitale Nachweise sicher speichern und grenzüberschreitend nutzen können. Die Wallet soll digitale Souveränität stärken, indem Nutzende selbst bestimmen, welche Daten sie teilen. Gleichzeitig schafft sie eine europäische, unabhängige Infrastruktur, die höchste Datenschutz- und Sicherheitsstandards erfüllt. Durch gemeinsame Standards ermöglicht sie eine nahtlose Nutzung in Verwaltung, Wirtschaft und Alltag und bildet damit ein zentrales Fundament für eine moderne und effiziente digitale Gesellschaft.

- **Wie ist die technische Architektur geregelt? Gibt es eine Beschreibung der nötigen Sicherheitsstandards?**

Die Umsetzung der EUDI-Wallet basiert auf der europäischen [eIDAS-2.0-Verordnung](#), den entsprechenden Durchführungsverordnungen (sog. “Implementing Acts”) und der EU-weiten Architektur- und Referenzrahmen-Spezifikation (oft als “ARF” abgekürzt), welche die zentralen technischen Standards, Sicherheitsmechanismen und Interoperabilitätsvorgaben definieren.

Die Entwicklung der staatlichen Wallet in Deutschland ist in einem [öffentlichen Architektur- und Konsultationsprozess](#) erfolgt. Das BSI begleitet die Umsetzung durch technische Vorgaben, Verfahren und Sicherheitsanforderungen. Die sich gerade in der Erstellung befindliche (und daher öffentlich noch nicht einsehbare) technische Richtlinie (TR) [TR-03189](#) legt fest, wie die EUDI-Wallet gestaltet sein soll und welche Komponenten darin zusammenwirken. Die Cybersicherheit-Zertifizierung der betreibenden Organisation erfolgt nach [ISO/IEC-27001](#); zusätzlich gelten spezifische technische Sicherheitsanforderungen gemäß den Vorgaben des BSI und des ARF.

Frequently Asked Questions

- **Wer ist der Auftraggeber der staatlichen EUDI-Wallet in Deutschland?**
Die Bundesregierung hat beschlossen, eine staatliche EUDI-Wallet bereitzustellen, die ab 2027 schrittweise eingeführt wird. Die fachliche Federführung liegt im Bundesministerium für Digitales und Staatsmodernisierung (BMDS). Die technische Umsetzung erfolgt im Rahmen des nationalen EUDI-Wallet-Projekts, welches durch die Bundesagentur für Sprunginnovation (SPRIND) mit weiteren Projektpartnern durchgeführt wird.
- **Macht die Einführung der Wallet verschiedene bisher genutzte Apps oder "Karten" überflüssig?**
Die Wallet wird eine sichere und datenschutzfreundliche Alternative zu vielen bestehenden Apps und analogen Dokumenten sein. In welchem Ausmaß sie genutzt wird und inwiefern sie einen Ersatz für bisher verwendete Apps und Karten darstellt, liegt in der Entscheidung der Nutzer:innen und Organisationen.
- **Wird das in Dänemark laufende System der MitID als Vorbild genommen oder wurde es in der Entwicklung per Evaluation einbezogen?**
Die deutsche Umsetzung basiert primär auf eIDAS 2.0, den entsprechenden Durchführungsverordnungen und dem EU-ARF. Nationale Modelle anderer Länder dienen nicht als verbindliche Grundlage, es besteht jedoch ein Austausch zwischen dem deutschen EUDI-Wallet-Projekt und den Projektteams in anderen EU-Ländern. Die eIDAS 2.0 Verordnung gilt in allen Mitgliedsländern und auch diese müssen mindestens eine EUDI-Wallet bereitstellen, was oft mit der Weiterentwicklung bestehender eID-Systeme wie der MitID einhergeht.

2. Nutzungsszenarien und Nutzungsumfang

- **Ist ein weltweiter Nutzen angedacht?**
Das grundlegende Ziel ist die Interoperabilität innerhalb der EU. Darüber hinaus ist auch die weltweite Nutzbarkeit ein klares Anliegen für die Zukunft.
- **Funktioniert die Wallet auch für Personen, die keinen deutschen Personalausweis besitzen, sondern einen ausländischen Reisepass und/oder eine deutsche Aufenthaltserlaubnis?**
Ja, die EUDI-Wallet kann grundsätzlich von allen Menschen zum Speichern und Teilen digitaler Nachweise genutzt werden, auch von Personen ohne deutschen Personalausweis oder elektronischen Aufenthaltstitel.
Möchte man die Wallet zur sicheren Identifizierung nutzen, ist diese Funktion an in Deutschland ausgegebene Identitätskarten mit aktiver Onlineausweis-Funktion (eID) gebunden (d.h. Personalausweis oder elektronischer Aufenthaltstitel).
- **Wie kommen Menschen aus anderen EU-Ländern in Deutschland an die EUDI-Wallet, müssen sie die aus ihrem Herkunftsland verwenden oder die aus Deutschland?**
Jeder Mitgliedstaat stellt eigene, aber interoperable EUDI-Wallets bereit. Bürger:innen und Einwohner:innen aus anderen EU-Staaten haben grundsätzlich die freie Wahl, ob sie die deutsche EUDI-

Frequently Asked Questions

Wallet nutzen möchten oder eine Wallet ihres Herkunfts- bzw. Aufenthaltslandes, die im Binnenmarkt künftig gegenseitig anerkannt wird.

- **Funktioniert die EUDI-Wallet nur mit Smartphone?**
Für die Nutzung der staatlichen National EUDI-Wallet wird ein Smartphone mit dem Betriebssystem iOS (Apple) und Android (Google) benötigt.
- **Gibt es auch Wallets für Organisationen?**
Für derartige Wallets ist derzeit eine weitere Verordnung in Arbeit, für die auf Seiten der deutschen Bundesregierung das Bundesministerium für Digitales und Staatsmodernisierung (BMDS) verantwortlich ist. Das nationale EUDI-Wallet-Projekt fokussiert auf die Bereitstellung der EUDI-Wallet (für natürliche Personen).
- **Wie verhält es sich im Fördermittel-Antragsverfahren mit digitalen Unterschriften? Wir müssen als gemeinnützige Organisation regelmäßig Fördermittel beantragen und dafür kostenpflichtige Zertifikate erwerben, um qualifizierte elektronische Signaturen leisten zu können. Wird es künftig möglich sein, diese Signaturen über die EU-weit geplante EUDI-Wallet zu nutzen, oder handelt es sich dabei um ein völlig anderes System, das nicht zur qualifizierten elektronischen Signatur gemäß eIDAS dient?**
Die EUDI-Wallet wird die qualifizierte elektronische Signatur (QES) zu einem späteren Zeitpunkt unterstützen. Die Bereitsteller von Fördermittel-Antragsverfahren können die EUDI-Wallet mit ihrer QES-Funktion nutzen, um den Antragsprozess digital, rechtssicher und nutzerfreundlich zu verbessern.

Weisen Sie entsprechende Anbieter gerne auf diese zukünftige Möglichkeit hin, da es sich hierbei um zentrale Anwendungsfälle für die Akzeptanz des EUDI-Wallet-Ökosystems sowie für die Nutzerfreundlichkeit der Wallet handelt.

Frequently Asked Questions

3. Wie funktioniert's?

- **Teile ich als Nutzer:in einen Nachweis, oder stimme ich einer Anfrage zur Nutzung z.B. durch eine Behörde (oder einer anderen vertrauenden Stelle/"Relying Party") "nur" zu? Oder geht beides?**
Nutzende verwalten selbstbestimmt ihre Nachweise in der EUDI-Wallet. Daten sind nur auf dem Smartphone der Nutzenden gespeichert und werden nur nach ausdrücklicher Freigabe in der Wallet an Dritte übertragen. Je nach Anwendungsfall kann es dabei variieren, wie genau der Prozess bis hin zur aktiven Freigabe abläuft. Grundsätzlich gibt es folgende Schritte:

1. Verbindungsaufbau ("Request")

Der Datenaustausch zwischen Wallet-Nutzer:in und der vertrauenden Stelle („Relying Party“), die Daten aus der Wallet empfangen möchte, wird beispielsweise durch Klicken auf eine Schaltfläche auf einer Website oder durch Scannen eines QR-Codes bzw. via NFC/Bluetooth mit dem Gerät, auf dem die Wallet installiert ist, gestartet.

2. Überprüfung der vertrauenden Stelle ("Trust Check")

Bevor die Daten gesendet werden, validiert die Wallet-App die Identität der Relying Party. Über digitale Vertrauenslisten wird sichergestellt, dass es sich um ein registriertes und vertrauenswürdigen Gegenüber handelt. In der App wird transparent angezeigt, wer genau die Anfrage stellt.

3. Selektive Offenlegung ("Consent & Selective Disclosure")

Die Nutzer:in erhält eine Übersicht der angeforderten Daten. Erst nach ausdrücklicher Bestätigung werden die Informationen für die Übertragung freigegeben. Alle Datenanfragen und (durchgeführten sowie abgelehnten) Transaktionen sind für die Nutzer:in in der Wallet dokumentiert und einsehbar.

4. Sicherer Transfer & Validierung

Die Daten fließen verschlüsselt direkt von der Wallet zur vertrauenden Stelle. Diese kann die Echtheit der Informationen sofort kryptografisch prüfen, da jedes Attribut vom ursprünglichen Aussteller digital signiert wurde. Eine Rückfrage beim Aussteller ist nicht nötig, was die Privatsphäre der Nutzer:in schützt – Aussteller von digitalen Nachweisen sind nicht automatisch in ihre Verwendung eingebunden.

- **Ist für die Nutzung der EUDI-Wallet eine E-Mail-Adresse verpflichtend?**
Nein.
- **Was sind die Personenidentifizierungsdaten (PID) in der EUDI-Wallet? Welche Ausweisdokumente brauche ich für das erstmalige Hinzufügen der PID?**
Die PID (kurz für Personenidentifizierungsdaten) kann aktuell aus den Chip-Daten eines Personalausweises oder elektronischen Aufenthaltstitel (eAT) mit aktiver Onlineausweis-Funktion generiert und in die Wallet übertragen werden. Die PID ist Voraussetzung für die Nutzung der Wallet-Ausweisfunktion und wird rechtlich dem bisherigen Online-Ausweisverfahren (eID) gleichgestellt sein. Im Gegensatz zum Online-Ausweisverfahren (siehe nächste Frage) brauche ich im Fall der PID mein Ausweisdokument nur für das erstmalige Hinzufügen in die Wallet. Danach wird die PID nur unter Nutzung des Smartphones verwendet.

Frequently Asked Questions

- **Woher weiß man, dass die Onlineausweis-Funktion (eID) des Personalausweises/elektronischen Aufenthaltstitels (eAT) aktiviert ist?**

Die Online-Ausweisfunktion ist bei Personalausweisen, die seit dem 15. Juli 2017 beantragt wurden, automatisch aktiviert. Ob die eID-Funktion eines Personalausweises oder eAT aktiviert ist, lässt sich etwa mit Hilfe der Ausweis-App prüfen. Grundsätzlich gilt: Für die Nutzung der eID im bisherigen Online-Ausweisverfahren wird ein NFC-fähiges Smartphone oder Kartenleser und die AusweisApp benötigt. Zudem muss eine PIN gesetzt werden und diese bekannt sein bzw. für das erstmalige Festlegen dieser PIN die sog. Transport-PIN vorliegen. Weitere Informationen zur Online-Ausweisfunktion finden Sie [hier](#).

- **Kann ich die Wallet auf verschiedenen Geräten installieren?**

Ja. Da digitale Nachweise lokal auf dem jeweiligen Endgerät gespeichert werden, müssen sie entsprechend auf jedem Gerät eingerichtet werden. Aus Sicherheitsgründen kann es in Bezug auf die Anzahl der Geräte, auf die ein bestimmter Nachweis eingerichtet werden kann, zu Einschränkungen kommen, wie z.B. bei Einrichtung der PID.

- **Wird in der EUDI-Wallet für die Nutzenden der jeweilige Datentransfer geloggt? Können die Nutzenden also explizit in einer Log-Ansicht sehen: Am 31.12.2027 um 12.43 Uhr wurden genau diese Daten xy an folgenden externen Dritten xy übertragen bzw. von einer bestimmten Stelle angefragt und die Freigabe abgelehnt?**

Ja, eine solche Funktion ist vorgesehen. Diese Ansicht wird Nutzenden innerhalb der Wallet-App zugänglich sein und ist dadurch vor dem Zugriff Unbefugter geschützt.

- **Welche Anforderungen muss ein Smartphone erfüllen, um die EUDI-Wallet nutzen zu können?**

Das Smartphone muss auf einem gängigen, aktuellen Betriebssystem (iOS oder Android) laufen. Für das erstmalige Hinzufügen der PID (Personenidentifizierungsdaten) ist ein Smartphone mit NFC-Funktionalität erforderlich, da das persönliche Ausweisdokument an die NFC-Kontaktstelle gehalten werden muss.

- **Wie funktioniert die Kryptographie in der EUDI-Wallet?**

Die EUDI-Wallet nutzt moderne Verschlüsselungsverfahren (starke Kryptographie und hardwaregestützte Schlüsseln), die von Sicherheitsforscher:innen weltweit als sicher eingestuft werden. Das kryptographische Schlüsselmateriale besteht aus privaten und öffentlichen Schlüsseln ("Private/Public Keys"), über die die Vertrauenswürdigkeit der digitalen Nachweise in der EUDI-Wallet abgesichert wird. Die privaten Schlüsseln für die digitalen Nachweise werden in einem speziellen Hardware-Sicherheitsmodul gespeichert (wie in einem Tresor). Die kryptographische Verschlüsselung von Inhalten bietet Schutz vor Fälschung und Identitätsdiebstahl.

- **Warum sind digitale Nachweise fälschungssicher?**

Digitale Nachweise in der EUDI-Wallet sind kryptografisch signierte Nachweise, deren Echtheit und Integrität jede vertrauende Stelle über die EU-weite Vertrauensinfrastruktur mithilfe sogenannter öffentlicher Schlüsseln verifizieren kann.

Frequently Asked Questions

- **Wie wird verhindert, dass sich eine andere Person als ich ausweisen kann?**

Bei jeder Nutzung der Wallet-Ausweisfunktion muss sich der Nutzer/die Nutzerin authentifizieren. Das erfolgt durch den Besitz des Smartphones (Besitzfaktor) und die Eingabe einer 6-stelligen PIN (Wissensfaktor). Mit diesen beiden Faktoren wird dann der Zugriff auf ein Hardware-Sicherheitsmodul auf einem Sicherheitsserver freigeschaltet, mit dem dann die Antwort auf die Anfrage der vertrauenden Stelle unterschrieben/kryptographisch signiert wird.

- **Was passiert, wenn ich mein Smartphone verliere?**

Nutzer:innen können über eine Webseite des Betreibers der staatlichen Wallet zu jedem Zeitpunkt ihre Wallet sperren lassen, gerade wenn sie keinen Zugriff mehr auf das entsprechende Smartphone haben. Die in der Wallet hinterlegten Nachweise müssen bei der erneuten Nutzung der EUDI-Wallet erneut hinzugefügt werden. Es ist geplant, diese Prozesse mit Blick auf die Nutzungsfreundlichkeit zu verbessern.

- **Wie wird sichergestellt, dass ein digitaler Nachweis aktuell ist?**

Die Aktualität wird sichergestellt, indem bei jeder Überprüfung durch eine vertrauende Stelle die Signatur und der Gültigkeitsstatus (z. B. statisches Ablaufdatum und Gültigkeit) eines Nachweises geprüft werden. Die Gültigkeit kann vom Aussteller beeinflusst werden (z.B. Zurückziehung), daher wird diese auf der Basis sogenannter Statuslisten geprüft. Dabei erfährt der Aussteller nicht, für welchen Nachweis die Prüfung erfolgt.

Manche Nachweise sind wie auch manche Papierdokumente dauerhaft gültig (z. B. Diplome), andere können kürzere Gültigkeiten haben.

- **Was muss eine Organisation erfüllen, um Wallet-Nachweise zu akzeptieren?**

Eine Organisation muss sich im EUDI-Ökosystem registrieren und erhält nach u.a. einer erfolgreichen Identifizierung ein Zugangs- und Registrierungszertifikat für die Organisation und den Anwendungsfall. Dieses zweistufige Verfahren erfolgt über standardisierte EU-Schnittstellen und wird zukünftig durch eine Online-Website ("EUDI-Wallet Hub DE") digital unterstützt. In einer öffentlichen Übersicht (sog. Transparenzregister) sind die registrierten Organisationen und Anwendungsfälle einsehbar. Das bedeutet, dass der Öffentlichkeit Informationen über die Aktivitäten von vertrauenden Stellen/„Relying Parties“ bezüglich der Abfrage und des Auslesens von Daten aus der EUDI-Wallet zur Verfügung stehen.

- **Was muss eine Organisation erfüllen, um selbst Nachweise auszustellen?**

Eine Organisation muss sich im EUDI-Ökosystem als Aussteller registrieren. Dies beinhaltet neben Registrierungsschritten und der technischen Integration auch die Identifizierung der Organisation. Nach erfolgreicher Registrierung werden die Aussteller in die Vertrauensinfrastruktur aufgenommen, damit vertrauende Parteien sie als berechtigten Herausgeber eines bestimmten Nachweises erkennen können. Danach stellt sie digitale Nachweise nach den europaweit einheitlichen technischen Standards des Architektur- und Referenzrahmens (ARF) und für die verschiedenen Nachweise geltenden Regelwerks ("Rulebook") aus (z. B. definierte Datenformate, Signaturen, Statuslisten).

Frequently Asked Questions

- **Wie werden wiederkehrende Prüfungen automatisiert (z. B. Leistungsansprüche, Qualifikationen, Identität)?**

Die EUDI-Wallet vereinfacht Abfrage und Überprüfung von u.a. Ausweisdaten, Qualifikationen und Leistungsansprüchen, da digitale Nachweise in einem maschinenlesbaren Format vorliegen und die Ende-zu-Ende-Digitalisierung von Prozessen ermöglichen. Gleichzeitig sind Nutzende über die aktive Zustimmung zur Datenfreigabe immer in die über die Wallet ausgeführten Prozesse eingebunden. Es gibt keine Prozesse, die ohne das Zutun der Nutzenden automatisiert im Hintergrund ablaufen.

- **Wie schützt die Wallet besonders sensible Daten?**

Die EUDI-Wallet schützt sensible Daten, indem sie sie ausschließlich lokal und kryptographisch verschlüsselt auf dem Gerät speichert. Die dafür nötigen privaten Schlüssel ("Private Key") liegen in einer hardwaregeschützten Komponente, sodass sie nicht ausgelesen oder kopiert werden können. Der Zugriff auf die Wallet und ihre Funktionen ist zusätzlich durch starke Authentisierung (PIN + Gerätesperre) abgesichert.

Die Wallet gibt nur die von Nutzenden freigegebenen Daten weiter. Entsprechend dem Prinzip der selektiven Offenlegung ("Selective Disclosure") ist es über die Wallet möglich, nur einen bestimmten Teil eines Nachweises zu präsentieren (z.B. "über 18 Jahre alt") ohne dabei weitere personenbezogene Daten (wie das genaue Geburtsdatum) preiszugeben. Dabei prüft die Wallet bei jeder Transaktion automatisch, ob die jeweilige vertrauende Stelle/Relying Party nur die Informationen abfragt, die sie für diesen Anwendungsfall zuvor registriert hat.

Jede vertrauende Stelle, die die Wallet in ihre Prozesse einbinden möchte, muss einen entsprechenden Registrierungsprozess mit einer Identifizierung durchlaufen und in diesem Zuge ihre Anwendungsfälle offenlegen sowie welche Daten sie für diesen Anwendungsfall abfragen will. Nutzende sehen vor jeder Datenfreigabe, wer ihre Daten wofür anfordert, und vertrauende Stellen müssen sich der Wallet gegenüber authentifizieren. So sind die Nutzenden immer im Bilde, mit wem sie ihre Daten teilen. Auf dieser Basis können Nutzende auch rechtliche Schritte gegen vertrauende Parteien einleiten.

Gleichzeitig verhindert die Wallet, dass die Nutzung der Wallet im Sinne einer Profilbildung nachverfolgt werden kann. Die Datenübertragung erfolgt ausschließlich und direkt zwischen der digitalen Brieftasche der Nutzer:in und der Relying Party. Aussteller von digitalen Nachweisen sind nicht automatisch in das Teilen dieser Nachweise eingebunden und erhalten keine Informationen über deren Verwendung. Geht das Gerät verloren, kann die Wallet-Instanz aus der Ferne gesperrt werden, sodass niemand sie weiter nutzen kann.

- **Dürfen Organisationen Kopien digitaler Nachweise speichern oder müssen sie dies sogar?**
Grundsätzlich gilt: Die Wallet liefert nach Freigabe durch die Nutzer:in nur die für einen konkreten Anwendungsfall von einer vertrauenden Stelle/Relying Party registrierten Daten und keine vollständigen Dokumentenkopien.

Ob eine Kopie des digitalen Nachweises (inklusive Signaturen und Metadaten) erforderlich ist, hängt von der rechtlichen Situation ab. In der Regel werden vertrauende Parteien Daten aus den Nachweisen extrahieren, verarbeiten und bei Bedarf auch speichern. Die Wallet selbst schafft keine neuen

Frequently Asked Questions

Speicherpflichten, sondern hilft Einrichtungen eher dabei, weniger Daten verarbeiten zu müssen. Bestehende gesetzliche Pflichten, insbesondere die DSGVO, bleiben jedoch unverändert bestehen.

4. Betreuer:innen und Vollmacht

- **Ich bin rechtliche Betreuerin in einem Betreuungsverein (Vereinsbetreuerin). Kann ein:e Betreuer:in die Daten der betreuten Menschen verwalten? Wie ist das mit Zugangsrechten und Nutzung durch Dritte (Betreuer:in/Bevollmächtigte)?**

Derzeit: Nein. Uns ist die Wichtigkeit dieses Themas jedoch bewusst und wir arbeiten an einer zukünftigen Umsetzung der Stellvertretungsfunktion (z.B. für gesetzliche Betreuer:innen oder Eltern).

- **Können Minderjährige die Wallet nutzen, bzw. wie verhält sich die Berechtigung der Eltern für ihre Kinder?**

Minderjährige können die Wallet nutzen und dort digitale Nachweise speichern und vorzeigen. Je nachdem, ob Jugendliche ab 16 Jahren ein Ausweisdokument mit aktivierter eID-Funktion besitzen, können sie auch die Wallet-Ausweisfunktion der Wallet nutzen.

5. Freiwillige Nutzung und Kosten

- **Inwieweit wird die Nutzung einer digitalen Briefftasche verpflichtend bzw. für bestimmte Zwecke unumgänglich?**

Die Nutzung der EUDI-Wallet bleibt für Nutzende freiwillig und kostenfrei. Die regulatorischen Vorgaben sehen vor, dass Nutzenden alternative Verfahren durch vertrauende Parteien/Relying Parties angeboten werden müssen.

- **Was kosten digitale Nachweise?**

Die Wallet-Funktion selbst ist kostenfrei – also das Speichern, Vorzeigen und Prüfen von Nachweisen. Kosten können dann anfallen, wenn der Inhalt des Nachweises kostenpflichtig ist oder schon heute Gebühren hat (z. B. Eintrittsticket, Führungszeugnis, amtliche Bescheinigung). Die Kosten für die Entwicklung und Einführung der dem EUDI-Ökosystem zugrunde liegenden Infrastruktur (etwa im Bundeshaushalt eingeplante Mittel) werden von der öffentlichen Hand getragen.

6. Backup und Speicherung

- **Kann ich ein Backup meiner Wallet in meiner Cloud erstellen?**

Für Personenidentifizierungsdaten (PID) sind Cloud-Backups aus Sicherheitsgründen nicht vorgesehen. Perspektivisch kann es ein Backup für digitale Nachweise geben, die keine kryptografische Bindung an eine bestimmte Wallet erfordern.

Frequently Asked Questions

7. Probleme: Handy verloren/gestohlen/kaputt oder Akku leer

- **Was ist bei technischen Schwierigkeiten? Smartphone defekt, Akku leer...usw.?**
Kann die Wallet in der Beratung oder im Rettungsdienst auch ohne Internet genutzt werden?
Die PID für die Nutzung der sicheren Wallet-Ausweisfunktion benötigt in der aktuellen Architektur eine Internetverbindung, weil die Prüfung über einen Server-basierten Sicherheitsschlüssel erfolgt. Andere Nachweise können jedoch perspektivisch offline präsentiert werden. Lösungsansätze hierfür werden aktuell erarbeitet.
- **Was passiert mit meinen Daten, wenn ich mein Handy verloren habe?**
Geht das Smartphone verloren, bleiben die in der EUDI-Wallet gespeicherten Nachweise geschützt. Der Zugriff ist über die von der Nutzer:in für die Wallet vergebene PIN und die allgemeine Gerätesperre (d.h. Smartphone-PIN oder Biometrie) abgesichert, sodass Unbefugte nicht auf die Wallet zugreifen können. Die verlorene Wallet-Instanz kann vergleichbar mit einer Kreditkarte widerrufen werden, ist dann aber, anders als im Fall einer gesperrten Kreditkarte, dauerhaft unbrauchbar (keine Wiederherstellung dieser Instanz möglich). Für die Nutzung auf einem neuen Gerät ist also eine Neueinrichtung der Wallet nötig (d.h. erneuter Download der Wallet-App, erneutes Hinzufügen von Nachweisen). So bleibt der Missbrauch ausgeschlossen und persönliche Daten werden auch bei Geräteverlust nicht offengelegt.
- **Was passiert, wenn man den Personalausweis verliert / abgelaufen ist?**
Für die Initialisierung der Wallet-Ausweisfunktion mittels PID ist ein gültiges Ausweisdokument mit aktiver Online-Ausweisfunktion erforderlich. Die ausgestellte PID maximal so lange gültig ist wie das dazugehörige "analoge" Ausweisdokument. Nach Erhalt eines neuen Ausweisdokuments muss die PID entsprechend ebenfalls neu eingerichtet werden.
- **Wie wird verhindert, dass eine gesperrte Wallet benutzt wird?**
Eine gesperrte Wallet kann nicht mehr genutzt werden, da ihr Widerrufsstatus in der Infrastruktur hinterlegt wird und jede Wallet-Interaktion eine Authentizitätsprüfung durchläuft. Zusätzlich können Aussteller von Nachweisen auf der Basis des Status ihrer jeweiligen Nachweisen sperren.

8. Anbindung existierenden Services und Apps

- **Wird die BundID in die EUDI-Wallet eingebunden?**
Die Integration von EUDI-Wallet und BundID ist geplant, auch um Behörden die Anbindung an die EUDI-Wallet zu erleichtern. So soll es möglich sein, dass Identifizierung und Nachweisaustausch mit der Verwaltung im Zusammenspiel von EUDI-Wallet und BundID funktionieren. Die BundID bildet somit zukünftig eine Art Eingangstor zur öffentlichen Verwaltung, welches Nutzende mit der EUDI-Wallet öffnen und passieren können.
- **Wird die ePA in die EUDI-Wallet eingebunden?**
Die ePA und die EUDI-Wallet sind zwei separate Anwendungen. Die ePA ist eine zentrale Gesundheitsakte:

Frequently Asked Questions

Daten liegen in Aktensystemen der Telematikinfrastruktur; Zugriffe werden zentral protokolliert; viele Abläufe laufen über Backend Komponenten im Hintergrund. Die EUDI-Wallet ist dagegen ein dezentraler Nachweis-„Speicher“ auf dem Smartphone: Nutzer:innen steuern jede Freigabe aktiv, präsentieren signierte Nachweise direkt an die vertrauende Stelle, und es gibt keine zentrale Datenspeicherung oder automatische Einbindung und Information von Nachweis-Ausstellern über die Nutzung der Wallet. Es ist zukünftig jedoch vorgesehen, dass die EUDI-Wallet mit der [GesundheitsID](#) integriert wird, letztere kann dann zum Zugang zur ePA verwendet.

- **Wird es Integrationsmöglichkeiten in Standard-Software wie Connect Vivendi oder ähnliche geben können?**

Integrationsmöglichkeiten hängen stark von den entsprechenden Anwendungsfällen und vorliegenden Fachverfahren ab. Das nationale EUDI-Wallet-Projekt stellt Leitfäden für die technische Entwicklung für alle Wallet-Funktionen (sog. „Developer Guides“) zur Verfügung, um die Integration in bestehende Systeme möglichst einfach zu gestalten. Die Integration obliegt den jeweiligen Anbietern.

- **Wie wird die Wallet an IT-Systeme von Organisationen angebunden?**

Die Anbindung erfolgt über einheitliche, EU-weit standardisierte Schnittstellen, die es Organisationen ermöglichen, Wallet-Nachweise sicher anzufordern, entgegenzunehmen und zu prüfen. Damit funktioniert die Integration wie bei einem modernen, interoperablen Login-/Datenfreigabe-System, ohne technische Abhängigkeit von einzelnen Herstellern.

Für detaillierte technische Informationen, Praxisbeispiele und Leitfäden empfiehlt sich folgende Anlaufstelle für alle Fragen rund um das nationale EUDI-Wallet-Ökosystem in Deutschland, das „Ecosystem Knowledge Centre“:

https://bmi.usercontent.opencode.de/eudi-wallet/eidas2/ecosystem_knowledge_centre/

- **Kann die Wallet in bestehende Social-Care-Software integriert werden (Pflege, Migration, Jugendhilfe)?**

Die EUDI-Wallet lässt sich über offene, EU-weit standardisierte Schnittstellen in bestehende Social-Care-Systeme wie Pflege-, Migrations- oder Jugendhilfesoftware einbinden. Die Wallet nutzt interoperable Standards und dokumentierte APIs, sodass digitale Nachweise schnell, rechtssicher und datenschutzkonform geprüft werden können.

Anbieter erhalten technische Leitfäden, Code-Beispiele und Schnittstellenbeschreibungen, und Organisationen können ihre Integration vorab in der EUDI-Wallet Sandbox testen.

9. Barrierefreiheit und Inklusion: Digitale Affinität, Sprache, Armut, marginalisierte Gruppen

- **Viele Menschen besitzen kein Smartphone. Wie kann sichergestellt werden, dass auch wohnungslose und ältere Menschen einen sicheren Umgang erlangen?**

Die EUDI-Wallet wird zur freiwilligen und kostenfreien Nutzung zur Verfügung stehen. Die Möglichkeit der Nutzung von analogen Nachweisen besteht weiterhin. Darüber hinaus arbeiten wir an Informationsangeboten für alle Nutzungsinteressierten.

Frequently Asked Questions

- **Wie wird sichergestellt, dass Menschen, die altersbedingt, gesundheitlich (z. B. Sehbehinderung/Blindheit) oder aufgrund fehlender Schriftsprachkenntnisse die EUDI-Wallet nicht selbstständig nutzen können, weiterhin gleichberechtigten Zugang zu wichtigen Dienstleistungen behalten? Welche konkreten Unterstützungsstrukturen sind geplant, damit diese Gruppen nicht vom digitalen Fortschritt ausgeschlossen werden?**

Die EUDI-Wallet wird transparent und nutzerzentriert entwickelt, um eine inklusive und breite Zugänglichkeit sicherzustellen. Die EUDI-Wallet wird nach BITV 2.0 Richtlinien barrierefrei umgesetzt. Seit Beginn des Projekts findet ein reger und stetiger Austausch mit zivilgesellschaftlichen Organisationen statt, um Anforderungen und Perspektiven bestmöglich in die Entwicklung einzubeziehen. Informationsangebote sind geplant.

- **Wie schützt die EUDI-Wallet besonders gefährdete Gruppen (z. B. Migrant:innen oder religiöse Minderheiten) vor Profilbildung oder Missbrauch?**

Die EUDI-Wallet verhindert gemäß der Prinzipien von "Unlinkability" (Unverknüpfbarkeit) und "Unobservability" (Unbeobachtbarkeit) gezielt Profilbildung und Missbrauch, indem sie personenbezogene Daten ausschließlich lokal und verschlüsselt speichert und keine zentrale Nachverfolgung ermöglicht. Einzelne Nachweise und Transaktionen werden technisch nicht miteinander verknüpft, sodass auch für Migrant:innen oder religiöse Minderheiten keine Nutzungsprofile entstehen können. Ebenfalls gilt im Sinne der Datensparsamkeit das Prinzip der selektiven Offenlegung. Bei der selektiven Offenlegung werden nur die für einen konkreten Zweck angeforderten Informationen freigegeben. Dies ermöglicht es, einen Nachweis zu erbringen (z.B. "über 18 Jahre alt") ohne dabei weitere personenbezogene Daten (wie das genaue Geburtsdatum) preiszugeben.

10. Use Cases

- **Soll perspektivisch auch der "digitale Euro" in die Wallet? Ob der digitale Euro eingebunden werden wird, wird sicherlich einen großen Einfluss auf die Verbreitung der App haben.**

Das ist denkbar. Vorgaben von der europäischen Ebene stehen hier noch weitestgehend aus.

- **Gibt es eine gute Übersicht, welche Use Cases mit der EUDI-Wallet perspektivisch möglich sein könnten? Insbesondere für die freie Wohlfahrt?**

Das Ecosystem Knowledge Centre stellt erste [Use-Case-Sammlungen](#) für Relying Parties bereit, beispielsweise aus dem Bereich Mobilität oder zur Umsetzung von Vergünstigungen (z.B. durch die Wallet-basierte Überprüfung von Studierendenausweisen, Ehrenamtskarten etc.) sowie zur Identifizierung im digitalen und analogen Raum (z.B. zur Zugangskontrolle zu Unternehmensressourcen).

- **Ich habe heute gerade diesen interessanten Anwendungsfall gesehen: [youtube.com/watch?v=SFoU14H9BQE](https://www.youtube.com/watch?v=SFoU14H9BQE) - Bezahlen per Wero und Altersverifikation über Perso in einem Schritt. Aber wie kann man sicherstellen, dass so ein Händler nicht noch mehr Daten verlangt? Ich werde dann ja nicht an der Kasse sagen: "Ach, wenn Sie diese Daten haben wollen, dann kauf ich lieber doch nicht."**

Dienste dürfen nur die für ihren konkreten Anwendungsfall zuvor registrierten Daten anfordern. Vertrauende Stellen müssen zuvor einen entsprechenden Registrierungsprozess durchlaufen und es ist

Frequently Asked Questions

öffentlich einsehbar, welche Daten sie für ihren Anwendungsfall abfragen. Welche Daten abgefragt werden, macht das Wallet den Nutzenden gegenüber vollständig transparent. Die Daten werden nur nach Zustimmung der Nutzenden geteilt.

- **Könnte man mit der Wallet eine Altersbeschränkung für die Nutzung von Social Media technisch umsetzen?**

Eine technische Umsetzbarkeit wäre mit der EUDI-Wallet auf datensparsame Art gegeben, jedoch liegt eine solche Entscheidung auf der Seite des Gesetzgebers.

- **Ich bearbeite Anträge in der Selbsthilfeförderung, in denen zwei legitimierte Vertreter:innen die Anträge nach dem 4-Augen-Prinzip unterschreiben müssen. Bisher leider nur analog möglich und die Anträge müssen im Original per Post an mich als Kassenverband gesendet werden. Gibt es da eine digitale Möglichkeit?**

Über die geplante Signaturfunktion mittels qualifizierter elektronischer Signatur (QES) lassen sich digitale Dokumente rechtskräftig unterzeichnen. Einsatzmöglichkeiten hängen stark von den entsprechenden Anwendungsfällen und aktuellen Verfahren ab.

11. Digitale Nachweise

- **Wenn ich in der Wallet auch mein Erste-Hilfe-Zertifikat, mein Hochschulzeugnis etc. habe und ich mein Smartphone verliere, dann kann es doch nicht wie in der analogen Welt sein, dass ich all das sperre und dann neu beantragen muss? Kann ich davon nicht zumindest Teile in einem Backup speichern und die dann wieder einspielen?**

Für einige Nachweise wird eine erneute Einrichtung erforderlich sein. Gleichzeitig wird man für viele Nachweise ein Backup durchführen können, sodass eine Wiederherstellung entsprechend einfacher möglich ist.

- **Wie speichere und verwalte ich Nachweise, wenn ich sie nicht in der Wallet haben möchte oder haben kann?**

Digitale Nachweise und die Wallet ersetzen nicht automatisch bisherige Verfahren zur Ausstellung von Zertifikaten, Zeugnissen, usw. Vielmehr ist davon auszugehen, dass es zukünftig vermehrt die Option geben wird, sich zu entscheiden, ob man einen Nachweis digital über die Wallet und/oder auf andere Art und Weise aufbewahren und nutzen möchte.

- **Können selten benötigte Dokumente ausgelagert werden? Kann man digitale Nachweise flexibel verwalten?**

Ja. Digitale Nachweise können prinzipiell jederzeit aus der Wallet gelöscht und wieder hinzugefügt werden. Je nach Sicherheitsanforderung eines Nachweises und ob dieser kryptographisch gebunden ist, können Nachweise perspektivisch über ein Backup verwaltet werden.

Frequently Asked Questions

12. Herausforderungen im Beratungskontext

- **Wie ist bei der Digitalisierung von Behördendienstleistungen die Beratungspflicht von Behörden und die Beratung durch Dritte mitgedacht?**

Die Wallet ist eine Anwendung, welche bei der Digitalisierung von behördlichen Prozessen unterstützen kann. Die Umsetzung und Ausgestaltung liegt hierbei beim Verantwortlichen der Behördendienstleistung. Die Wallet ersetzt keine Beratung durch eine Behörde. Es wird auch weiterhin möglich sein, sich in Person oder schriftlich (auch digital) an Behörden zu wenden.

- **Wie können Beratungsstellen sicher unterstützen, ohne fremde Smartphones zu bedienen?**

Beratungsstellen können Klient:innen mit Informations- und Weiterbildungsangeboten unterstützen. Aktuell werden Konzepte und Materialien entwickelt, die Nutzenden den Umgang mit der Wallet erklären sollen. Damit diese Ressourcen für alle Menschen zugänglich und verständlich sind, hat das Projekt frühzeitig damit begonnen, unterschiedliche Zielgruppen zu konsultieren und in die Entwicklung der EUDI-Wallet einzubeziehen. Der Erfolg eines solchen partizipativen Ansatzes hängt von der Beteiligung einer Vielzahl verschiedener Akteur:innen ab. Wir freuen uns, wenn Sie bei Fragen oder Ideen hierzu auf uns zukommen.

- **Wie kann eine Organisation sicherstellen, dass sie bei "falschen" Nachweisen nicht haftet?**

Haftungsfragen werden noch in der nationalen Gesetzgebung geklärt.

13. "Sandbox" und Testen

- **Gibt es Testumgebungen und/oder Pilot-Programme?**

In Deutschland steht mit der "[EUDI-Wallet Sandbox](#)" eine produktionsnahe Testumgebung bereit. Sie ist das zentrale Tor zum deutschen und europäischen EUDI-Ökosystem und ermöglicht Organisationen, realitätsnah zu testen – ausschließlich mit Testdaten. Zum Start unterstützt die Sandbox Anwendungsfälle für die sichere Identifizierung mittels PID.

Die nationale Sandbox ist notwendig, um die technische Integration und Funktionsweise der EUDI-Wallet mit Systemen der Relying Parties zu testen, damit die Lösungen für die Nutzenden möglichst fehlerfrei funktionieren. Die Sandbox ist Teil des Registrierungsprozesses von Relying Parties und wird dauerhaft zur Verfügung stehen.

Deutschland arbeitet zudem mit Hilfe von Prototypen, die im Rahmen eines [von SPRIND organisierten Innovationswettbewerbs](#) entwickelt wurden. Parallel dazu laufen europaweit sog. "Large-Scale-Piloten" wie [APTITUDE](#) und [WE BUILD](#) in denen zentrale Use Cases und Interoperabilität geprüft werden.

- **Braucht es nicht auch Tests in echter Umgebung mit Endnutzer:innen? Gibt es da auch einen Zugang, sowas wie eine Beta?**

Relying-Parties benötigen Testmöglichkeiten um die technische Funktionalität ihrer Systeme und der EUDI-Wallet zu testen. Dies tun sie als Vorstufe in der nationalen Sandbox, bevor sie für Endnutzer:innen erreichbar sind. Notwendige Tests finden hier dauerhaft ohne Echtdaten statt. Tests mit echten

Frequently Asked Questions

Nutzer:innen finden hingegen an mehreren Stellen statt. Zum einen erfolgen im Rahmen der Entwicklung der EUDI-Wallet kontinuierliche Nutzer:innen-Tests mit dem Ziel, die Nutzerakzeptanz und Nutzerfreundlichkeit zu erhöhen. Zum anderen fließt öffentliches Feedback fortlaufend über Konsultations- und Dialogformate in die Ausgestaltung ein.

Darüber hinaus ist im Zuge des Rollouts und der Produktivnahme der EUDI-Wallet eine „Closed Beta“ vorgesehen. Ziel ist es, Systeme und Prozesse unter möglichst realitätsnahen Bedingungen mit einem eingeschränkten Kreis von Endnutzer:innen zu erproben. Die konkreten Details zur Ausgestaltung dieser „Closed Beta“ werden derzeit ausgearbeitet.

- **Muss dann auch jede Behörde den Sandbox-Onboarding Part durchmachen?**

Grundsätzlich muss jede Organisation – und damit auch jede Behörde – den Registrierungsprozess und somit das Sandbox-Onboarding durchlaufen. Die konkrete Ausgestaltung des Registrierungs- und Onboardingprozesses unterscheidet sich jedoch je nach Interaktionsmodell der jeweiligen Behörde, da insbesondere innerhalb der Verwaltung mehrere Integrationsoptionen vorgesehen sind. Zum einen kann eine Behörde – gegebenenfalls mit Unterstützung eines technischen Dienstleisters – die EUDI-Wallet direkt in ihre Fachverfahren und Prozesse integrieren. Zum anderen besteht die Möglichkeit einer indirekten Nutzung über bestehende Verwaltungssysteme, etwa über die BundID oder im Kontext der Registermodernisierung bzw. über NOOTS. Die entsprechenden Details zur konkreten Ausgestaltung werden derzeit erarbeitet.

Weiterführende Einblicke in den Umsetzungsstand geben Unterlagen des IT-Planungsrats von Ende November 2025: <https://www.it-planungsrat.de/beschluss/b-2025-36-it>.

Konkrete Informationen zum aktuellen Registrierungsprozess finden sich hier: https://bmi.usercontent.opencode.de/eudi-wallet/eidas2/ecosystem_knowledge_centre/.

14. Interesse als Multiplikator:innen

- **Wie wird die Bevölkerung über die EUDI-Wallet informiert? Stehen Multiplikator:innen, bspw. auf kommunaler Ebene, zur Verfügung, die zu Infoveranstaltungen eingeladen werden können?**

Um die Bevölkerung auf unterschiedliche Art und Weise anzusprechen, werden aktuell Konzepte für die Öffentlichkeitsarbeit entwickelt bzw. weiterentwickelt. Ein Beispiel dafür sind Kooperationen mit Organisationen wie der BAGFW bei der Umsetzung von Online-Informationsveranstaltungen. Mit diesen wollen wir frühzeitig potenzielle Multiplikator:innen für bestimmte Bereiche und Zielgruppen erreichen. Wir befinden uns mitten in diesem Prozess und freuen uns daher über Ihren Input, beispielsweise wenn Sie uns zu Veranstaltungen einladen möchten oder Ideen für Formate, Ressourcen usw. haben.

15. Wer macht mit?

- **Welche Institutionen sind verpflichtet, eine Nutzung der EUDI-Wallet zu akzeptieren und für welche Zwecke?**

Öffentliche Stellen in allen EU-Ländern sind verpflichtet, die EUDI-Wallet als rechtmäßigen

Frequently Asked Questions

Identitätsnachweis zu akzeptieren, sofern sie für ihre Dienste eine Identifizierung voraussetzen. Außerdem müssen sie die Wallet zur Authentifizierung ihrer Kunden akzeptieren. So zum Beispiel zur Authentifizierung für öffentliche Online-Zugänge (Login).

Private Stellen, welche auf Grundlage von gesetzlichen Vorgaben zur Identifizierung ihrer Kunden verpflichtet sind (z.B. Banken, Mobilfunkanbieter), müssen die EUDI-Wallet als Identitätsnachweis akzeptieren. Ein Beispiel ist das Geldwäschegesetz (GWG)-konforme Eröffnen eines Bankkontos.

Es gibt ein Diskriminierungsverbot zwischen offiziellen, zertifizierten EUDI-Wallets: Vertrauende Stellen ("Relying Parties") müssen (sobald sie gesetzlich verpflichtet sind EUDI-Wallets zu akzeptieren oder sobald sie generell das Nachweisen aus der Wallet ermöglichen) Nachweise aus jeder anerkannten EUDI-Wallet akzeptieren.

16. Unsere Position und Antworten auf journalistische Artikel

- **Wie wird mit den Erfahrungen zur eID umgegangen, bei dem ein Betrugsanteil sicher vermutet wird?**
<https://www.sueddeutsche.de/wirtschaft/eid-ausweis-sicherheit-kriminalitaet-li.3352907>
Wir nehmen Hinweise auf Missbrauch sehr ernst und leiten daraus konkrete Schutzmaßnahmen ab. Der in der Vergangenheit diskutierte Betrug bezog sich auf die eID-Karte für EU/EEA-Bürger:innen („Unionsbürgerkarte“) und Herausforderungen bei der Ausgabe dieses spezifischen Dokuments über die jeweils zuständigen Meldebehörden – dieses Dokument wird in der ersten Ausbaustufe der EUDI-Wallet in Deutschland nicht unterstützt. Personen aus anderen EU-Mitgliedstaaten werden in Zukunft die Möglichkeit haben, mit der EUDI-Wallet einen Identitätsnachweis aus ihrem Herkunfts- bzw. Aufenthaltsland zu erbringen.
- **Wie sieht Ihr Standpunkt zu der von [Netzpolitik.org](https://netzpolitik.org) geäußerten Kritik an der EUDI-Wallet aus?**
<https://netzpolitik.org/2025/digitale-brieftasche-auf-einem-aehnlich-ungen-unguten-weg-wie-die-elektronische-patientenakte/>
Wir setzen uns mit Kritik an der EUDI-Wallet offen und transparent auseinander, zum Beispiel im Rahmen von Online-Konsultationen oder anderen Formaten. Hinsichtlich des Beitrags von [Netzpolitik.org](https://netzpolitik.org) möchten wir klarstellen, dass die Wallet strikt nach den europäischen Sicherheits- und Datenschutzvorgaben der novellierten eIDAS-Verordnung und des EU-Architekturrahmens entwickelt wird, die auf Prinzipien wie Datensparsamkeit, "Unlinkability" (Unverknüpfbarkeit) und "Unobservability" (Unbeobachtbarkeit) beruhen sowie ein mehrstufiges Registrierungsverfahren für diejenigen vertrauenden Stellen (sog. Relying Parties) vorsieht, die in der Wallet gespeicherte Nachweise in ihre Prozesse einbinden und entsprechend Daten abfragen wollen. Deutschland setzt auf einen transparenten, schrittweisen Ansatz mit offener Dokumentation, öffentlichen Konsultationen und einer offiziellen Sandbox, um Sicherheit, Praxistauglichkeit und den Schutz von Nutzenden sicherzustellen (weitere Details zur Entscheidung signierte Daten vs. authentifizierter Kanal in der nächsten Frage). Die Sicherheit der Lösung wird durch die Zusammenarbeit mit dem BSI sichergestellt. Zum Datenschutz ist das Projekt in regelmäßigem Austausch mit dem BfDI.

Die Architektur der staatlichen Wallet ist insbesondere darauf optimiert worden, dass keine Stelle die Nutzung des Wallets beobachten kann. Jede Nutzung wird ausschließlich zwischen der Wallet-App auf dem Smartphone der Nutzer:in und der vertrauenden Stelle/Relying Party abgewickelt. Selbst bei der

Frequently Asked Questions

hochsicheren Wallet-Ausweisfunktion, bei der aus Sicherheitsgründen ein Server mit einem Hardware-Sicherheitsmodul verwendet wird, kann nicht verfolgt werden, welcher Nutzer/welche Nutzerin welche Daten mit welcher Partei austauscht. Das System ist dabei auf höchstem Niveau gegen Identitätsdiebstahl abgesichert. Die Basis dafür sind Signaturen, so wie Signaturen auch das Rückgrat der Sicherheit des Internets sind. In Bezug auf einen Missbrauch von (signierten) Daten gelten die gesetzlichen Regeln, z.B. der DSGVO. Und durch die durchgängige Identifizierung und Authentifizierung von vertrauenden Stellen und die öffentliche Deklaration der beabsichtigten Verwendung von Daten aus der Wallet hat das Ökosystem einen hohen Grad an Transparenz und Mechanismen, um ggf. rechtliche Schritte einleiten zu können.

- **Warum setzt die EUDI-Wallet auf signierte Daten statt auf einen authentifizierten Kanal?**
Signierte Nachweise erlauben es, die Echtheit und Unverändertheit direkt beim Empfänger zu prüfen, ohne Beteiligung des Ausstellers des jeweiligen Nachweises – ein Schutz hinsichtlich der in der öffentlichen Debatte teilweise unter dem Stichwort „Phone Home-Funktion“ diskutierten Sorge, Aussteller von Nachweisen könnten immer automatisch in die Nutzung der von ihnen bereitgestellten Nachweise eingebunden sein/benachrichtigt werden, wenn eine Überprüfung der von ihnen ausgestellten Nachweise erfolgt. Die Verwendung signierter Daten schützt die Privatsphäre (keine zentrale Nachverfolgung), erhöht Robustheit (auch offline in sog. „Proximity“-Szenarien möglich) und schafft EU-weite Interoperabilität gemäß eIDAS 2.0/ARF. Die Entscheidungsfindung zum Thema signierte Daten vs. authentifizierter Kanal kann sowohl beim [Positionspapier von SPRIND GmbH](#) als auch [auf OpenCoDE](#) nachverfolgt werden.