



Informationen für IT-Dienstleister – Stand: 06.10.2026. Version 1.0 (erste Fassung)

EUDI-Wallet: Anbindung in der Praxis

Optionen, Verfügbarkeiten und Entscheidungskriterien

Über diese Orientierungshilfe

Dieses Dokument dient als eine kompakte Orientierungshilfe zur Anbindung der öffentlichen Verwaltung an die staatliche EUDI-Wallet „d-you“. Sie ergänzt den Handlungsleitfaden und ersetzt ihn nicht.

Die Orientierungshilfe richtet sich an kommunale IT-Dienstleister, Portalbetreiber und Fachverfahrenshersteller, die Kommunen bei der Anbindung beraten und die technische Umsetzung verantworten.

Das Dokument beschreibt die verfügbaren Anbindungsoptionen, ihren jeweiligen Reifegrad und die Kriterien, anhand derer eine Entscheidung vorbereitet und getroffen werden kann. Vertiefende technische Detailinformationen finden Sie im Handlungsleitfaden.

Es handelt sich um eine erste Fassung, die fortlaufend aktualisiert wird. Die jeweils aktuelle Version finden Sie auf digitale-verwaltung.de.

Ab dem 02. Januar 2027 steht die staatliche EUDI-Wallet „d-you“ bereit. Für IT-Dienstleister stellt sich damit eine konkrete Frage: Welcher Anbindungsweg ist für die von uns betreuten Kommunen und ihre jeweiligen Fachverfahren der richtige – und was ist davon heute schon umsetzbar?

Was die Anbindung technisch umfasst

Die Anbindung der öffentlichen Verwaltung an d-you ist keine einzelne Maßnahme, sondern orientiert sich an den drei Funktionalitäten der staatlichen EUDI-Wallet, die unabhängig voneinander betrachtet und bewertet werden sollten.

- **Funktionalität 1** – Identifizierung und Authentifizierung: Nutzende weisen sich gegenüber einem Onlinedienst mit der EUDI-Wallet aus. Grundlage dafür ist der sogenannte Digitale Ausweis (Personenidentifizierungsdaten, kurz PID). Verpflichtend ab dem 02. Januar 2027, sofern das digitale Verwaltungungsverfahren eine Identifizierung oder Authentifizierung vorsieht.
- **Funktionalität 2** – Ausstellung von Nachweisen: Eine öffentliche Stelle stellt einen elektronisch gesiegelten Nachweis (EAA – Electronic Attestation of Attributes) in die EUDI-Wallet aus. Für Bundesbehörden sollen die Ausstellung von Nachweisen (Funktionalität 3) nach einer Übergangsfrist verpflichtend werden. Der Entwurf des Digitale-Identitäten-Gesetzes (DIdG) sieht dafür 24 Monate nach Inkrafttreten vor; die konkrete Frist wird derzeit noch parlamentarisch beraten. Für Länder und Kommunen bleiben beide Funktionalitäten freiwillig.
- **Funktionalität 3** – Entgegennahme von Nachweisen: Ein Onlinedienst oder Fachverfahren nimmt einen vorgelegten Nachweis entgegen und prüft ihn kryptografisch und fachlich. Das betrifft nicht nur Onlineverfahren: Auch vor Ort, etwa im Bürgerbüro, können Nachweise aus der EUDI-Wallet entgegengenommen und geprüft werden – dafür steht die mobile Verifizierungsanwendung EUDI Check DE zur Verfügung. Freiwillig, sicher ohne die Daten weiterzuverarbeiten und mit dem höchsten Automatisierungspotenzial.

Welche dieser oben genannten Funktionalitäten in einem Verfahren genutzt werden sollen, entscheidet maßgeblich über den Anbindungsweg. Zum Start von d-you am 02. Januar 2027 stehen

vielfältige Nachweise aus Wirtschaft und Verwaltung zur Verfügung, darunter z. B. der digitale Führerschein, der Sozialpass oder die Rentenbescheinigung.

Welche Nachweistypen zu einem bestimmten Zeitpunkt tatsächlich spezifiziert und verfügbar sind, ist jederzeit live über das [Ecosystem Knowledge Center](#) in der [Use-Case-Sammlung](#) abrufbar.

Der folgende Abschnitt beschreibt die Optionen zur Anbindung an die EUDI-Wallet. Die Zuordnung von Funktionalität zu Anbindungsweg finden Sie am Ende des Abschnitts.

Die Anbindungsoptionen

A – Direkte Anbindung an die EUDI-Wallet (mit oder ohne Wallet-Adapter, mit oder ohne ZAP)

Onlinedienste und Fachverfahren werden unmittelbar an das EUDI-Wallet-Ökosystem angebunden, ohne zwischengeschaltete Plattform. Optional kann ein Wallet-Adapter als technische Vermittlungskomponente eingesetzt werden (z.B. von Governikus). Er abstrahiert unterschiedliche Nachweisformate und stellt standardisierte Schnittstellen für die Entgegennahme und Ausstellung von Nachweisen bereit; technische Prüfungen auf Gültigkeit und Echtheit der Nachweise, Siegel und Zertifikate laufen darüber. Ohne Wallet-Adapter steigt die technische Komplexität deutlich, insbesondere bei Schnittstellen, Zertifikats- und Schlüsselmanagement sowie Sicherheitsanforderungen. Eine weitere direkte Anbindungsoption ist die zentral bereitgestellte, bundesweit nachnutzbare Infrastruktur des Bundes für die Ausstellung und Prüfung von EUDI-Wallet Nachweisen (ZAP). Der ZAP befindet sich derzeit noch in Entwicklung, die produktive Nutzung ist Stand heute ab April 2027 geplant. Mit ZAP können Fachverfahren Wallet-basierte Nachweise in ihre Verwaltungsprozesse einbinden, ohne eigene Austell- oder Prüfinfrastrukturen aufzubauen oder zu betreiben. Möglich macht dies ein zentral bereitgestellter, schnittstellenbasierter Dienst, der von mehreren Behörden gemeinsam genutzt werden kann.

B.1 – Zentrale Anbindung über Basiskomponenten des Bundes (indirekt)

Die Nutzung erfolgt über bestehende Infrastrukturkomponenten des Bundes, im Fokus steht die BundID (inklusive Zentralem Bürgerpostfach, ZBP). Zum Start der EUDI-Wallet wird die BundID die staatliche EUDI-Wallet als ergänzendes Identifizierungs- und Authentifizierungsmittel akzeptieren. Für die Nachweisausstellung über das Zentrale Bürgerpostfach wird die BundID derzeit technisch erweitert, um die dafür nötigen fachlichen, organisatorischen und technischen Voraussetzungen zu erfüllen.

B.2 – Zentrale Anbindung über föderale Infrastrukturen (indirekt)

Die Anbindung kann über Landesportale, kommunale Plattformen oder bestehende föderale Infrastrukturen wie ServiceBW erfolgen. Vorteil ist die einheitliche Umsetzung über mehrere Verwaltungen hinweg und die Reduktion individueller Umsetzungsaufwände – besonders relevant für kommunale IT-Dienstleister und Plattformbetreiber.

Wichtig: Stellt das jeweilige Bundesland ein Angebot zur Anbindung bereit, sollte dieses vorrangig geprüft und berücksichtigt werden, bevor eine eigene Lösung aufgebaut wird. Welche Angebote das im Einzelnen sind, unterscheidet sich je nach Land; bitte klären Sie das direkt mit der zuständigen Stelle Ihres Landes.

C – Sonderfall: Registerbasierte Ausstellung über NOOTS

NOOTS ist kein eigenständiger Anbindungsweg für alle drei Funktionalitäten, sondern ein Sonderfall ausschließlich für die Ausstellung von Nachweisen (Funktionalität 2). Nachweise werden dabei aus

den über NOOTS angebundenen Registern in einem EUDI-Wallet-konformen Format erzeugt. Voraussetzung ist, dass das jeweilige Register bereits über NOOTS angeschlossen ist und die Daten strukturiert vorliegen. Dieser Weg eignet sich insbesondere für standardisierte Registereuskünfte.

D – Hybride Anbindungsmodelle

In der Praxis kann kombiniert werden: Identifizierung und Authentifizierung über die BundID, rechtssichere Bescheidzustellung über das Zentrale Bürgerpostfach (ZBP) und direkte Anbindung für die digitale Nachweisprüfung. Das erlaubt einen schrittweisen Einstieg entlang der eigenen Digitalisierungsplanung.

Geplante Infrastrukturkomponenten

Die folgenden Komponenten sind angekündigt, stehen aber nicht zum Start zur Verfügung. Sie sollten in Ihrer Planung derzeit nicht als gesetzt vorausgesetzt werden:

- Zentraler Ausstell- und Prüfdienst (ZAP): bundesweit nachnutzbarer, mandantenfähiger Dienst zur Ausstellung und Prüfung von Nachweisen. Geplante Produktionsbereitschaft Januar 2027, produktive Nutzung ab April 2027 geplant.
- Registerbasierte Ausstellung über NOOTS, unterstützt durch einen zentralen Issuing-Dienst (ZID): setzt voraus, dass das jeweilige Register bereits über NOOTS angeschlossen ist. Geplante Produktionsbereitschaft Januar 2027, produktive Nutzung ab April 2027 vorgesehen – abhängig vom Fortschritt der Registeranbindung und der Verfügbarkeit der NOOTS-Infrastruktur.
- Single-Point-of-Verification (SPoV): Verifikationsmechanismus für qualifizierte Vertrauensdiensteanbieter, mit dem Attributwerte auf Verlangen Nutzender gegenüber authentischen Quellen fachlich verifiziert werden können (Art. 45e eIDAS-VO). In Entwicklung; steht zum Go-Live der EUDI-Wallet nicht bereit.

Auf einen Blick: Welche Option deckt welche Funktionalität ab?

- Funktionalität 1 (Identifizierung und Authentifizierung): über alle Wege möglich (Hinweis: bei NOOTS nur in Kombination mit dem Nachweisabruf). Die indirekte Anbindung über die BundID reicht aus, um die rechtliche Verpflichtung nach der eIDAS-Verordnung zu erfüllen. Wer bereits an die BundID angebunden ist und die Authentifizierungsmittel nicht eingeschränkt hat, muss nichts weiter tun. Weitere Informationen dazu finden Sie im [BundID Self-Service-Portal \(SSP\)](#).
- Funktionalität 2 (Ausstellung von Nachweisen): über alle Wege möglich. Hinweis: Zum Start am 02. Januar 2027 wird über das Zentrale Bürgerpostfach der BundID zunächst nur der Anwendungsfall Dresden-Pass der Landeshauptstadt Dresden unterstützt. Die Ausstellung anderer Nachweise über das Zentrale Bürgerpostfach soll ab Q2 2027 unterstützt werden.
- Funktionalität 3 (Entgegennahme von Nachweisen): nach aktueller Planung nur über die direkte Anbindung, da die BundID die Entgegennahme von anderen Nachweisen als der PID (Personenidentifizierungsdaten) zum Start im Januar 2027 nicht abdeckt.

Die Optionen im Vergleich

Dimension	Zentral über BundID (indirekt)	Direkt mit Wallet-Adapter	Direkt ohne Wallet-Adapter
Integrationsaufwand	gering für Funktionalität 1 – u. a. durch Nachnutzung bestehender Schnittstellen, bei Funktionalitäten 2 und 3 mittlerer Aufwand	mittel – Zusatzkomponente, Wallet-Adapter-Anbindung und Datenanpassungen	hoch – neue Schnittstellen, Validierung, Sicherheitsmechanismen, Zertifikats-Handling
Betrieb und Wartung	weitgehend zentral getragen	Wallet-Adapter im Eigenbetrieb (On-Premise) oder als Software-as-a-Service möglich, Monitoring und Absicherung erforderlich	vollständig bei der anbietenden Stelle: Monitoring, Updates, Audits
Fachliche Flexibilität	begrenzt – BundID gibt Prozesse und Roadmap vor	hoch – der Wallet-Adapter kann auf Basis der Anforderungen der Fachprozesse und Onlinedienste konfiguriert werden	am höchsten – präzise Anpassungen möglich
Funktionsabdeckung	Identifizierung/Authentifizierung; Nachweisausstellung über ZBP in Entwicklung; Entgegennahme von Nachweisen zum Start der EUDI-Wallet am 02. Januar 2027 nicht vorgesehen	alle drei Funktionalitäten	alle drei Funktionalitäten
Nutzendenfreundlichkeit	Systemwechsel und BundID-Konto erforderlich	weniger Systemwechsel	weniger zusätzliche Systemwechsel
Organisatorische Last	gering – zentrale Relying-Party-Rolle, keine Einzelregistrierung im EUDI-Wallet-Ökosystem vorgesehen	mittel – Governance zwischen Wallet-Adapter-Betreiber und Fachressorts erforderlich	hoch – eigene Registrierung als Relying Party, Zertifikatsmanagement, ggf. Konformitätsbewertung (nur für QEAA- und PubEAA-Provider vorgeschrieben)
Abhängigkeiten	Release Zyklen und Priorisierung der BundID; die BundID kann zum	Abhängigkeit vom Wallet-Adapter-Betreiber; ein zentral betriebener Wallet-	keine Intermediäre, dafür volle Eigenverantwortung



Dimension	Zentral über BundID (indirekt)	Direkt mit Wallet-Adapter	Direkt ohne Wallet-Adapter
	Single Point of Failure werden	Adapter kann zum Single Point of Failure werden	
Typisch geeignet für	Kommunen mit begrenzten Ressourcen und kurzfristigem Umsetzungsbedarf	IT-Dienstleister von EfA-Diensten, bundesweit nachgenutzten Verfahren oder digitale Vorreiter und Pilotvorhaben	technisch erfahrene Organisationen mit eigener Wallet-Expertise

Reifegrad und Verfügbarkeit der Komponenten

Nicht alle Komponenten stehen zum Start zur Verfügung. Die folgende Übersicht benennt offene Zeitpunkte ausdrücklich, damit sich einschätzen lässt, ob das Warten auf eine kommende Komponente individuell sinnvoll ist.

Komponente	Zweck	Stand	Konsequenz für die Planung
EUDI-Wallet-Sandbox	Offizielle Testumgebung für die staatliche EUDI-Wallet zur Erprobung von Digitalem Ausweis (PID)- und Nachweisfunktion	verfügbar seit Dezember 2025	Anwendungsfälle können heute eingereicht und erprobt werden; Teilnahme ist Voraussetzung für den späteren Produktivbetrieb bei eigener Direktanbindung
Staatliche EUDI-Wallet „d-you“	Bereitstellung durch den Bund	Bereitstellung ab 02. Januar 2027	Dieses Datum ist der Referenzzeitpunkt für alle Umsetzungsplanungen
BundID: Identifizierung und Authentifizierung	Identifizierung/Authentifizierung von natürlichen Personen für alle an die BundID angebundenen Dienste	Umsetzung zum Start ab 02. Januar 2027 vorgesehen	tragfähigster Weg, um die ab dem 02. Januar 2027 geltende Akzeptanzpflicht fristgerecht zu erfüllen
BundID / ZBP: Nachweise ausstellen	Ausstellung von Nachweisen über das Zentrale Bürgerpostfach	zum Start zunächst für den Pilotanwendungsfall Dresden-Pass der Landeshauptstadt Dresden	schrittweise Öffnung für weitere fachlich zuständige Stellen ab ca. Q2 2027 angekündigt
Wallet-Adapter (z. B. von Governikus)	Vermittlungskomponente; standardisierte Schnittstellen für	ab 02. Januar 2027 als Produkt des IT-Planungsrats (entwickelt von	auch andere marktverfügbare Wallet-Adapter sind grundsätzlich zulässig, sofern sie die

Komponente	Zweck	Stand	Konsequenz für die Planung
	Entgegennahme und Ausstellung von Nachweisen	Governikus) vorgesehen (On-Premise oder Software-as-a-Service)	Anforderungen des EUDI-Wallet-Ökosystems erfüllen
Zentraler Ausstell- und Prüfdienst (ZAP)	bundesweit nachnutzbarer, mandantenfähiger Dienst zur Ausstellung und Prüfung von Nachweisen	geplante Produktionsbereitschaft Januar 2027, produktive Nutzung ab April 2027 geplant	nicht als gesetzt einplanen; Alternativweg vorsehen
NOOTS-spezifischer Zentraler Issuing Dienst (ZID)	registerbasierte Ausstellung von Nachweisen	geplante Produktionsbereitschaft Januar 2027, produktive Nutzung ab April 2027 geplant.	zusätzlich abhängig vom Fortschritt der Registeranbindung
EUDI Check DE	mobile Verifizierungsanwendung zur Vor-Ort-Prüfung von digitalen Nachweisen	Zeitpunkt der geplanten Produktionsbereitschaft offen, nur über Apple App Store und Google Play Store; Voraussetzung ist die Registrierung als Wallet Relying Party im EUDI Hub DE	Keine Weiterverarbeitung der Nachweisdaten im Fachverfahren möglich; Prüfgeräte mit Update-Versorgung und Secure Element erforderlich – Beschaffung einplanen

Für die verpflichtende Akzeptanz der EUDI-Wallet als Identifizierungsmittel in Onlineverfahren, die eine Identifizierung oder Authentifizierung voraussetzen, steht mit der BundID ein belastbarer Weg zur Verfügung; hier ist Abwarten nicht sinnvoll. Bei den freiwilligen Funktionalitäten kann es dagegen sinnvoll sein, den Aufbau zentraler Komponenten abzuwarten – vorausgesetzt, die fachliche Vorbereitung in der jeweiligen Kommune läuft parallel weiter. Dazu gehört, die betroffenen Verfahren zu identifizieren, die benötigten Nachweise fachlich zu definieren, die Datenqualität zu prüfen und die Zuständigkeiten zwischen Kommune, Fachverfahrenshersteller und IT-Dienstleister zu klären.

Entscheidungskriterien zur Bestimmung der passenden Anbindungsoption

Der Bund empfiehlt öffentlichen Stellen, die Verwaltungsanbindung an die EUDI-Wallet in einem ersten Schritt auf die Identifizierung und Authentifizierung auszurichten. Gleichzeitig sollte die spätere Nachweisausstellung bereits bei der Auswahl der Anbindungsoption berücksichtigt werden; für registerbasierte Nachweise wird empfohlen, perspektivisch eine Bereitstellung über NOOTS anzustreben und entsprechende Registeranbindungen voranzutreiben. Die Auswahl der konkreten Anbindungsoption bleibt dabei eine individuelle Entscheidung der jeweiligen öffentlichen Stelle und sollte sich an den jeweiligen fachlichen und technischen Anforderungen orientieren.

Der IT-Planungsrat hat die Direktanbindung als langfristiges Zielbild empfohlen (siehe Kapitel 3.2 im [Konzept des IT-Planungsrats](#) vom Juni 2026). Für die Entscheidung im Einzelfall sind vor allem folgende Punkte maßgeblich:

- **Bestehende Vorgaben:** Gibt es eine Landesstrategie, eine festgelegte Zielarchitektur oder eine Standardlösung? Diese gehen einer eigenen Bewertung vor.
- **Vorhandene Infrastruktur:** Besteht eine BundID-Anbindung? Werden Landesportale oder föderale Plattformen genutzt? Sind Register angebunden oder ist eine NOOTS-Anbindung geplant?
- **Benötigte Funktionalitäten:** Reicht Identifizierung/Authentifizierung, oder sollen Nachweise ausgestellt oder entgegengenommen werden?
- **Digitaler Reifegrad des Verfahrens:** Handelt es sich um ein digital reifes Verfahren mit hohem Automatisierungs- oder Nachnutzungspotenzial, etwa einen EfA-Dienst?
- **Ressourcen und Kompetenzen:** Sind Architektur-, Schnittstellen- und Sicherheitskompetenzen sowie Betriebsressourcen dauerhaft verfügbar?
- **Bescheidzustellung:** Wird zusätzlich eine rechtssichere Bescheidzustellung benötigt? Dann ist der Weg über BundID und Zentralem Bürgerpostfach vorrangig zu prüfen, da aktuell nur das Zentrale Bürgerpostfach eine rechtssichere Bescheidzustellung ermöglicht.

Welche Verfahren fachlich Vorrang haben, entscheiden die fachlich Verantwortlichen in der jeweiligen Kommune. Ihre Aufgabe als IT-Dienstleister ist es, für die priorisierten Verfahren gemeinsam mit den fachlichen Verantwortlichen den passenden Anbindungsweg vorzuschlagen und umzusetzen.

Hinweis für EfA-Dienste

Für Onlinedienste, die nach dem Einer-für-Alle-Prinzip (EfA) bundesweit nachgenutzt werden, ist die direkte Anbindung besonders wirtschaftlich: Identifizierungs-, Präsentations- und Verifikationsflüsse werden einmalig implementiert und anschließend bundesweit nachgenutzt.

Was die anbindende Stelle leisten muss

Anbindungsweg	Anforderungen
Indirekt über die BundID	• Anbindung an die BundID herstellen oder aktualisieren • Konfiguration der SAML-Schnittstelle prüfen: Die EUDI-Wallet muss als zulässiges Identifizierungs- und Authentifizierungsmittel ergänzt werden, sofern die Authentifizierungsmittel eingeschränkt wurden • Umgang mit Gastzugängen und mit abweichenden Identitätsattributen fachlich bewerten • keine eigene Registrierung als Relying Party erforderlich – die BundID übernimmt diese Rolle zentral
Indirekt über föderale Infrastrukturen	• Anbindung an die jeweilige Plattform herstellen oder aktualisieren • Anforderungen, Registrierungsverfahren und Rollenverteilung beim Betreiber der Plattform erfragen – diese sind je nach Land und Lösung unterschiedlich

Anbindungsweg	Anforderungen
	• Klären, welche der drei Funktionalitäten die Plattform abdeckt
Direkt, mit oder ohne Wallet-Adapter	• Registrierung als Relying Party im EUDI-Wallet-Ökosystem und Erklärung der beabsichtigten Nutzung • Zertifikats- und Schlüsselmanagement einrichten und betreiben • Testanbindung in der EUDI-Wallet-Sandbox durchlaufen, danach Wechsel in den Produktivbetrieb • Monitoring, Wartung, Support und regulatorische Anpassungen dauerhaft sicherstellen • Konformitätsbewertung nur, sofern als QEAA- oder PubEAA-Provider ausgestellt werden soll

Unabhängig vom Anbindungsweg: Vorbereitung der Nachweisausstellung

Sollen Nachweise ausgestellt werden, fallen unabhängig von der gewählten Anbindungsoption dieselben fachlichen Vorarbeiten an. Sie liegen bei der fachlich zuständigen Stelle, nicht beim IT-Dienstleister allein:

- (AuthentischeQuelle bestimmen: Welches System oder welche Organisation ist die fachlich maßgebliche und rechtlich verantwortete Datenquelle, etwa ein Melde-, Führerschein- oder Fachverfahrensregister?
- Rechtliche Grundlage prüfen: Ist die digitale Ausstellung zulässig, oder besteht Anpassungsbedarf?
- Strukturierte Daten bereitstellen: Der Nachweis wird als Satz einzelner Attribute übermittelt. Unstrukturierte Daten, etwa PDF-Dokumente, müssen dafür in ein maschinenlesbares Format überführt werden.
- Nachweischema, Rulebook und Lebenszyklusregeln definieren – oder ein vorhandenes Schema nachnutzen.
- Attributsatz auf das fachlich erforderliche Minimum begrenzen.

Nachweise vor Ort prüfen: Cross-Device-Flow und EUDI Check DE

Die bisherigen Abschnitte gehen vom Same-Device-Flow aus: Nutzende rufen einen Onlinedienst auf demselben Smartphone auf, auf dem auch die EUDI-Wallet liegt. Für Servicestellen ist das wenig praktikabel. Für die Vorlage von Nachweisen vor Ort stehen deshalb zwei Wege zur Verfügung.

Cross-Device-Flow über den Wallet-Adapter

Der Verwaltungsakt wird als Onlinedienst realisiert, den Mitarbeitende am PC oder Tablet aufrufen. Wird ein Nachweis benötigt, zeigt der Wallet-Adapter einen QR-Code an, den die Nutzenden mit ihrem Smartphone scannen. Nach der Freigabe fließen die Daten über den Wallet-Adapter in den aufrufenden Onlinedienst und können dort weiterverarbeitet werden. Die Ausstellung von Nachweisen funktioniert analog.



Weil die Nutzenden dabei durch die Mitarbeitenden der Servicestelle beaufsichtigt werden, ist sichergestellt, dass für Identifizierung, Präsentation und Empfang dasselbe Gerät und dieselbe EUDI-Wallet verwendet werden. Für einen rein online durchgeführten Cross-Device-Flow ist das derzeit technisch noch nicht abschließend gelöst.

EUDI Check DE

EUDI Check DE ist die Verifier-App des EUDI-Wallet-Ökosystems zur Prüfung von Nachweisen, die vor Ort aus einer deutschen EUDI-Wallet präsentiert werden. Sie wird im Auftrag des Bundes von der Common Codes GmbH entwickelt. Die geplante Produktionsbereitschaft ist bisher offen, die Verifier-App wird aber kostenfrei und quelloffen zur Verfügung gestellt. Die Prüfung erfolgt vollständig in physischer Nähe zwischen Prüfgerät und Gerät der Nutzenden (Proximity); Nachweisdaten werden ausschließlich lokal geprüft. Es gibt keinen Export und keine Schnittstelle, über die Ergebnisse in die behördlichen Systeme oder Fachverfahren übernommen werden. Es gibt weiterhin keine Prüfprotokolle in Form zentral erfasster Prüfvorgänge und keine digitalen Prüfbelege. Die App ist offline-first ausgelegt: Vertrauenslisten und Widerrufsinformationen werden vorab synchronisiert. Fehlt eine Vertrauensliste, wird das Ergebnis nach einem definierten Ampelmodell abgestuft dargestellt, statt den Vorgang abubrechen.

Aspekt	Was Sie einplanen müssen
Bezug der Anwendung	Ausschließlich über Apple App Store und Google Play Store. Eine Bereitstellung über behördeneigene Verteilkanäle ist nicht vorgesehen. Stellen, deren Geräte den Zugriff auf die öffentlichen Stores einschränken, müssen das berücksichtigen.
Anforderungen an das Prüfgerät	Derselbe Gerätekreis wie bei der EUDI-Wallet: Smartphone mit laufender Update-Versorgung und hardwaregestützter Schlüsselspeicherung über Secure Element oder vergleichbare TEE. Altgeräte ohne Update-Versorgung oder Hardwareabsicherung sind nicht nutzbar – bei der Gerätebeschaffung einplanen.
Einrichtung	Die Organisation legt ihr Konto im EUDI Hub an und registriert sich als Wallet Relying Party. Beim ersten Login werden die benötigten Anwendungsfälle aus der Liste des Hub ausgewählt; Zugriffs- und Registrierungszertifikate werden automatisch bezogen und auf dem Gerät eingerichtet. Private Schlüssel werden lokal erzeugt und verlassen das Gerät nicht. Manuelles Zertifikatsmanagement, eigener IT-Betrieb, Serverkomponente oder Fachverfahrensanbindung sind nicht erforderlich.
Keine zentrale Geräteverwaltung	Kein Mobile Device Management, kein Massen-Onboarding, keine vorkonfigurierte Auslieferung von Geräteflotten. Jedes Gerät wird einzeln eingerichtet. Je Installation ein Organisationskonto, je Prüfvorgang ein Anwendungsfall (Intended Use). Bei vielen Prüfgeräten den Einrichtungsaufwand je Gerät einplanen.
Anzeige des Ergebnisses	Das Prüfergebnis wird unmittelbar angezeigt, zusammen mit den für den registrierten Anwendungsfall angefragten Attributen. Der Umfang richtet sich nach dem Verwendungszweck – bei einer reinen Altersprüfung etwa nur das entsprechende Prädikat.

Aspekt	Was Sie einplanen müssen
Keine Weiterverarbeitung	EUDI Check DE speichert keine Nachweis- oder Identitätsdaten und führt kein Prüfprotokoll. Es gibt keine Schnittstelle, um ein Ergebnis oder Attribut an ein anderes System zu übergeben – weder Rückruf noch Export noch API. Screenshots sind unterbunden.

EUDI-Wallet-Sandbox: heute schon testen

Die EUDI-Wallet-Sandbox ist die offizielle deutsche Testumgebung. Sie steht öffentlichen wie privaten Organisationen offen und ermöglicht es, Anwendungsfälle ausschließlich mit Testdaten zu erproben. Unterstützt werden die Identifizierungs- und Authentifizierungsfunktion über den Digitalen Ausweis (Personenidentifizierungsdaten, kurz PID) sowie Nachweisausstellung und -entgegennahme (zum Start nur EAAs).

Der Weg in die EUDI-Wallet-Sandbox

1. Onboarding-Anforderungen prüfen und die Sandbox-Readiness-Checkliste nutzen (bmi.usercontent.opencode.de/eudi-wallet/developer-guide/sandbox/onboarding/sandbox_readiness_checklist/)
2. Eigenen Anwendungsfall definieren und zur Prüfung einreichen
3. Onboarding-Schritte durchlaufen, einschließlich Kick-off mit dem Projektteam
4. Technische Anbindung aufsetzen und Abruf sowie Verarbeitung der Daten erproben

Bei eigener Umsetzung einer Direktanbindung sind das Testen der Anwendungsfälle und die Teilnahme an der EUDI-Wallet-Sandbox Voraussetzung für den späteren Produktivbetrieb.

Direkt einsteigen und hier informieren

- Developer Guide mit technischer Dokumentation und Onboarding Informationen: bmi.usercontent.opencode.de/eudi-wallet/developer-guide/
- Informationsseite des Orchestrators mit Onboarding-Prozess und Ansprechpersonen: eudi-wallet.gov.de/ecosystem-knowledge-center
- EUDI-Wallet Projektwebsite: eudi-wallet.gov.de
- Teilnahme am EUDI-Wallet-Ökosystem: www.eudi-wallet.gov.de/oekosystem/teilnahme

Konsequenz für die Anbindungsentscheidung

Öffentliche Stellen, die ein Prüfergebnis in ein Fachverfahren übernehmen oder einen Nachweis der erfolgten Prüfung vorhalten müssen, benötigen eine integrierte Lösung und damit einen anderen Anbindungsweg – etwa die Direktanbindung mit Wallet-Adapter im Cross-Device-Flow. EUDI Check DE kann in diesen Fällen als Übergangslösung dienen, um Nachweise ab dem Go-Live überhaupt prüfen zu können, während die integrierte Lösung aufgebaut wird.

Zielgruppe von EUDI Check DE sind Akzeptanzstellen, die ein Prüfergebnis im Moment der Vorlage benötigen und anschließend nichts aufbewahren müssen – etwa Bürgerbüros, Bäder, Museen, Sportvereine oder Einlasskontrollen.

Aufwand und zeitliche Planung bei der Umsetzung einer Anbindungslösung

Erfahrungswert aus dem Pilotvorhaben der Landeshauptstadt Dresden: rund sieben bis neun Monate von der Analyse bis zum Roll-out. Davon entfallen etwa zwei Monate auf die Anbahnung und die Erhebung der Betroffenheit, rund zwei bis drei Monate auf Stakeholderanalyse, Rollenklärung und Umsetzungsvereinbarung, zwei bis drei Monate auf die technische Umsetzung und etwa ein Monat auf Onboarding und Betriebsaufnahme. Die Phasen überlappen sich teilweise.

- Verfahren, die zeitnah zum Start produktiv sein sollen, gehören wegen der Vorlaufzeiten **sofort** in die fachliche und organisatorische Vorbereitung.
- Für alle übrigen Verfahren mit Identifizierungs- und Authentifizierungsbedarf ist zunächst die Erfüllung der Akzeptanzpflicht sicherzustellen; die weitergehende Anbindung kann für das Folgejahr eingeplant werden.
- Verfahren ohne Identifizierungs- und Authentifizierungsbedarf können zurückgestellt und regelmäßig neu bewertet werden.

Nächste Schritte und weiterführende Quellen

- Betroffene Verfahren der betreuten Kommunen systematisch erheben und nach benötigten Funktionalitäten sortieren
- Anbindungsweg je Verfahren vorschlagen und mit der jeweiligen Kommune sowie dem Land abstimmen
- Anwendungsfall in der EUDI-Wallet-Sandbox einreichen und die technische Anbindung erproben
- Frühzeitigen Austausch mit BMDS und Common Codes GmbH zur Auswahl der Anbindungsoption suchen – über [das Kontaktformular auf eudi-wallet.gov.de](#)
- EUDI-Wallet Projektwebsite: [eudi-wallet.gov.de](#)
- Teilnahme am EUDI-Wallet-Ökosystem: [www.eudi-wallet.gov.de/oekosystem/teilnahme](#)
- Developer Guide mit Informationen zu den Open-Source-Bibliotheken sowie Onboarding-Informationen: <https://bmi.usercontent.opencode.de/eudi-wallet/developer-guide/>
- Liste der Service Provider, die bei der Integration unterstützen: [FAQ auf eudi-wallet.gov.de, Thema „Sandbox“](#)
- Zielbild und Konzept zur Verwaltungsanbindung: [Beschluss des IT-Planungsrats](#)
- Vertiefte technische und regulatorische Einordnung: [Handlungsleitfaden des BSI zur Anbindung der EUDI-Wallet](#) (Januar 2026)
- Informationen zur Anbindungsoption über die BundID: [BundID SSP](#)



Stand: 06.10.2026. Einzelne Infrastrukturkomponenten und Zeitpläne befinden sich noch in Konkretisierung. Angaben zu Komponenten im Aufbau sind entsprechend gekennzeichnet und werden aktualisiert, sobald belastbare Festlegungen vorliegen.

Anhang

(Stand: 09.10.2026)

I. Anhang: Fragen und Antworten

Was sind Nachweise und was unterscheidet sie von Bescheiden?

Dabei ist zwischen Nachweis und Bescheid zu unterscheiden: Ein Nachweis belegt lediglich Attribute, also Eigenschaften natürlicher Personen oder Organisationen, während ein Bescheid einen Verwaltungsakt im Sinne des § 35 VwVfG darstellt. Die EUDI-Wallet dient der Bereitstellung und Nutzung digitaler Nachweise, ersetzt jedoch keine Bescheide und bietet selbst keine Möglichkeit zur rechtssicheren Bescheidzustellung (siehe Tabelle 2: Abgrenzung Begriffe Nachweis und Bescheid).

Bescheid	Nachweis laut eIDAS-VO 910/2014
Ein Bescheid stellt gemäß § 35 VwVfG einen Verwaltungsakt dar, also eine hoheitliche Entscheidung, die einen Einzelfall verbindlich regelt und unmittelbare Rechtswirkung nach außen erzeugt.	Ein Nachweis dokumentiert Tatsachen oder Attribute (z. B. Ausbildungsstatus, Wohnsitz, Berechtigungen), ist aber keine hoheitliche Regelung und löst keine Rechtsfolgen im verwaltungsrechtlichen Sinne aus. Ein Nachweis dient ausschließlich dazu, bestimmte Merkmale zu belegen.

Tabelle 1: Abgrenzung Begriffe Nachweis und Bescheid

Welche Arten von Nachweisen gibt es und was muss beachtet werden?

Im EUDI-Wallet-Ökosystem können unterschiedliche Arten elektronischer Nachweise bereitgestellt werden. Zum Start der EUDI-Wallet im Jahr 2027 werden Nachweise in Deutschland jedoch zunächst ausschließlich als Electronic Attestations of Attributes (EAAs) bereitgestellt. Perspektivisch können auch Qualified Electronic Attestations of Attributes (QEAA) sowie Public Electronic Attestations of Attributes (Pub-EAA) relevant werden. Die Anforderungen und Rollen dieser Nachweisarten unterscheiden sich hinsichtlich Vertrauensniveau, regulatorischer Vorgaben und Verantwortlichkeiten der ausstellenden Stelle.

Ein qualifizierter Nachweis (QEAA) muss im Vergleich zu einem nicht-qualifizierten Nachweis (EAA) zusätzliche regulatorische und technische Anforderungen nach eIDAS erfüllen.

Perspektivisch setzt die Ausstellung von Pub-EAAs beispielsweise voraus, dass die ausstellende Stelle selbst die authentische Quelle ist oder im unmittelbaren Auftrag einer authentischen Quelle einer



öffentlichen Stelle handelt. In Deutschland betrifft dies insbesondere registerführende Stellen und fachlich zuständige Behörden.

Die finalen Anforderungen für QEAA- und Pub-EAA-Aussteller werden derzeit auf europäischer Ebene konkretisiert. Für die Einordnung geeigneter Attestierungstypen kann der Decision Guide des nationalen Blueprints¹ herangezogen werden.

Was sind Rulebooks?

Ein Rulebook² ist die verbindliche Spezifikation für einen Nachweistyp: Es legt fest, welche Attribute ein Nachweis enthält, wie er ausgestellt wird und wie eine prüfende Stelle ihn verifiziert. Bevor eine Behörde ein eigenes Rulebook erstellt, sollte sie prüfen, ob bereits ein passendes Rulebook existiert – etwa im Katalog der Attestierungen³. Die Übernahme eines bestehenden Rulebooks ist empfohlen, um Interoperabilität zwischen Behörden sicherzustellen.

Nur, wenn kein passendes Rulebook existiert, sollte eine Behörde ein eigenes entwickeln – idealerweise in Abstimmung und Zusammenarbeit mit anderen Stellen mit ähnlichem Bedarf, um Doppelarbeiten und uneinheitliche Schemata zu vermeiden. Hierbei werden bestehende Strukturen des Datenmanagement der Registermodernisierung nachgenutzt. Nähere Anleitung zur Erstellung eines Rulebooks findet sich in der Implementer-Dokumentation zu Rulebooks.

Wie unterscheiden sich verschiedene Verifizierungstypen?

Die Verifizierung von Nachweisen im Rahmen von Verwaltungsverfahren ist von der fachlichen Verifikation von Attributwerten gegenüber authentischen Quellen bei Ausstellung oder bereits ausgestellten Nachweisen auf Verlangen Nutzender zu unterscheiden. Während öffentliche Stellen bei der Entgegennahme von Nachweisen deren Echtheit, Gültigkeit und Integrität prüfen, dient der nach Art. 45e eIDAS-Verordnung (EU) 2024/1183 vorgesehene Verifikationsmechanismus für qualifizierte Vertrauensdiensteanbieter (QTSP) der fachlichen Bestätigung einzelner Attributwerte bereits ausgestellter Nachweise gegenüber einer authentischen Quelle. Hierfür können Mitgliedstaaten zentrale Überprüfungsstellen (Single Points of Verification, SPoV) bereitstellen. Der Mechanismus wird auf Veranlassung der nutzenden Person ausgelöst und ersetzt nicht die Verifizierung von Nachweisen durch öffentliche Stellen im Rahmen ihrer Verwaltungsverfahren.

¹ Decision Guide <https://bmi.usercontent.opencode.de/eudi-wallet/eidas-2.0-architekturkonzept/content/ecosystem-concepts/trust/decision-guide/>

² Rulebook: <https://bmi.usercontent.opencode.de/eudi-wallet/developer-guide/eaa/rulebook/?h=rule>

³ Katalog der Attestierungen <https://sandbox.eudi-wallet.org/catalog>



Was ist eine Authentische Quelle?

Eine „Authentische Quelle“ ist ein Datenspeicher oder ein Datensystem, der bzw. das als primäre Quelle für Daten oder Attribute natürlicher Personen und Organisationen dient und als solche anerkannt ist⁴. Die Anerkennung kann auf dem Unionsrecht, dem nationalen Recht oder der Verwaltungspraxis beruhen. Authentische Quellen können in der Verantwortung einer öffentlichen Stelle liegen oder von einer privaten Stelle betrieben werden. Eine durch die eIDAS-Verordnung definierte Mindestliste von Attributen muss elektronisch durch QTSPs überprüfbar sein, sofern sie aus Authentischen Quellen des öffentlichen Sektors stammen⁵.

Was ist ein (Q)EAA-Provider?

(Q)EAA-Provider sind Organisationen, die elektronische Attributsbescheinigungen (EAA) beziehungsweise qualifizierte elektronische Attributsbescheinigungen (QEAA) für Nutzende der EUDI-Wallet ausstellen. Sie übernehmen die Rolle des Issuers und sind für die Erstellung, Signierung bzw. Siegelung sowie die Bereitstellung der Nachweise verantwortlich. Die ausgestellten Nachweise können in der EUDI-Wallet gespeichert und gegenüber Wallet Relying Parties zur Nachweisführung verwendet werden. Für QEAA-Provider gelten zusätzliche Anforderungen nach der eIDAS-Verordnung, insbesondere hinsichtlich Konformitätsbewertung, Vertrauensniveau und Einbindung qualifizierter Vertrauensdiensteanbieter, die zertifiziert sein müssen. Die finalen europäischen Vorgaben sowie deren nationale Auslegung für QEAA-Provider und Zertifizierungsschemata befinden sich derzeit noch in der Konkretisierung. QEAA bzw. die dazu gehörigen QTSP müssen zertifiziert werden.

Was ist ein Pub-EAA-Provider?

Pub-EAA-Provider sind Behörden (öffentliche Stellen) oder bevollmächtigte Vertreter von Behörden, die selbst oder im Namen einer authentischen Quelle Bescheinigungen ausstellen. Die Berechtigung zur Ausstellung dieser Bescheinigungen setzt eine Konformitätsbewertung durch eine notifizierte Konformitätsbewertungsstelle voraus⁶. Pub-EAA-Provider werden durch den Mitgliedstaat an die EU-Kommission gemeldet, inkl. Angabe der Konformitätsbewertung und werden in einer EU-Vertrauensliste veröffentlicht⁷. Zusätzlich sind die Provider mit einem eindeutigen behördlichen

⁴ Art. 3 Abs. 47, eIDAS-Verordnung (EU) 910/2014, zuletzt geändert durch eIDAS-Verordnung (EU) 2024/1183 <https://bmi.usercontent.opencode.de/eudi-wallet/developer-guide/ea/rulebook/?h=rule>

⁵ Art. 45e i. V. m. Anhang VI, eIDAS-Verordnung (EU) 910/2014, zuletzt geändert durch eIDAS-Verordnung (EU) 2024/1183 https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202401183

⁶ Art. 45f. Abs. 1, 2 und 6, eIDAS-Verordnung (EU) 910/2014, zuletzt geändert durch eIDAS-Verordnung (EU) 2024/1183, Durchführungsverordnung (EU) 2024/2982 https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202402982

⁷ Art. 45f. Abs. 3, eIDAS-Verordnung (EU) 910/2014, zuletzt geändert durch eIDAS-Verordnung (EU) 2024/1183



Identifizierung sowie einem gültigen Zugriffs- und Registrierungszertifikat ausgestattet⁸. Die fachliche Zuständigkeit eines Pub-EAA-Providers wird bereits im Rahmen der Registrierung im EUDI-Wallet-Ökosystem berücksichtigt. Die Identität und Rolle der ausstellenden öffentlichen Stelle werden u.a. durch den national zuständigen Registrar geprüft und über Zugriffs- und Registrierungszertifikate verbindlich abgebildet, die zusammen mit den EU-Vertrauenslisten als zentraler Vertrauensanker für Relying Parties dienen. Darüber hinaus stellen auf EU-Ebene veröffentlichte Attestation Rulebooks und Kataloge strukturierte Informationen zu Nachweistypen und ausstellenden Stellen bereit und unterstützen so die maschinelle Einordnung der ausgestellten Bescheinigungen. Von Pub-EAA-Providern ausgestellte Bescheinigungen sollten so erstellt werden, dass sichergestellt ist, dass sie von Relying Parties als QEAA anerkannt werden können. Die finalen europäischen Vorgaben sowie deren nationale Auslegung für Pub-EAA-Provider befinden sich derzeit noch in der Konkretisierung.

Was ist eine Wallet Relying Party?

Wallet Relying Parties sind natürliche Personen oder Organisationen, die auf eine elektronische Identifizierung vertrauen – etwa durch eine EUDI-Wallet, andere elektronische Identifizierungsmittel oder Vertrauensdienste⁹. Wallet Relying Parties können von Nutzenden der EUDI-Wallet sowohl personenidentifizierende Daten (PID) als auch nicht-PID-bezogene Attributsbescheinigungen ((Q/Pub-)EAA) anfordern und müssen auch in der Lage sein, deren Echtheit des Siegels und Gültigkeit zu überprüfen¹⁰. Die Wallet Relying Party (Verifier) prüft die durch Nutzende der EUDI-Wallet präsentierte Nachweise auf deren Echtheit des Siegels und Gültigkeit.

Wie funktionieren Registrierungs- und Zertifikatsanforderungen?

Die Rollen - (Q)EAA-/ Pub-EAA-Provider und Wallet Relying Parties - unterliegen denselben Registrierungs- und Zertifikatsanforderungen, unterscheiden sich jedoch funktional: Issuer erzeugen und siegeln/signieren Nachweise, während Wallet Relying Parties (Verifier) diese Nachweise im Rahmen eines Prozesses verifizieren, und zweckgebunden nutzen.

Zum Zweck des Onboardings ist eine vorherige Registrierung bei der zuständigen nationalen Registrierungsstelle – dem sogenannten Relying Party Registrar¹¹ – erforderlich Art. 5b Abs. 1 und 3¹².

⁸ Durchführungsverordnung (EU) 2025/848 https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202500848

⁹ Art. 3 Nr. 6, eIDAS-Verordnung (EU) 910/2014, zuletzt geändert durch eIDAS-Verordnung (EU) 2024/1183

¹⁰ Art. 5a Abs. 5a ii, eIDAS-Verordnung (EU) 910/2014, zuletzt geändert durch eIDAS-Verordnung (EU) 2024/1183

¹¹ Wallet Relying Party Registrar in der Implementer Guidance der SPRIND:

<https://bmi.usercontent.opencode.de/eudi-wallet/eidas-2.0-architekturkonzept/content/ecosystem-vision-and-fundamentals/what-is-the-ecosystem/?h=wallet+relying#wallet-relying-party-registrar-wrp-registrar>

¹² eIDAS-Verordnung (EU) 910/2014, zuletzt geändert durch eIDAS-Verordnung (EU) 2024/1183



Dafür müssen Wallet Relying Parties Daten zur Ausstellung eines Zugriffs- und Registrierungszertifikates bereitstellen:

- Das Zugriffszertifikat dient der Authentifizierung der Wallet Relying Party gegenüber der EUDI-Wallet. Es wird durch den Wallet Relying Party Registrar ausgestellt und enthält die für die technische Identifikation der Wallet Relying Party notwendigen Attribute. Die rechtliche Grundlage bildet Anhang IV der DVO 2025/848¹³.
- Das Registrierungszertifikat dient der Transparenz und Nachvollziehbarkeit der Datenverarbeitung durch die Wallet Relying Party. Es dokumentiert, welche Attribute von der Wallet Relying Party angefordert werden und zu welchem Zweck. Die rechtliche Grundlage bildet Anhang V der DVO 2025/848.

Das Schlüsselpaar des Zugriffszertifikats wird von der jeweiligen Organisation erzeugt und der passende Private Key verbleibt ausschließlich dort. Der Public Key des Zugriffszertifikats wird jedoch vom Wallet Relying Party Registrar im Zertifikat beglaubigt.

Das Registrierungszertifikat wird vom Registrar erzeugt, ist an das Zugriffszertifikat gebunden (kein eigenes Key Binding) und dient der Bescheinigung der Registrierung gegenüber der EUDI-Wallet. Es ist zudem öffentlich einsehbar, sodass andere Wallet Relying Parties den registrierten Nutzungszweck und die dafür benötigten Attribute einsehen können.

Vertrauenslisten sind ein zentrales Instrument zur Sicherstellung von Transparenz und Vertrauenswürdigkeit im EUDI-Wallet-Ökosystem. Gemäß Art. 22 in eIDAS-VO 910/2014 müssen diese Listen von benannten Stellen geführt, verwaltet und veröffentlicht werden. Sie enthalten die Vertrauensanker zur Prüfung der Akteure.

Die Vertrauenslisten umfassen unter anderem (Bezug zu eIDAS-VO 910/2014):

- PID-Provider (Art. 9 Absatz 1 Buchst. d),
- EUDI-Wallet Provider (Art. 5d Absatz 1),
- QEAA-Provider (Art. 22 Absatz 1),
- Pub-EAA-Provider (Art. 45f Absatz 3),
- sowie registrierte Relying Parties (Art. 5a Absatz 18 Buchst. a).

Diese Listen dienen als technische und organisatorische Vertrauensanker und sind Voraussetzung für die EU-weite Interoperabilität. Sie ermöglichen die automatisierte Prüfung von Zertifizierungsstatus, Widerrufen und weiteren Metadaten durch Wallet Relying Parties und EUDI-Wallets. Die genaue

¹³ Durchführungsverordnung (EU) 2025/848 https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202500848



Ausgestaltung der Vertrauenslisten, die technischen Formate und die Schnittstellen zur EU-Kommission und zur Kooperationsgruppe sind in den entsprechenden Durchführungsrechtsakten geregelt und werden im Rahmen der nationalen Umsetzung konkretisiert.

Was macht der Wallet Relying Party Registrar (WRP Registrar)?

Für alle Akzeptanzstellen (Relying Parties) ist der Wallet Relying Party Registrar zuständig. Dieser führt das Register, prüft die Registrierungsangaben nach Maßgabe der Registrierungsrichtlinie und erfasst insbesondere die angemeldeten Verwendungszwecke und Attribute¹⁴.

Nach aktuellem Stand soll die Registrierung von Wallet Relying Parties in Deutschland über einen zentralen Registrar erfolgen, der in eine nationale EUDI-Wallet-Ökosystem-Managementplattform eingebunden ist. Für juristische Personen ist eine Identifizierung über „Mein Unternehmenskonto“ auf Basis eines ELSTER-Organisationszertifikats vorgesehen. Ergänzend wird die Identifizierung einer natürlichen Person verlangt, die die Registrierung für die Organisation oder Behörde bestätigt. Für öffentliche Stellen und andere Wallet Relying Parties bedeutet dies, dass sie sich vor der produktiven Nutzung der EUDI-Wallet registrieren und die erforderlichen Angaben zu ihrem Anwendungsfall sowie den angeforderten Nachweisen bereitstellen müssen.

Was ist ein PID-Provider?

Der PID-Provider ist für die Ausstellung, Verwaltung und den Widerruf der PID zuständig. Der „Anbieter von Personenidentifizierungsdaten“ wird als eine natürliche oder juristische Person definiert, die für die Ausstellung und den Widerruf der PID verantwortlich ist und sicherstellt, dass diese kryptografisch an eine EUDI-Wallet gebunden sind¹⁵. Die Auswahl des PID-Providers erfolgt national und ist nicht durch die eIDAS-Verordnung vorgegeben. Der PID-Provider ist bundesweit einer zentralen Stelle zugeordnet und steht in direktem Austausch mit weiteren Komponenten des EUDI-Wallet-Ökosystems.

Was ist ein Qualifizierter Vertrauensdiensteanbieter (QTSP)

Ein QTSP ist ein zertifizierter Anbieter qualifizierter Vertrauensdienste, der etwa qualifizierte elektronische Signaturen, Siegel oder Zertifikate ausstellt¹⁶. QTSPs müssen regelmäßig Konformitätsbewertungen durch akkreditierte Stellen durchlaufen und der Aufsichtsstelle Prüfberichte vorlegen¹⁷. Alle qualifizierten QTSPs mit gültiger Notifizierung sind von den

¹⁴ Art. 2, Nr. 5, Durchführungsverordnung (EU) <https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:32024R2980>

¹⁵ Art. 2, Durchführungsverordnung (EU) 2024/2977 <https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:32024R2977>

¹⁶ Art. 3 Abs. 20, Art. 24 ff., eIDAS-Verordnung (EU) 910/2014, zuletzt geändert durch eIDAS-Verordnung (EU) 2024/1183

¹⁷ Art. 20 Abs. 1, eIDAS-Verordnung (EU) 910/2014, zuletzt geändert durch eIDAS-Verordnung (EU) 2024/1183



Mitgliedstaaten an die EU-Kommission zu melden und werden in einer EU-Vertrauensliste veröffentlicht¹⁸.

Was ist ein Vermittler?

Ein Vermittler (sog. Intermediary bzw. Intermediär) ist eine technische oder organisatorische Stelle, die im Auftrag einer Relying Party mit der EUDI-Wallet kommuniziert, ohne selbst als Relying Party registriert zu sein. Er übernimmt Aufgaben wie die Weiterleitung von Anfragen, Schnittstellenintegration, Validierung von Attributsbescheinigungen oder Anbindung bestehender Systeme, ohne selbst personenbezogene Attribute zu speichern, auszustellen oder auszuwerten¹⁹. Der Vermittler muss über ein gültiges Zugriffszertifikat sowie über ein Registrierungszertifikat verfügen, das nach Prüfung und Freigabe durch die jeweilige Relying Party durch den Registrar ausgestellt wird. Dieses Registrierungszertifikat enthält die Information, dass der Vermittler im Auftrag der Relying Party handelt und somit ist der Vermittler befähigt, Anfragen zu den im Registrierungszertifikat definierten Attributen an die EUDI-Wallet zu übermitteln.

Was macht der EUDI-Wallet Provider?

Der EUDI-Wallet Provider ist für die Bereitstellung und den Betrieb einer Wallet-Lösung verantwortlich. Die rechtliche Grundlage bildet Art. 2 Abs. 8 der DVO (EU) 2024/2981. Dort wird der EUDI-Wallet Provider als eine natürliche oder juristische Person definiert. EUDI-Wallet Provider müssen sicherstellen, dass ihre Wallet-Lösungen den Anforderungen der eIDAS-Verordnung entsprechen und gemäß Art. 5a in eIDAS-VO 910/2014 zertifiziert sind. Die Zertifizierung umfasst unter anderem die Prüfung der technischen Sicherheit, der Nutzerkontrolle und der Interoperabilität mit anderen Komponenten des EUDI-Wallet-Ökosystems.

Die Rolle des EUDI-Wallet Providers kann sowohl von öffentlichen als auch von privaten Organisationen übernommen werden. In Deutschland wird die initiale staatliche EUDI-Wallet durch die Bundesagentur für Sprunginnovationen (SPRIND) bereitgestellt. Diese Lösung dient als nationale Referenzimplementierung und erfüllt die Anforderungen an eine vertrauenswürdige, datenschutzkonforme und EU-interoperable EUDI-Wallet Infrastruktur. Die konkrete Ausgestaltung der Rolle, die technischen Anforderungen und die Zertifizierungsprozesse werden im nationalen Kontext definiert.

¹⁸ Art. 22, eIDAS-Verordnung (EU) 910/2014, zuletzt geändert durch eIDAS-Verordnung (EU) 2024/1183

¹⁹ Art. 5b Abs 10, eIDAS-Verordnung (EU) 910/2014, zuletzt geändert durch eIDAS-Verordnung (EU) 2024/1183; ARF 3.11



Was macht der Wallet-Adapter?

Der Wallet-Adapter übersetzt sowohl die eingehenden als auch die ausgehenden Anfragen/Antworten (d. h. Requests/Responses) zwischen der Wallet Relying Party und der EUDI-Wallet. Das bedeutet z.B. die Übersetzung eingehender JSON-Formate der Wallet Relying Party in SD-JWT VC, die Entgegennahme der Antworten der EUDI-Wallet im SD-JWT-VC-Format und die Übertragung dieser zurück in JSON – ohne selbst personenbezogene Attribute zu speichern, auszustellen oder auszuwerten. Außerdem orchestriert dieser Prüf- und Verifizierungsprozesse von Attributsbescheinigungen, insbesondere durch die Prüfung kryptografischer Siegel und Zertifikate zur Sicherstellung von Echtheit und Gültigkeit.

Wie funktioniert die Nutzung bei EU-Ausländerinnen/ EU-Ausländern und bei EUDI-Wallets anderer EU-Mitgliedstaaten in deutschen Verwaltungsdiensten?

Antwort: Gemäß der novellierten eIDAS-Verordnung sollen EUDI-Wallets grenzüberschreitend (in der EU) nutzbar, kostenlos und freiwillig sein. Deutschland setzt diese Vorgaben zunächst durch die Bereitstellung einer staatlichen EUDI-Wallet um. Europäische Interoperabilität wird über einheitliche Standards, Zertifizierung, Vertrauenslisten und gemeinsame Anforderungen an die Wallet-Architektur, Anbieter und Relying Parties abgesichert. Personen mit einer EUDI-Wallet eines anderen EU-Mitgliedstaats sollen ihre dort ausgestellten Identitätsdaten und Nachweise grundsätzlich auch in deutschen Verwaltungsdiensten nutzen können, soweit der jeweilige Dienst diese Nachweise unterstützt.

EU-Bürgerinnen und EU-Bürger anderer Mitgliedsstaaten können die staatliche EUDI-Wallet alternativ grundsätzlich auch ohne digitalen Ausweis (PID) – basierend auf deutschem Personalausweis und elektronischem Aufenthaltstitel (eAT) – nutzen. Sie können in der staatlichen EUDI-Wallet digitale Nachweise empfangen, speichern und vorzeigen und damit entsprechend Dienste nutzen, die keinen digitalen Ausweis erfordern. Für die Identifizierung bleibt hingegen die EUDI-Wallet des eigenen Herkunftsstaates maßgeblich. Nur diese enthält die national gültigen Personenidentifizierungsdaten (PID).

II. Anhang: Direkte Anbindung: Wallet-Adapter Onboarding Dokumentation Governikus

i) Kurzübersicht



Abbildung 1: Wallet-Adapter Onboarding Überblick

ii) Annahmen

- Die Präsentation und das Ausstellen von Nachweisen erfolgt über das Internet mit Hilfe eines Onlinedienstes (Remote Presentation).
- Der Onlinedienst und die EUDI-Wallet werden auf demselben Gerät (Smartphone des Bürgers) aufgerufen (Same-Device-Flow).

iii) Einführende Hinweise

- Die PID stellt fachlich gesehen eine besondere Form eines Nachweises dar. Technisch jedoch unterscheidet sich ein Abruf der PID nicht wesentlich vom Abruf eines anderen Nachweises. Daher erfolgt die Beschreibung für die Szenarien 1 und 3 hier gemeinsam.
- Das EUDI Hub befindet sich derzeit in der Entwicklung und steht noch nicht in vollem Funktionsumfang zur Verfügung. Vorerst werden essentielle Funktionen des EUDI Hub durch die SPRIND Sandbox bereitgestellt. Der Wechsel von Sandbox zu EUDI Hub soll im Laufe des Jahres 2026 erfolgen.
- Alle hier getroffenen Aussagen zum EUDI Hub entsprechen dem aktuellen Kenntnisstand und können noch deutlichen Änderungen unterliegen.
- Keine der hier getroffenen Aussagen zum EUDI Hub kann in irgendeiner Form als verbindlich angesehen werden. Die einzig belastbaren Informationen zum EUDI Hub kommen von den Herstellern des EUDI Hub selbst.

iv) Checkliste für die Anbindung

Die Checkliste beschreibt die notwendigen Schritte zur Anbindung einer vorhandenen Instanz des Wallet-Adapters, entweder bei einem dienstleistenden Rechenzentrum oder bei Governikus. Die Einrichtung und Installation On-Premise sind nicht Teil dieser Checkliste, werden aber in der



Installationsanleitung des Wallet-Adapters beschrieben. Diese kann bei Bedarf durch Governikus bereitgestellt werden²⁰.

Schritte in Klammern können durch das Zertifikatsmanagement des Wallet-Adapters übernommen werden bzw. entfallen bei der Nutzung dieser Funktion. Dies setzt einen hinreichenden Entwicklungsstand seitens des EUDI Hub voraus.

Anbindung des Wallet-Adapters für Testzwecke:

1. Vorbereitung
 - a. Prüfen Sie, welche Nachweistypen bereits definiert sind und den Anforderungen des eigenen Use Cases genügen (z.B. PID)
2. Im EUDI Hub (Registrar) für Testbetrieb registrieren
 - a. Nutzeraccount anlegen
 - b. Wallet-Adapter als gewünschten Intermediär benennen
 - c. (Registrierungszertifikate für Testbetrieb erstellen)
 - d. (Registrierungszertifikate für Testbetrieb herunterladen)
3. Wallet-Adapter Testsystem anbinden
 - a. Bei Governikus / Betreiber für Testbetrieb anmelden
 - b. Authentisierungsdaten austauschen
 - c. Registrierungszertifikate einrichten
 - i. Option 1: (Registrierungszertifikate übermitteln)
 - ii. Option 2: Use Case und benötigte Daten über Wallet-Adapter definieren
 - d. Gegen die Schnittstelle des Wallet-Adapters implementieren
 - e. Bei Bedarf: Absprachen für Layout-Anpassungen des UI durchführen
4. Tests durchführen
 - a. Nationale EUDI-Wallet herunterladen
 - b. Test-PID mit Test PID-Issuer einrichten
 - c. Testfälle durchspielen

²⁰ <https://www.governikus.de/kontakt/>



Wechsel auf Produktivsystem:

1. Registrierung im EUDI Hub auf Produktivbetrieb wechseln
 - a. Organisationsidentität durch z.B. Mein Unternehmenskonto (ELSTER) nachweisen
 - b. Verantwortliche Person benennen
 - c. Multi-Faktor-Authentisierung einrichten
2. Auf produktive Wallet-Adapter-Instanz wechseln
 - a. Klärung der Nutzungsberechtigung (Berechtigte Nutzende der Anwendung Governikus oder vertragliche Grundlage)
 - b. Aufgerufene Wallet-Adapter Endpunkte anpassen
 - c. Authentisierungsdaten für Produktivsystem austauschen

Für das Ausstellen von Nachweisen in die EUDI-Wallet sind ggf. folgende Zusatzschritte notwendig:

1. Einen (qualifizierten) Vertrauensdiensteanbieter für die Signatur beauftragen
2. Den auszustellenden Nachweis definieren
 - a. Fachliche Konzeption der notwendigen Daten und des Lebenszyklus
 - b. Das maschinenlesbare Nachweisschema erstellen
 - c. Das menschenlesbare Nachweis-Rulebook erstellen
 - d. Nachweisschema und Nachweis-Rulebook im EUDI Hub hochladen

Bei den notwendigen Schritten kann Governikus beratend unterstützen. Auch bei Fragen oder Unterstützungsbedarfen bezüglich des Wallet-Adapters kann sich direkt an Governikus gewendet werden.

v) Details zur Anbindung

Im Folgenden werden die einzelnen Schritte der Checkliste näher ausgeführt. Dabei wird jeweils zwischen einer fachlichen Beschreibung, die möglichst auf technische Details verzichtet und einer detaillierten Beschreibung, welche sich vor allem an Entwickler und Betreiber richtet, unterschieden. Es steht Lesenden frei, sich auf die Textteile zu konzentrieren, die ihnen den höchsten Nutzen bieten.



vi) Testanbindung

Vorbereitung (fachlich)

Zum Start der EUDI-Wallet Anfang 2027 wird es voraussichtlich nur eine kleine Anzahl verfügbarer Nachweistypen geben, von denen die PID sicherlich der wichtigste ist. Diese enthält einen festdefinierten verpflichtenden Mindestdatensatz und je nach Ausstellungsland ggf. noch Zusatzattribute.

Die Liste der vorhandenen Attribute und ihre Übereinstimmung mit Attributen des elektronischen Personalausweises kann im [PID-Rulebook des Blueprints](#) nachgesehen werden.

Weitere Nachweistypen werden mit der Skalierung des EUDI-Wallet-Ökosystems hinzukommen. Diese werden über den EUDI Hub im so genannten Catalogue of Attestations (Nachweiskatalog) veröffentlicht.

Es sollte als erstes geprüft werden, welche Nachweistypen bereits vorhanden sind, welche Attribute diese enthalten und welche Nutzungsregeln das zugehörige Rulebook definiert. Gibt es keinen vorhandenen Nachweistyp, der alle benötigten Attribute enthält, kann ggf. die Kombination unterschiedlicher Nachweistypen helfen.

Vorbereitung (technisch)

Für Nachweise sind derzeit vor allem folgende drei Datenformate relevant:

1. SD-JWT VC
2. mDoc (ISO/IEC 18013-5 and ISO/IEC 23220-2)
3. W3C VC (optional)

Der Wallet-Adapter übersetzt die unterschiedlichen Datenformate in eine einheitliche Datenstruktur, sodass die Details der Datenformate für die anschließenden Dienste irrelevant sind. Zum aktuellen Zeitpunkt unterstützt der Wallet-Adapter SD-JWT VCs.

Im EUDI Hub (Registrar) für Testbetrieb registrieren (fachlich)

Um Vertrauen in die Teilnehmenden des EUDI-Wallet-Ökosystems herzustellen, müssen diese im zentralen Registrar des jeweiligen Mitgliedstaates registriert sein. In Deutschland heißt dieses System zusammen mit den unterstützenden Services EUDI Hub. Durch die Registrierung im EUDI Hub kann ein Onlinedienst gegenüber der EUDI-Wallet nachweisen, dass er vertrauenswürdig ist und mit Zustimmung der Nutzenden Daten erhalten darf. Die Registrierung im Hub ermöglicht auch die Sperrung von Onlinediensten im Falle eines Fehlverhaltens.

Das Anlegen eines Nutzendenaccounts für den Testbetrieb erfordert nur minimalen Aufwand und keine spezielle Validierung der Organisationsidentität.



Damit der Wallet-Adapter im Namen einer Organisation tätig werden darf, - um Nachweise abzurufen und auszustellen sowie Zertifikate zu erzeugen oder zu erneuern - muss dieses Vertrauensverhältnis im EUDI Hub bestätigt werden.

Alle Teilnehmenden des EUDI-Wallet-Ökosystems müssen definieren, in welcher Rolle sie tätig werden möchten und welche Nachweistypen sie nutzen möchten. Diese Information wird in einem sogenannten Registrierungszertifikat gespeichert, welches anschließend veröffentlicht wird und so durch die Öffentlichkeit (z.B. Datenschutzbehörden) geprüft werden kann. Die Informationen aus dem Registrierungszertifikat werden den Nutzenden der EUDI-Wallet angezeigt, damit diese eine informierte Entscheidung treffen können, ob sie einen Nachweis präsentieren bzw. annehmen möchten.

Für den Abruf von Nachweisen aus der EUDI-Wallet muss festgelegt werden, welche Nachweistypen angefragt werden sollen, welche Daten aus den angefragten Nachweisen genutzt werden sollen und zu welchem Zweck dies geschieht. Für jeden Anwendungszweck muss ein eigenes Registrierungszertifikat definiert werden. Registrierungszertifikate für den Abruf von Nachweisdaten könnten beispielsweise folgende Angaben enthalten:

- Nachweistyp: PID, Datensatz: Vorname, Nachname, Adresse, Zweck: Prüfen der Wohnanschrift
- Nachweistyp: PID, Datensatz: 18_oder_älter, Zweck: Altersprüfung

Für die Ausstellung von Nachweisen in die EUDI-Wallet muss das Registrierungszertifikat die Information enthalten, welcher Nachweistyp ausgestellt werden soll.

Die erstellten Registrierungszertifikate müssen vom Wallet-Adapter bei jeder Interaktion mit der EUDI-Wallet präsentiert werden, damit diese prüfen kann, ob der Nachweisabruf / die Nachweisausstellung in Übereinstimmung mit den registrierten Use Cases geschieht. Hierfür muss der Wallet-Adapter das Zertifikat technisch verfügbar haben. Daher ist es notwendig, das Registrierungszertifikat aus dem EUDI Hub herunterzuladen und an den Wallet-Adapter zu übermitteln (s.u.).

Wird das Zertifikatsmanagement des Wallet-Adapters genutzt, so werden die notwendigen Angaben für die Erstellung der Registrierungszertifikate über den Wallet-Adapter erfasst. Hierdurch ist der Wallet-Adapter in der Lage die benötigten Zertifikate über eine technische Schnittstelle des EUDI Hub zu erzeugen, anzupassen und zu erneuern. Das Herunterladen aus dem EUDI Hub und Übermitteln an den Wallet-Adapter entfällt in diesem Fall.

Im EUDI Hub (Registrar) für Testbetrieb registrieren (technisch)

Nach der Registrierung beim EUDI Hub erhalten die Teilnehmenden ein Zugriffszertifikat, welches sie als legitime Teilnehmende des EUDI-Wallet-Ökosystems ausweist und für jeden Anwendungsfall ein Registrierungszertifikat, welches Angaben zum Anwendungsfall enthält.



Das Zugriffszertifikat ist ein echtes Zertifikat mit zugehörigem Private Key. Dieser Private Key wird genutzt, um durch entsprechende Proofs nachzuweisen, dass Teilnehmende legitime Nutzende des Zugriffszertifikats sind. Zusätzlich enthält das Zugriffszertifikat die SAN-DNS Erweiterung, welche angibt, von welchen Hosts das Zertifikat genutzt werden darf. Bei Nutzung eines Intermediärs wird dessen Zugriffszertifikat genutzt, um sich gegenüber der EUDI-Wallet als Teilnehmende des EUDI-Wallet-Ökosystems zu legitimieren.

Das Registrierungszertifikat ist ein vom EUDI Hub signierter JSON-Datensatz, welcher einen Anwendungsfall eines Onlinedienstes beschreibt. Es gibt kein zugehöriges Schlüsselmaterial. Die Registrierungszertifikate sind in einem öffentlichen Speicher abgelegt und können von beliebigen Personen eingesehen werden. Es enthält keine kritischen oder geheimen Daten. Bei Verwendung eines Intermediärs wird das Registrierungszertifikat des angeschlossenen Onlinedienstes genutzt, an dessen Stelle der Intermediär mit der EUDI-Wallet interagiert.

Die Registrierungszertifikate sind kryptographisch an ein oder mehrere Zugriffszertifikate gebunden und können nur mit diesen Zugriffszertifikaten zusammen genutzt werden. Es ist möglich die Registrierungszertifikate eines Onlinedienstes an das Zugriffszertifikat eines technischen Dienstleisters zu binden, um diesem zu ermöglichen, im Namen des Onlinedienstes mit der EUDI-Wallet zu interagieren. Das entsprechende Zugriffszertifikat des Intermediärs wird dann im Registrierungszertifikat referenziert. Die EUDI-Wallet prüft bei jeder Interaktion, dass ein Registrierungszertifikat nur von einem berechtigten Host-System genutzt wird.

Wallet-Adapter Testsystem anbinden (fachlich)

Wenn Sie Interesse an der Nutzung des Testsystems haben, melden Sie sich bitte bei Governikus oder dem zuständigen Betreiber, um die Details zu besprechen und das Onboarding zu starten. In diesem Schritt kann auch bereits besprochen werden, auf welcher Grundlage eine spätere Nutzung des Produktivsystems erfolgen kann (s.u.).

Damit die Anbindung des Testsystems technisch erfolgen kann, benötigt Governikus / der Betreiber einige technische Angaben zum anzuschließenden System. Im Gegenzug werden die Authentisierungsdaten mitgeteilt, die notwendig sind, um sich gegenüber dem Wallet-Adapter zu authentisieren.

Zur Interaktion mit der EUDI-Wallet im Auftrag des anzubindenden Systems benötigt der Wallet-Adapter die Registrierungszertifikate für die vorgesehenen Use Cases des anzubindenden Systems. Sollten diese bereits im EUDI Hub erstellt worden sein, müssen diese an Governikus / den Betreiber übermittelt werden. Dies kann z.B. per E-Mail erfolgen.

Sollten bisher noch keine Registrierungszertifikate erstellt worden sein, kann dies über das Zertifikatsmanagement des Wallet-Adapters geschehen. Hierzu müssen die benötigten Angaben (Nachweistyp, Datensatz, Verwendungszweck) gemacht werden. Anschließend erzeugt der Wallet-Adapter im EUDI Hub die benötigten Registrierungszertifikate und lädt diese herunter.



Nach diesen initialen Maßnahmen muss der anzuschließende Onlinedienst die Schnittstelle des Wallet-Adapters anbinden. Hierfür sind Implementierungsarbeiten auf Seiten des Onlinedienstes notwendig. Die Details zur Schnittstelle sind der Schnittstellenbeschreibung zu entnehmen.

Das Layout der Nutzeroberflächen des Wallet-Adapters ist in begrenztem Umfang anpassbar, um sich möglichst nahtlos in das Design der Nutzeroberflächen des anzuschließenden Onlinedienstes einzufügen. Die Details hierfür sind mit Governikus / dem Betreiber abzusprechen und durch diesen umzusetzen.

Wallet-Adapter Testsystem anbinden (technisch)

Welche Authentisierungsdaten für die Anbindung des Wallet-Adapters benötigt werden, hängt vom angestrebten Anwendungsfall ab.

Für das **Abrufen von Nachweisen** werden folgende Angaben vom anzubindenden Onlinedienst benötigt:

- Redirect-URLs an welche die Nutzenden nach erfolgter Datenfreigabe zurückgeleitet werden

Im Gegenzug erhält der anzubindende Onlinedienst von Governikus / dem Betreiber folgende Informationen:

- Client ID
- Client Secret
- URL des Well-Known Endpunkt des Wallet-Adapters

Für das **Ausstellen von Nachweisen** in die EUDI-Wallet werden folgende Angaben benötigt:

- Zertifikat für die Push Request Signatur
- Zertifikat für die Datensatz Signatur
- Callback-URL des Onlinedienstes
- JWT Issuer Namen, der im JWT des Dataset hinterlegt ist

Diese Zertifikate können selbst-signiert sein. Die Anforderungen an die Signaturalgorithmen und die Schlüssellänge sind der Schnittstellendokumentation des Wallet-Adapters zu entnehmen.

Im Gegenzug erhält der anzubindende Onlinedienst von Governikus / dem Betreiber folgende Informationen:

- Client ID
- Client Secret



- URL des PUSH-Endpunktes

Die Details zur Einrichtung der Registrierungszertifikate sind stark vom Entwicklungsstand des EUDI Hub abhängig. Die Übermittlung der Zertifikate, die im EUDI Hub manuell erstellt wurden, kann vorerst per E-Mail erfolgen.

Für den Nachweisabruf wird eine Standard OpenIDConnect-Schnittstelle verwendet.

Für das Ausstellen von Nachweisen wird eine eigene Schnittstelle verwendet, die sich an den Pushed Authorization Request in OAuth 2.0 anlehnt. Hier wird eine initiale PUSH-Request an das Backend des Wallet-Adapters geschickt, um die notwendigen Daten zur Nachweisausstellung zu übermitteln. Als Antwort erhält der anzuschließende Onlinedienst eine RedirectUrl, an welche er die Nutzenden weiterleitet. Die Ausstellung des Nachweises endet gemäß OpenID4VCI für Nutzende in der EUDI-Wallet. Es findet also keine Rückleitung zum ursprünglichen Onlinedienst statt. Der Wallet-Adapter kann den Onlinedienst jedoch über den Abschluss des Ausstellungsvorgangs informieren, falls dieser einen entsprechenden Callback-Endpunkt zur Verfügung stellt.

Die technischen Details zur Ausgestaltung der UI-Anpassungen befinden sich derzeit noch in Abstimmung.

Tests durchführen (fachlich / technisch)

Für die Durchführung von Tests wird die nationale EUDI-Wallet der SPRIND empfohlen, da diese anfangs die einzig zugelassene EUDI-Wallet Lösung für Deutschland darstellt. Diese kann durch registrierte Nutzende aus dem EUDI Hub (Sandbox) heruntergeladen werden. Es gibt Versionen der nationalen EUDI-Wallet für iOS und Android. Es wird empfohlen, die Tests mit beiden Versionen durchzuführen, da diese sich in ihrem Verhalten aktuell noch deutlich unterscheiden.

Für den Großteil der Testfälle wird die Personalisierung der EUDI-Wallet mit einer PID benötigt. Dieser Prozess kann direkt aus der EUDI-Wallet heraus angestoßen werden. Für die Erzeugung einer PID ist die Identifizierung des Nutzers mittels Online-Ausweis (eID) erforderlich. Die EUDI-Wallet bietet zusätzlich die Möglichkeit den internen Kartensimulator der AusweisApp zu nutzen, um eine Testidentität in die EUDI-Wallet zu laden. Dadurch werden keine spezialisierten Testausweise benötigt.

vii) Wechsel zur produktiven Nutzung

Registrierung im EUDI Hub auf Produktivbetrieb wechseln (fachlich)

Um die EUDI-Wallet produktiv nutzen zu können, muss der Status des anzubindenden Onlinedienstes im EUDI Hub von Testbetrieb auf Produktivbetrieb gesetzt werden. Hierfür ist die eindeutige Identifizierung der Organisation notwendig und die Erlaubnis, im Namen dieser zu handeln. Dies wird voraussichtlich über ein ELSTER-Organisationszertifikat geschehen.



Zusätzlich ist es nötig, eine verantwortliche Person zu benennen, welche bei Bedarf kontaktiert werden kann.

Um die Sicherheit des registrierten Nutzeraccounts zu erhöhen, ist es an dieser Stelle notwendig, eine Multi-Faktor-Authentisierung für den Account einzurichten.

Für den Produktionsbetrieb müssen neue Registrierungszertifikate erstellt werden. Dies kann auf Grundlage der bereits für den Testdurchlauf erstellten Zertifikate geschehen. Wird das Zertifikatsmanagement des Wallet-Adapters verwendet, kann dieser die Aufgabe übernehmen.

Registrierung im EUDI Hub auf Produktivbetrieb wechseln (technisch)

Die genaue technische Ausgestaltung des Prozesses ist derzeit noch unklar.

Die Ausstellung neuer Zertifikate ist nötig, da die zugrundeliegenden Vertrauensanker auf unterschiedlichen Trusted Lists veröffentlicht werden.

Auf produktive Wallet-Adapter-Instanz wechseln (fachlich)

Spätestens zu diesem Zeitpunkt muss die vertragliche Grundlage für die Anbindung des Wallet-Adapters vorliegen.

Die Testsysteme und Produktivsysteme des Wallet-Adapters sind eigenständige technische Systeme, die unter unterschiedlichen Adressen aufgerufen werden und unterschiedliche Authentisierungsdaten verwenden. Dadurch soll das Risiko minimiert werden, dass Tests ggf. gegen ein Produktivsystem laufen.

Zur Anbindung des Produktivsystems des Wallet-Adapters ist es daher notwendig, dass der anzubindende Onlinedienst bzw. die für Produktion gedachte Instanz, die korrekten Endpunkte des Wallet-Adapter Produktivsystems aufruft. Für die Authentisierung gegenüber dem Produktivsystem werden dem Betreiber des anzubindenden Onlinedienstes die hierfür notwendigen Authentisierungsdaten mitgeteilt.

Auf produktive Wallet-Adapter-Instanz wechseln (technisch)

Keine besonderen Bemerkungen.

viii) Zusatzschritte für das Ausstellen von Nachweisen

Einen (qualifizierten) Vertrauensdiensteanbieter für die Signatur beauftragen (fachlich)

Die Integrität und Authentizität elektronischer Nachweise, die in eine EUDI-Wallet ausgestellt werden, können durch elektronische Siegel sichergestellt werden. Integrität bedeutet, dass der Nachweis



unverändert ist, während Authentizität den Aussteller und die Echtheit des Nachweises nachweist. Über das zugehörige Zertifikat lässt sich zudem der Aussteller des Nachweises eindeutig identifizieren. Im Rahmen der Validierung wird geprüft, ob das verwendete Zertifikat vertrauenswürdig ist und beispielsweise auf einer entsprechenden Trust List geführt wird.

Sofern für einen Nachweis ein qualifiziertes elektronisches Siegel erforderlich ist, muss ein qualifizierter Vertrauensdiensteanbieter (qVDA) eingebunden werden. Der qVDA führt vor der Ausstellung eines qualifizierten Zertifikats eine Identitätsprüfung gemäß den Anforderungen der eIDAS-Verordnung durch und stellt die erforderlichen qualifizierten Vertrauensdienste bereit. Anschließend kann der Vertrauensdiensteanbieter im Namen des Kunden Siegel erstellen und garantiert durch eine entsprechende technische Absicherung dafür, dass ein Siegel tatsächlich im Namen dieses Kunden veranlasst wurde. Für diesen Dienst fallen Gebühren an. Für die Identitätsprüfung und Beauftragung ist zwingend die direkte Kommunikation zwischen qVDA und der Behörde notwendig, die die Nachweise ausstellen möchte. Anschließend kann der Wallet-Adapter so konfiguriert werden, dass er für das Siegel der Nachweise den beauftragten qVDA und das Zertifikat der ausstellenden Behörde nutzt.

Einen (qualifizierten) Vertrauensdiensteanbieter für die Signatur beauftragen (technisch)

[Hier folgen ggf. noch Informationen.]

Den auszustellenden Nachweis definieren (fachlich)

Sollte kein bereits definierter Nachweistyp zu den Anforderungen des geplanten Use Cases passen, steht es jedem Teilnehmenden des EUDI-Wallet-Ökosystems frei, eigene Nachweistypen zu definieren und dem EUDI-Wallet-Ökosystem zur Verfügung zu stellen. Je nachdem, wie viele Behörden einen ähnlichen Nachweistyp ausstellen wollen oder wie groß der vorgesehene Nutzendenkreis für den Nachweistyp ist, kann es sinnvoll sein, die Definition des Nachweistyps zusammen mit anderen Teilnehmenden des EUDI-Wallet-Ökosystems abzustimmen.

Für die fachliche Definition eines Nachweistyps muss eine Vielzahl von Fragen beantwortet werden, von denen hier nur einige angerissen werden können:

1. Welche Daten soll der Nachweistyp enthalten?
2. Aus welcher Quelle sollen die Daten stammen?
3. Sollen immer alle Daten des Nachweises offengelegt werden oder ist es möglich nur einzelne Datenfelder abzufragen?
4. Wer ist berechtigt diesen Nachweistyp auszustellen?
5. Wer ist berechtigt diesen Nachweistyp abzurufen?



6. Wie wird Vertrauen zwischen den ausstellenden Instanzen und den abrufenden Instanzen etabliert? (Für die öffentliche Verwaltung ist dies häufig über die Trust Lists des Ökosystems gegeben.)
7. Wie sieht der Lebenszyklus des Nachweistyps aus?
 - a. Wann wird der Nachweistyp erstellt / ausgegeben?
 - b. Wann läuft er ab?
 - c. Unter welchen Bedingungen wird ein bereits ausgestellter Nachweis widerrufen?

Die technische Beschreibung des Nachweistyps findet durch eine sogenannte Schemadefinition statt. Diese ist maschinenlesbar und ermöglicht es den abrufenden Relying Parties, einen erhaltenen Nachweis gegen die Schemadefinition auf Korrektheit zu prüfen.

Die menschenlesbare Beschreibung des Nachweistyps findet in einem sogenannten Rulebook statt. Dieses dient dazu potenziellen Nutzenden des Nachweistyps (Aussteller und Abrufer) den Nachweistyp zu erklären. Insbesondere soll aus diesem Dokument klar werden, warum dem Nachweistyp und seinen enthaltenen Daten vertraut werden kann.

Die genauen Prozesse zur Erstellung, Pflege und Bereitstellung der Schemata und Rulebooks sind zum aktuellen Zeitpunkt noch nicht durch die zuständige Stelle definiert.

Den auszustellenden Nachweis definieren (technisch)

Die Art und Weise, wie der neue Nachweistyp maschinenlesbar zu beschreiben ist, hängt vom Format des auszustellenden Nachweises ab (W3C VCDM, SD-JWT VC oder mDoc). Für die maschinenlesbare Beschreibung von SD-JWT VCs werden JSON-Schemata verwendet.

Die menschenlesbare Beschreibung kann z.B. als PDF erfolgen.

ix) Vor-Ort Präsentation und Ausstellung

Mit dem Wallet-Adapter

Bisher wurde betrachtet, wie die Anbindung an das EUDI-Wallet-Ökosystem für den Fall funktioniert, dass Bürgerinnen und Bürger einen Onlinedienst über das Internet nutzen. Im Folgenden soll gezeigt werden, wie die Präsentation und das Ausstellen von Nachweisen in einer Servicestelle der öffentlichen Verwaltung funktionieren kann.

Bisher wurde davon ausgegangen, dass Bürgerinnen und Bürger auf ihren Smartphones einen Onlinedienst aufrufen, um Nachweise zu präsentieren oder ausgestellt zu bekommen, und dass sich die EUDI-Wallet auf demselben Smartphone befindet (Same-Device-Flow, remote presentation / issuing). Dieses Vorgehen ist für den Einsatz in Servicestellen der öffentlichen Verwaltung wenig



praktikabel. Daher wird im Folgenden der Fall betrachtet, dass sich ein Onlinedienst, welcher einen Nachweis abrufen oder ausstellen will, und die EUDI-Wallet der Bürgerinnen und Bürger auf unterschiedlichen Geräten befinden (Cross-Device-Flow).

In diesem Szenario kann der durchzuführende Verwaltungsakt als ein Onlinedienst realisiert werden, den Mitarbeitende der Servicestelle auf einem PC oder einem Tablet aufrufen. Wird ein Nachweis aus der EUDI-Wallet von Bürgerinnen und Bürgern benötigt, so wird der Wallet-Adapter aufgerufen. Dieser zeigt über den PC des Mitarbeitenden einen QR-Code an, welchen Bürgerinnen und Bürger mit dem Smartphone scannen können. Hierdurch wird die EUDI-Wallet geöffnet und die Nutzenden zur Freigabe der benötigten Daten aufgefordert. Wird die Freigabe erteilt, fließen die Daten aus der EUDI-Wallet über den Wallet-Adapter zum aufrufenden Onlinedienst auf dem PC der Behörde und können weiterverarbeitet werden. Das Ausstellen von Nachweisen funktioniert analog.

Dadurch, dass Bürgerinnen und Bürger die gesamte Zeit über durch den Mitarbeiter der Servicestelle beaufsichtigt werden, kann sichergestellt werden, dass für die Identifizierung (z.B. mittels PID), die Präsentation weiterer Nachweise und ggf. den Empfang von Nachweisen dasselbe Smartphone und dieselbe EUDI-Wallet verwendet werden. Dies ist bei einem rein online durchgeführten Cross-Device-Flow derzeit technisch noch nicht abschließend gelöst.

Mit der Verifier-App EUDI Check DE

Die Verifier-App EUDI Check DE ist aktuell in Entwicklung durch die SPRIND, um Nachweise, welche aus der EUDI-Wallet präsentiert werden, zu verifizieren und steht zum Go-Live der EUDI-Wallet zunächst nicht zur Verfügung. Nach aktueller Planung unterstützt EUDI Check DE Geräte, die weiterhin Sicherheitsupdates des Herstellers erhalten und über ein Secure Element oder eine vergleichbare verfügbare vertrauenswürdige Ausführungsumgebung verfügen. Weiter ist eine Registrierung als Relying Party im EUDI Hub. Die Verifier-App steht zum Go-Live der EUDI-Wallet am 02. Januar 2027 ausschließlich für iOS über den Apple App Store und für Android über den Google Play Store zur Verfügung. Eine Nachnutzung der im Nachweis enthaltenen Daten ist in diesem Fall nicht möglich, da die App nur die Echtheit und Gültigkeit des Nachweises verifiziert.

Governikus Wallet Adapter – Technische Sicht

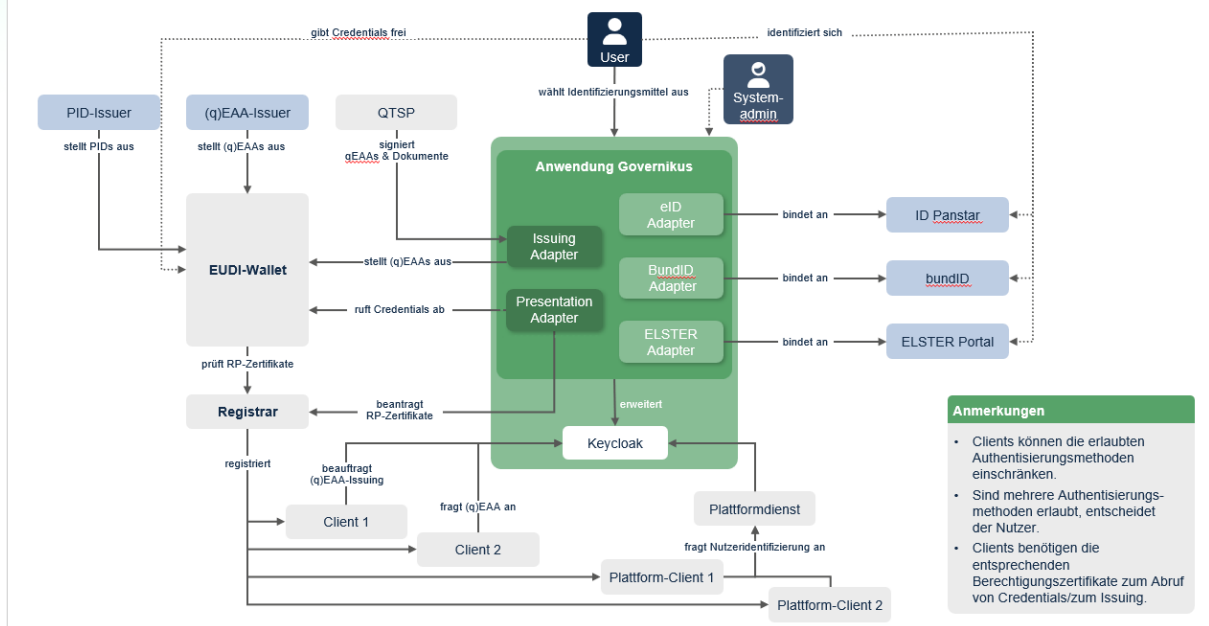


Abbildung 2: Technische Sicht Wallet-Adapter Governikus

Vorteile des Wallet-Adapters

- Wallet-Adapter erleichtert Anbindung an die EUDI-Wallet und reduziert Eigenentwicklungsaufwände und Pflege
- Zukunftssichere OpenID Connect (OIDC) Schnittstelle zu einem sich schnell entwickelnden EUDI-Wallet-Ökosystem
- Flexible und nutzerfreundliche Einsatzmöglichkeiten, unter anderem für synchrone (bspw. ohne Ablage im Postfach) und asynchrone Ausstellungsszenarien
- Transparenz für Nutzende bei Wallet-Interaktionen durch Anzeige der anfragenden Stelle in der Wallet
- Datensparsamkeit durch gezielte Abfrage von Attributen für den spezifischen Zweck (z B. Altersverifizierung) möglich
- Entlastung der Onlinedienste durch Zertifikatsverwaltung inklusive Abruf und automatisierter Erneuerung im Wallet-Adapter
- zusätzliche Funktionen wie QES-Anbringung und perspektivisch auch die Anbindung der European Business Wallet (EBW) werden zukünftig Teil des Wallet-Adapters

Nicht nur Wallet-Anbindung – sondern intelligente Steuerung des passenden Identifizierungsweges:

- EUDI-Wallet
- bundID
- ELSTER für natürliche Personen und Organisationen über „Mein Unternehmenskonto“
- Online-Ausweis
- europäische eID-Token, gemäß eIDAS-Verordnung



Governikus ID Mercury – Anwendung Governikus

- Wird als Identifizierungskomponente der Anwendung Governikus des IT-Planungsrates entwickelt
- Kontinuierliche Pflege und bedarfsgerechte Weiterentwicklung ist gewährleistet
- Anwendung Governikus steht Bund, Ländern und Kommunen flächendeckend zur Verfügung

Abbildung 3: Übersicht Vorteile Wallet-Adapter Governikus

III. Anhang: Prozessübersicht „Direkte Anbindung an die EUDI-Wallet bei Betrieb eines Wallet-Adapters am Beispiel des IT-Planungsrats Produkts“

Funktionalität 1: Sichere Identifizierung von Nutzenden mit der EUDI-Wallet



Nr.	Prozessschritt	Rolle	Beschreibung	Voraussetzung/ Anmerkung
1	Service Auswahl	Nutzender	Der Nutzende ruft die Webseite des Onlinediensts auf, wählt den gewünschten Service aus und startet den Identifizierungs-/ Authentifizierungsprozess.	<u>Bei Anbindung eines Wallet-Adapters:</u> Die fachlich zuständige Stelle ist als Wallet Relying Party registriert. Das Registrierungszertifikat wird dem Wallet-Adapter zur Ausübung seiner Rolle als Vermittler (Intermediary) übermittelt. Der Wallet-Adapter hat Zugriff bzw. hält die Registrierungszertifikate der Relying Party. <u>Falls kein Wallet-Adapter verwendet wird,</u> muss die fachlich zuständige Stelle selbst eine neue OpenID4VP Schnittstelle implementieren. <u>Bei Eigenbetrieb eines Wallet-Adapters:</u> Die fachlich zuständige Stelle verwaltet private Schlüssel der Zertifikate sicher, z. B. über HSM-basierte Key Storage Mechanismen. Sie betreibt den Wallet-Adapter als technische Komponente in der eigenen Systemlandschaft selbst.
2	Auswahl Identifizierungs- / Authentifizierungsmittel	Online-dienst / Fachl. zuständige Stelle	Der Onlinedienst der fachlich zuständigen Stelle fordert den Nutzenden zur Authentifizierung auf, z.B. über den Button "Mit EUDI-Wallet anmelden" oder eine sinngemäße Option. Daraufhin schickt der Onlinedienst die Datenanfrage an den Wallet-Adapter.	Ohne Wallet-Adapter muss die fachlich zuständige Stelle die Authentifizierungsanfrage an die EUDI-Wallet gemäß OpenID4VP-Standard versenden, inkl. Signierung der Authorization Request-Daten (siehe unten).
3	Erstellung Authorization Request	Wallet-Adapter	Der Wallet-Adapter: • erstellt eine Authorization Request gemäß OpenID4VP-Standard, inkl. DCQL Query, welche definiert, welche Credential und Attribute aus der	<u>Bei Anbindung eines Wallet-Adapters:</u> Der Wallet-Adapter nutzt sein eigenes Zugriffszertifikat. Zusätzlich stellt die fachlich zuständige Stelle dem Wallet-Adapter ihre eigenen



			EUDI-Wallet abgefragt werden sollen • präsentiert die Zertifikate • signiert die Authorization Request mit dem privaten Schlüssel des Zugriffszertifikats Der Wallet-Adapter stellt die Authorization Request für die EUDI-Wallet zum Abruf bereit.	Registrierungszertifikate zur Verfügung. <u>Bei Eigenbetrieb eines Wallet-Adapters:</u> Bei Eigenbetrieb nutzt der Wallet-Adapter das Zugriffszertifikat und die Registrierungszertifikate der Relying Party. Referenzen: EU 2025/848 Annex IV nr. 3 k (Zugriffszertifikat) & Annex V nr. 3 j (Registrierungszertifikat) OpenID4VP: OpenID Digital Credentials Protocols Working Group. (2025, 17. August). <i>OpenID for Verifiable Presentations 1.0 (Draft 20)</i>. OpenID Foundation. <u>OpenID for Verifiable Presentations 1.0</u>
4	Bereitstellung Authorization Request durch Link/QR Code	Wallet-Adapter	Der Nutzende wird aufgefordert seine Identität nachzuweisen. Der Wallet-Adapter zeigt dem Nutzenden eine Landing Page an. Dort werden sowohl ein Link als auch ein QR-Code angezeigt. Im Same-Device-Flow klickt der Nutzende auf den Link. Im Cross-Device-Flow scannt der Nutzende den QR-Code mit seinem Handy ab. Durch das im Link/QR-Code angegebene Protokoll (bspw.: openid4vp oder Haip-vp) weiß das Smartphone, dass eine Wallet geöffnet werden muss. Sind mehrere Wallets installiert, öffnet sich – je nach Betriebssystem – ein Auswahldialog zur Wahl der Wallet durch den Nutzenden.	Hinweis: QR Code Lösung ist nicht Phishing sicher und sollte nicht für LoA High sondern nur bis Substantial verwendet werden. Für LoA High gibt es das HAIP und dort nur den Same Device Flow, sowie perspektivisch die DC-API. Je nachdem, wie die Wallet-Adapter Komponente in die Systemlandschaft integriert ist, kann die Bereitstellung des Links/QR Codes variieren. In diesem Beispiel wird eine neue Landing Page erzeugt. Referenz: OpenID4VP: OpenID Digital Credentials Protocols Working Group. (2025, 17. August). <i>OpenID for Verifiable Presentations 1.0 (Draft 20)</i>. OpenID Foundation. <u>OpenID for Verifiable Presentations 1.0</u>
5	Verifizierung des Authorization Requests	EUDI-Wallet	Die EUDI-Wallet wird auf dem Endgerät gestartet, der Nutzende authentifiziert sich mit einem EUDI-Wallet	Referenz: ARF v3.0.0 (e.g 6.6. Trust throughout a PID or an attestation lifecycle)



			Authentifizierungsverfahren (z. B. PIN, biometrisch). Die EUDI-Wallet ruft die Authorization Request vom Endpunkt ab. Die EUDI-Wallet prüft die Echtheit der Anfrage und informiert den Nutzenden über das Prüfergebnis, inkl. der Information, ob mehr Attribute abgefragt werden, als im Registrierungszertifikat hinterlegt sind (= Overasking). •	
6	Prüfung und Freigabe der PID	Nutzender	Der Nutzende prüft die angeforderten PID-Attribute und gibt ihre Zustimmung zur Freigabe der ausgewählten PID-Attribute.	IETF OAuth Working Group. (2024, 8. Juli). <i>Selective Disclosure for JWTs (SD-JWT-VC) – draft-ietf-oauth-sd-jwt-vc-04</i> . IETF. <u>SD-JWT-based Verifiable Credentials (SD-JWT-VC)</u>
7	Präsentation der PID	EUDI-Wallet	Die EUDI-Wallet erstellt eine Authorization Response mit den genehmigten PID-Attributen (SD-JWT-VC) und sendet diese an den Wallet-Adapter.	Referenzen: ARF v.3.0.0 (e.g. 6.6.3.6 Relying Party Instance verifies the authenticity of the PID or attestation) Ohne die Implementierung des Wallet-Adapters, erhält die fachlich zuständige Stelle die PID als SD-JWT-VC-Response der EUDI-Wallet.
8	Validierung der PID	Wallet-Adapter	Der Wallet-Adapter prüft die empfangene PID-Attestation. Anschließend übersetzt der Wallet-Adapter die Response und sendet sie an den Onlinedienst der fachlich zuständigen Stelle.	Referenzen: PID-Verifizierung eIDAS-VO 910/2014 Art. 5a Nummer 5; ARF v.3.0.0; https://bmi.usercontent.open code.de/eudi-wallet/developer-guide/rp/guide/presentation/pid_presentation/#response-validation-checklist
9	Prüfung und Freigabe der Daten	Online-dienst / fachl. zuständige Stelle	Der Onlinedienst der fachlich zuständigen Stelle erhält die geprüften Daten und prüft, ob die Daten der nutzenden Person zu der Session gehören, Optional kann der Onlinedienst dem Nutzenden die Response präsentieren und zur Vorfürfüllung z.B. eines	Wird die Ident./Auth. als Teil eines Antragsprozesses durchgeführt, können die übermittelten Stammdaten zur Vorfürfüllung des Onlineformulars des Onlinedienstes verwendet werden. Dabei muss klar



			Onlineformulars im Rahmen einer Antragsstellung nutzen. Personendaten, welche aus der PID übernommen wurden, können nicht bearbeitet werden. Der Nutzende kann allerdings ergänzende Informationen, wie E-Mail-Adresse oder Telefonnummer ergänzen und die Inhalte noch einmal prüfen. Anschließend werden die Daten zur weiteren Verarbeitung für das Antragsverfahren freigegeben.	nachvollziehbar sein, welche Felder aus der PID stammen.
10	Erfolgreiche Ident./Auth. des Nutzenden	Online-dienst	Ist der Prozess erfolgreich, ist der Nutzende für die Nutzung des Services authentifiziert.	

Funktionalität 2: Ausstellung von Nachweisen über Onlinedienste/-portale in die EUDI-Wallet am Beispiel des Ausstellungsprozesses Dresden Pass; Fachlich zuständige Stelle in der Rolle eines EAA-Providers

Bedeutung Farbgebung: Einzelne Prozessschritte aktuell in Überarbeitung durch technische Erweiterung des IT Planungsrat Produkts (Sequenzieller Flow zu Nested Flow)

Nr.	Prozessschritt	Rolle	Beschreibung	Voraussetzung/ Anmerkung
0	Vorbedingung	Nutzender	Der Nutzende hat bei der fachlich zuständigen Stelle/Onlinedienst einen Prozess durchlaufen, welcher sie zum Abruf eines Nachweises berechtigt.	z.B. wurde ein Antragsprozess durchlaufen, auf den die Ausstellung eines Nachweises folgt.
1	Bereitstellung des Nachweises	Online-dienst	Die für den Nachweis notwendigen Daten werden als strukturierter Datensatz im JSON-Format von der fachlich zuständigen Stelle an den Onlinedienst übermittelt. Der Onlinedienst hält die Daten temporär vor. Der Nutzende wählt aus, den Nachweis in seine EUDI-Wallet auszustellen, z.B. durch eine entsprechende Schaltfläche.	Die Ausstellung (=Issuing) erfolgt über einen Ausstellungsservice. Dieser kann z.B. direkt über die Kommune in der Rolle eines EAA-Providers bereitgestellt werden. In diesem Beispiel übernimmt die LH Dresden die Rolle eines EAA-Providers und stellt die Ausstellungsfunktion über den Wallet-Adapter für die fachlich zuständigen Stellen bereit. Der Onlinedienst ist in der Lage z.B. über die Wallet-Adapter Komponente das Nachweisangebot an die EUDI-Wallet des Nutzenden zu stellen.



2	Datenübermittlung	Online-dienst	Die Daten für den Nachweis werden vom Onlinedienst an den Wallet-Adapter übertragen.	
3	Erstellung der Credential Offer	Wallet-Adapter	Auf Basis der strukturierten Daten wird ein Credential Offer gemäß OpenID4VCI-Protokoll erzeugt. Der Wallet-Adapter antwortet dem Onlinedienst durch Übermittlung der Adresse für die Landing Page (redirect uri).	In diesem Szenario würde die Kommune selbst als EAA-Provider agieren und der Wallet-Adapter als technische Ausstellungs-Komponente fungieren. Referenz: OpenID4VCI: OpenID Digital Credentials Protocols Working Group. (2025, 16. September). <i>OpenID for Verifiable Credential Issuance 1.0 (Final Status)</i>. OpenID Foundation. <u>OpenID for Verifiable Credential Issuance 1.0</u> https://bmi.usercontent.opencode.de/eudi-wallet/eidas-2.0-architekturkonzept/content/features/EAA/EAA-Issuance-OpenID4VC/
4	Redirect zur Wallet-Adapter Landing Page	Online-dienst	Der Nutzende wird automatisch zur Landing Page des Wallet-Adapters geleitet.	
4.5	Authentifizierung des Nutzenden	Wallet-Adapter	Der Wallet-Adapter führt eine Nutzenden-identifizierung mit Hilfe der PID durch, wie in Funktionalität 1 beschrieben. Der Wallet-Adapter überprüft, dass die identifizierte Person diejenige ist, welche zum Empfang des Nachweises berechtigt ist. Anschließend zeigt der Wallet-Adapter eine Seite für die Credential Offer an.	Hinweis: Die Beschreibung folgt noch dem sequenziellen Flow, da zum Zeitpunkt der Erstellung die EUDI-Wallet noch keinen nested flow unterstützt hatte. Da sich dies nun geändert hat, wird der Wallet-Adapter als IT PLR dahingehend umgebaut. Sobald die technische Anpassung erfolgt ist, wird auch die Beschreibung aktualisiert.
5	Bereitstellung der Credential Offer	Wallet-Adapter	Der Wallet-Adapter zeigt dem Nutzenden sowohl einen Link als auch einen QR-Code an. Im Same-Device-Flow klickt der Nutzende auf den Link. Im Cross-Device-Flow scannt der Nutzende den	Referenz: OpenID4VCI: OpenID Digital Credentials Protocols Working Group. (2025, 16. September). <i>OpenID for Verifiable Credential Issuance 1.0 (Final Status)</i>. OpenID Foundation. <u>OpenID for Verifiable Credential Issuance 1.0</u>



			QR-Code mit seinem Handy ab. Durch das im Link/QR-Code angegebene Protokoll (bspw.: openid4vci oder Haip-vvci) weiß das Smartphone, dass eine Wallet geöffnet werden muss. Sind mehrere Wallets installiert, öffnet sich – je nach Betriebssystem – ein Auswahldialog zur Wahl der Wallet durch den Nutzenden.	
6	Verifizierung der Credential Offer	EUDI-Wallet	Die EUDI-Wallet wird auf dem Endgerät gestartet, der Nutzende authentifiziert sich mit einem EUDI-Wallet Authentifizierungs-verfahren (z. B. PIN, biometrisch). Die EUDI-Wallet ruft die Credential Issuer's Metadaten vom bereitgestellten Endpunkt ab. Die EUDI-Wallet prüft die Echtheit der Anfrage und informiert den Nutzenden über das Prüfergebnis. Der Nutzende akzeptiert das ihm angebotene Credential.	Die Credential Issuer's Metadaten beinhalten: • Technische Informationen über den Aussteller • Übersetzungs- und Visualisierungsinformationen für das auszustellende Credential
7	Erstellung des Credential Request	EUDI-Wallet	Erst nach Zustimmung des Nutzenden erstellt die EUDI-Wallet den Credential Request nach OpenID4VCI und übermittelt die Credential Request an den Wallet-Adapter	Referenzen: EU 2025/848 Annex IV nr. 3 k (Zugriffszertifikat) & Annex V nr. 3 j (Registrierungszertifikat) Referenz: OpenID4VCI: OpenID Digital Credentials Protocols Working Group. (2025, 16. September). <i>OpenID for Verifiable Credential Issuance 1.0 (Final Status)</i>. OpenID Foundation. OpenID for Verifiable Credential Issuance 1.0
8	Verifizierung des Credential Requests	Wallet-Adapter	Der Wallet-Adapter prüft die Gültigkeit der EUDI-Wallet Instanz, des EUDI-Wallet Providers sowie weitere Eigenschaften der EUDI-Wallet	Um Missbrauch der Daten zu vermeiden, wird festgelegt, dass auch bei nicht-qualifizierten EAAs die erneute Identifizierung/Authentifizierung des Nutzenden durch den



			•	Aussteller (Issuer) gefordert wird; IETF OAuth Working Group. (2024, 8. Juli). <i>Selective Disclosure for JWTs (SD-JWT-VC) – draft-ietf-oauth-sd-jwt-vc-15</i> . IETF. SD-JWT-based Verifiable Credentials (SD-JWT-VC)
9	Anfügen einer Disclosure Policy	Wallet-Adapter	<i>Der Wallet-Adapter fügt optional eine Disclosure Policy an das Credential an, falls dies durch die fachlich zuständige Stelle angefordert wurde.</i>	<i>Funktionalität in erster Ausbaustufe der staatlichen EUDI-Wallet noch nicht unterstützt.</i>
10	Siegelung des Credentials	Wallet-Adapter	Der Wallet-Adapter erstellt auf Basis des im strukturierten Datensatz referenzierten Nachweisschemas das Credential und erstellt einen Hash-Wert über das gesamte Credential. Unter Einbeziehung eines QTSP wird der Hash-Wert mit einem fortgeschrittenen Siegel versehen.	Vorab muss bereits eine Vereinbarung zwischen der beantragenden Stelle (z.B. LH Dresden, BMDS) und dem QTSP vorliegen. Auf dieser Basis erstellt der QTSP ein Zertifikat, welches dann im Namen der Stelle vorgehalten wird.
11	Ausstellung des Credentials in die EUDI-Wallet	Wallet-Adapter	Der Wallet-Adapter erzeugt das SD-JWT-VC (Credential) und übermittelt es an die EUDI-Wallet des Nutzens	
12	Präsentation des Credentials	EUDI-Wallet	Die EUDI-Wallet präsentiert dem Nutzenden das empfangene Credential.	



IV. Anhang: Prozessübersicht „Indirekte Anbindung an die EUDI-Wallet“ am Beispiel BundID

Funktionalität 1: Sichere Identifizierung von Nutzenden mit der EUDI-Wallet

Nr.	Prozessschritt	Rolle	Beschreibung	Voraussetzung/ Anmerkung
1	Service Auswahl	Nutzender	Der Nutzende ruft die Webseite des Onlinediensts auf, wählt den gewünschten Service aus und startet den Identifizierungs-/ Authentifizierungsprozess. Der Onlinedienst leitet daraufhin die Datenanfrage als SAML-Request an die BundID.	Der Onlinedienst ist an die BundID angebunden. Die BundID (bzw. das BMDS als fachverantwortliche Stelle) ist als Relying Party registriert. Keine Anpassungen an bestehender SAML-Schnittstelle zur BundID nötig. Perspektivische Erweiterung der bestehenden Schnittstellen um OpenID Connect sehr wahrscheinlich, um die Anfrage weiterer Daten der PID (datensparsamen Altersverifikation, andere Nachweise) über die BundID zu ermöglichen.
2	Auswahl Identifizierungs- / Authentifizierungsmittel	Nutzender	Der Nutzende wird auf die Landing Page der BundID weitergeleitet und wählt dort die EUDI-Wallet als Ident./Auth. Methode aus.	
3	Erstellung Authorization Request	BundID IdP	Die BundID: • erstellt eine Authorization Request gemäß OpenID4VP-Standard • fügt das eigene Zugriffs- und Registrierungs-zertifikat an den Request hinzu • signiert die Authorization Request-Daten mit dem eigenen privaten Schlüssel	Referenzen: EU 2025/848 Annex IV nr. 3 k (Zugriffszertifikat) & Annex V nr. 3 j (Registrierungszertifikat) OpenID4VP: OpenID Digital Credentials Protocols Working Group (Credential=technischer Begriff für Nachweis). (2025, 17. August). <i>OpenID for Verifiable Presentations 1.0. (Final Status).</i> OpenID Foundation. OpenID for Verifiable Presentations 1.0;
4	Bereitstellung Authorization	BundID IdP	BundID stellt die Authorization Request für die EUDI-Wallet bereit. Dem Nutzenden wird in der 1.	Referenz: OpenID4VP: OpenID Digital Credentials Protocols Working Group. (2025, 17.



	Request durch Link/QR Code		Ausbaustufe ein Link bereitgestellt (siehe Hinweis). Der Nutzende klickt im Same-Device-Flow auf den Link. Durch das im Link angegebene Protokoll (bspw.: openid4vp oder Haip-vp) kann der Browser die Auswahl der zu verwendenden EUDI-Wallet über die entsprechende API durch den Nutzenden triggern.	August). <i>OpenID for Verifiable Presentations 1.0. (Final Status)</i>. OpenID Foundation. OpenID for Verifiable Presentations 1.0; Hinweis: Die Nutzung von Cross-Device-Flows (über mehrere Endgeräte) ist aufgrund aktueller fehlender technischer Voraussetzungen zur Absicherung des notwendigen hohen Vertrauensniveaus (LoA High) nicht von BSI empfohlen und für eine spätere Ausbaustufe vorgesehen
5	Verifizierung des Authorization Requests	EUDI-Wallet	Die EUDI-Wallet wird auf dem Endgerät gestartet, der Nutzende authentifiziert sich mit einem EUDI-Wallet Authentifizierungsverfahren (z. B. PIN, biometrisch). Die EUDI-Wallet ruft die Authorization Request vom Endpunkt ab. Die EUDI-Wallet prüft die Echtheit der Anfrage, informiert den Nutzenden über das Prüfergebnis und zeigt an, welche Daten von wem angefragt werden.	
6	Prüfung und Freigabe der PID	Nutzender	Der Nutzende prüft die angeforderten PID-Attribute und gibt seine Zustimmung zur Freigabe der ausgewählten PID-Attribute.	IETF OAuth Working Group. (2024, 8. Juli). <i>Selective Disclosure for JWTs (SD-JWT VC) – draft-ietf-oauth-sd-jwt-vc-15</i>. IETF. SD-JWT-based Verifiable Credentials (SD-JWT-VC)
7	Präsentation der PID	EUDI-Wallet	Die EUDI-Wallet erstellt eine Authorization Response mit den genehmigten PID-Attributen (SD-JWT-VC) und sendet diese an die BundID.	Referenzen: ARF v.3.0.0 (e.g. 6.6.3.6 Relying Party Instance verifies the authenticity of the PID or attestation)
8	Validierung der PID	BundID IdP	Die BundID prüft die empfangene PID-Attestation	Referenzen: PID-Verifizierung eIDAS-VO 910/2014 Art. 5a https://bmi.usercontent.open code.de/eudi-wallet/developer-guide/rp/guide/presentation/



				pid_presentation/#response-validation-checklist
9	Abgleich der PID-Response mit den Stammdaten (nur bei bestehendem BundID Konto)	BundID IdP	Die BundID: • gleicht die erhaltenen PID-Daten mit den eigenen Stammdaten ab • fügt optional das Postfach Handle an die Response an • schickt die eigenen Stammdaten als SAML Response an den Onlinedienst der fachlich zuständigen Stelle zurück	Die BundID schickt nicht die PID-Response an die fachlich zuständige Stelle. Die BundID nutzt stattdessen die PID, um sie mit den eigenen Stammdaten abzugleichen. Die fachlich zuständigen Stellen erhalten weiterhin die Stammdaten als SAML-Response. Hinweis: Wird ein Gastzugang verwendet, kann kein Stammdatenabgleich durchgeführt werden. In diesem Fall greift die bestehende Logik des Gastzugangs und es werden je nach gewähltem Zugangsmittel die Daten für den Online-Antrag übernommen, welche der Nutzende für die Identifizierung verwendet hat.
10	Prüfung und Freigabe der Daten	Online-dienst / fachl. zuständige Stelle	Der Onlinedienst der fachlich zuständigen Stelle erhält die geprüften Daten und prüft, ob die Daten der nutzenden Person zu der Session gehören, Optional kann der Onlinedienst dem Nutzenden die Response präsentieren und zur Vorausfüllung z.B. eines Onlineformulars im Rahmen einer Antragsstellung nutzen. Personendaten, welche aus der PID übernommen wurden, können nicht bearbeitet werden. Der Nutzende kann allerdings ergänzende Informationen, wie Emailadresse oder Telefonnummer ergänzen und die Inhalte noch einmal prüfen. Anschließend werden die Daten zur weiteren Verarbeitung für das Antragsverfahren freigegeben.	Wird die Ident./Authentifizierung als Teil eines Antragsprozesses durchgeführt, können die übermittelten Stammdaten zur Vorausfüllung des Onlineformulars des Onlinedienstes verwendet werden. Dabei muss klar nachvollziehbar sein, welche Felder aus den Stammdaten der BundID stammen.



11	Erfolgreiche Ident./Authentifizierung des Nutzenden	Online-dienst	Ist der Prozess erfolgreich, ist der Nutzende für die Nutzung des Services authentifiziert.	
----	---	---------------	---	--

Funktionalität 2: Ausstellung von Nachweisen aus dem BundID ZBP in die EUDI-Wallet

Nr.	Prozessschritt	Rolle	Beschreibung	Voraussetzung/ Anmerkung
0	Vorbedingung	Nutzender	Der/die Nutzende hat bei der fachlich zuständigen Stelle/Onlinedienst einen Prozess durchlaufen, welcher sie/ihn zum Abruf eines Nachweises berechtigt.	z.B. wurde ein Antragsprozess durchlaufen, auf den die Ausstellung eines Nachweises folgt.
1	Ausstellung des Nachweises in das Zentrale Bürgerpostfach (ZBP)	Fachlich zuständige Stelle	Die fachlich zuständige Stelle erstellt einen Nachweis (z.B. Dresden-Pass), welcher von einem Nutzenden zuvor beantragt wurde. Die für den Nachweis notwendigen strukturierten Daten werden als strukturierter Datensatz im JSON-Format von der fachlich zuständigen Stelle an das ZBP übermittelt.	Daten werden in hybridem Format menschen- und maschinenlesbar bereitgestellt: JSON + PDF/A inkl. Metadaten und in korrektem Nachweisschema. Für dezentrale kommunale Datenbestände (z.B. Dresden-Pass), muss jede fachlich zuständige Stelle die Bereitstellung der Daten in strukturierter Form selbstständig ermöglichen. Dies kann in Abstimmung mit Dienstleistern erfolgen, welche in bestimmten Fällen bereits die Daten für die aktuelle Nachweiserstellung aufbereiten.
2	Anmeldung im ZBP	Nutzender	Der Nutzende ruft das ZBP auf und authentifiziert sich mit einem BundID Authentifizierungsverfahren.	Die neue ZBP-Schnittstelle zur Bereitstellung strukturierter Daten in JSON, inkl. Metadaten muss integriert werden. Das ZBP stellt verschiedene Login-Optionen mit unterschiedlichen Vertrauensniveaus bereit: • eID, EUDI-Wallet (= hoch), • ELSTER (= substanziell) • Name + Passwort (= Basis)



3	Ausstellung des Nachweises in die EUDI-Wallet	Nutzender	Dem Nutzenden wird die Möglichkeit bereitgestellt, sich einen Nachweis aus dem ZBP als EAA (SD-JWT VC (Credential)) in die EUDI-Wallet ausstellen zu lassen.	Das ZBP stellt ein UI-Element bereit, über das der Nutzende die Ausstellung anstoßen kann. Z.B. ein Button "In meine EUDI-Wallet ausstellen" oder eine sinngemäße Option. Für die technische Transformation in standardisierte sowie gesiegelte Nachweisformate erfolgt eine kontrollierte Verarbeitung strukturierter Daten innerhalb der bestehenden gesicherten Infrastruktur. Die Daten verlassen die vielfach abgesicherte Infrastruktur des ITZBunds an dieser Stelle nicht. Zudem ist die gesamte Postfachkommunikation wie gehabt über die Netze des Bundes abgesichert.
4	Erstellung der Credential Offer	BundID als techn. Komponente eines EAA-Providers	Die BundID, als techn. Komponente eines EAA-Providers, ruft die strukturierten Daten aus dem ZBP ab und erzeugt ein Credential Offer gemäß OpenID4VCI-Protokoll.	Aktuell wird davon ausgegangen, dass das BMDS als EAA-Provider agiert und die BundID/das ZBP als technische Ausstellungs-Komponente fungiert. Referenz: OpenID4VCI: OpenID Digital Credentials Protocols Working Group. (2025, 16. September). <i>OpenID for Verifiable Credential Issuance 1.0 (Final Status)</i>. OpenID Foundation. <u>OpenID for Verifiable Credential Issuance 1.0</u>
5	Bereitstellung der Credential Offer	BundID als techn. Komponente eines EAA-Providers	Die BundID zeigt dem Nutzenden in der ersten Ausbaustufe einen Link an. Im Same-Device-Flow klickt der Nutzende auf den Link. Durch das im Link angegebene Protokoll (bspw.: OpenID4VCI oder Haip-vci) kann der Browser die Auswahl der zu verwendenden EUDI-Wallet über die entsprechende API durch den Nutzenden triggern.	Referenz: OpenID4VCI: OpenID Digital Credentials Protocols Working Group. (2025, 16. September). <i>OpenID for Verifiable Credential Issuance 1.0 (Final Status)</i>. OpenID Foundation. <u>OpenID for Verifiable Credential Issuance 1.0</u> Der Cross-Device Flow wird zu einer späteren Ausbaustufe unterstützt; Im Cross-Device-Flow scannt der Nutzende den QR-Code mit seinem



				Handy ab, um die Wallet-Auswahl zu starten.
6	Verifizierung der Credential Offer	EUDI-Wallet	Die EUDI-Wallet wird auf dem Endgerät gestartet, der Nutzende authentifiziert sich mit einem EUDI-Wallet Authentifizierungsverfahren (z. B. PIN, biometrisch). Die EUDI-Wallet ruft die Credential Issuer's Metadaten vom bereitgestellten Endpunkt ab. Die EUDI-Wallet prüft die Echtheit der Anfrage und informiert den Nutzenden über das Prüfergebnis. Der Nutzende akzeptiert das ihm angebotene Credential.	Die Credential Issuer's Metadaten beinhalten: - Technische Informationen über den Aussteller - Übersetzungs- und Visualisierungsinformationen für das auszustellende Credential
7	Erstellung des Credential Request	EUDI-Wallet	Die EUDI-Wallet erstellt den Credential Request gemäß OpenID4VCI-Standard und übermittelt die Credential Request an die BundID.	Referenz: OpenID4VCI: OpenID Digital Credentials Protocols Working Group. (2025, 16. September). <i>OpenID for Verifiable Credential Issuance 1.0 (Final Status)</i>. OpenID Foundation. <u>OpenID for Verifiable Credential Issuance 1.0</u>
8	Verifizierung des Credential Requests	BundID als techn. Komponente eines EAA-Providers	Die BundID prüft die Gültigkeit der EUDI-Wallet Instanz, des EUDI-Wallet Providers sowie weitere Eigenschaften der EUDI-Wallet. •	IETF OAuth Working Group. (2024, 8. Juli). <i>Selective Disclosure for JWTs (SD-JWT-VC) – draft-ietf-oauth-sd-jwt-vc-15</i>. IETF. <u>SD-JWT-based Verifiable Credentials (SD-JWT-VC)</u>
9	Anfügen einer Disclosure Policy	BundID als techn. Komponente eines EAA-Providers	<i>Die BundID fügt optional eine Disclosure Policy an das Credential an, falls dies durch die fachlich zuständige Stelle angefordert wurde.</i>	<i>Funktionalität in erster Ausbaustufe der staatlichen EUDI-Wallet noch nicht unterstützt.</i>
10	Siegelung des Credentials	BundID als techn. Komponente eines EAA-Providers	Die BundID erstellt auf Basis des im strukturierten Datensatz referenzierten Nachweisschemas das Credential und erstellt einen Hash-Wert über das gesamte Credential.	Vorab muss bereits eine Vereinbarung zwischen der beantragenden Stelle (BMDS) und dem QTSP vorliegen. Auf dieser Basis erstellt der QTSP ein entsprechendes Siegel-Zertifikat, welches



			Unter Einbeziehung eines QTSP wird der Hash-Wert mit einem fortgeschrittenen Siegel versehen (Hinweis: QTSPs erhalten keinen Zugriff auf die Inhaltsdaten des EAAs.)	dann im Namen des BMDS vorgehalten wird.
11	Ausstellung des Credentials in die EUDI-Wallet	BundID als techn. Komponente eines EAA-Providerks	Die BundID erzeugt das SD-JWT VC (Credential) und übermittelt es an die EUDI-Wallet des Nutzenden.	
12	Präsentation des Credentials	EUDI-Wallet	Die EUDI-Wallet präsentiert dem Nutzenden das empfangene Credential. Der Nutzende stimmt der Speicherung zu, woraufhin die EUDI-Wallet das Credential abspeichert.	

V. Anhang: Entscheidungsleitfaden zur Auswahl der Anbindungsoption

Frage 1: Gibt es bereits eine Landesstrategie oder zentrale Plattform zur EUDI-Wallet Anbindung?

- **Ja** → Die vorgegebene Landesstrategie, zentrale Plattform oder bestehende föderale Infrastruktur sollte vorrangig genutzt und an die EUDI-Wallet angebunden werden.
 - Ergebnis: **Zentrale Anbindung über föderale Infrastrukturen** oder vorgegebene Zielarchitektur.
- **Nein** → Weiter mit Frage 2.

Frage 2: Verlangt das digitale Verfahren aktuell eine Identifizierung oder Authentifizierung?

- **Ja** → Die EUDI-Wallet muss als Identifizierungs- und Authentifizierungsmittel berücksichtigt werden. Weiter mit Frage 3.
- **Nein** → Weiter mit Frage 5.

Frage 3: Besteht bereits eine BundID-Anbindung oder soll kurzfristig Rechtskonformität hergestellt werden?

- **Ja** →
 - Empfehlung: **Indirekte Anbindung an die EUDI-Wallet über die BundID**
 - insbesondere bei:



- bestehenden BundID-Anbindungen
- begrenzten Ressourcen
- kurzfristigem Umsetzungsbedarf

→ Weiter mit Frage 4.

- **Nein** → Weiter mit Frage 4.

Frage 4: Handelt es sich um ein digital reifes Verfahren mit hohem Automatisierungs- oder Nachnutzungspotenzial (z. B. EfA-Dienst, Landesportal, zentrale Plattform)?

- **Ja**
 - Empfehlung: **Direkte Anbindung an die EUDI-Wallet**
 - ggf. unter Nutzung eines Wallet-Adapters.
- **Nein**
 - Empfehlung: **Indirekte Anbindung über BundID oder bestehende Plattformen**

Frage 5: Soll das Verfahren Nachweise in die EUDI-Wallet ausstellen?

- **Nein** → Weiter mit Frage 8.
- **Ja** → Weiter mit Frage 6.

Frage 6: Ist neben der Nachweisausstellung auch eine Bescheidzustellung erforderlich?

- **Ja**
 - Empfehlung: **Indirekte Anbindung über BundID / ZBP**
 - da das ZBP zusätzlich die rechtssichere Zustellung von Bescheiden ermöglicht.
- **Nein** → Weiter mit Frage 7.

Frage 7: Liegen die zugrundeliegenden Daten bereits in Registern vor oder sollen perspektivisch über NOOTS bereitgestellt werden und benötigen kein Antragsverfahren?

- **Ja**
 - Empfehlung: **NOOTS-basierte Nachweisausstellung**
 - Insbesondere für:
 - Wohnsitznachweise



- Ausbildungsnachweise
- Steuerliche Basisnachweise
- Sonstige registerbasierte Nachweise
- **Nein**
 - Empfehlung: **Direkte Anbindung an die EUDI-Wallet**
 - bzw. Ausstellung über zentrale Issuing-Dienste (u.a. ZAP).

Frage 8: Verfügt die zuständige Stelle über ausreichende fachliche, technische und organisatorische Ressourcen für Betrieb und Weiterentwicklung einer eigenen EUDI-Wallet Anbindung?

- **Nein** →
 - Empfehlung: **Indirekte Anbindung über BundID / ZBP**
- **Ja**
 - Empfehlung: **Direkte Anbindung an die EUDI-Wallet**
 - bzw. Ausstellung über zentrale Issuing-Dienste (u.a. ZAP).

Frage 9: Müssen Bürgerinnen und Bürger heute Nachweise für das Verfahren einreichen?

- **Nein**
 - Für die Nachweisentgegennahme ist keine zusätzliche EUDI-Wallet Anbindung erforderlich.
- **Ja** → Weiter mit Frage 10.

Frage 10: Soll die Prüfung dieser Nachweise medienbruchfrei und automatisiert erfolgen?

- **Ja**
 - Empfehlung: **Direkte Anbindung an die EUDI-Wallet**
 - zur strukturierten Entgegennahme und automatisierten Prüfung von Nachweisen.
- **Nein**
 - Indirekte Anbindung ausreichend.



Frage 11: Werden für das Verfahren mehrere Anbindungswege benötigt?

Beispiele:

- BundID für Identifizierung
- ZBP für Bescheidzustellung
- NOOTS für Registerabruf
- Direkte Wallet-Anbindung für Nachweisprüfung

→ Empfehlung: **Hybrides Anbindungsmodell**



VI. Anhang: Gegenüberstellung Anbindungsoptionen

Dimension	Zentrale Anbindung über die BundID (Indirekte Anbindung)	Direkte Anbindung an die EUDI-Wallet mit Wallet-Adapter	Direkte Anbindung an die EUDI-Wallet ohne Wallet-Adapter
Technisch	- Schnittstellennutzung reduziert Integrationsaufwand aufgrund Nachnutzung BundID - Sicherheitsinfrastruktur senkt techn. Risiken aufgrund bestehender BundID-Mechanismen (Postfachhandling, rechtl. Absicherung) - Systemkopplung erhöht Abhängigkeit; BundID-Updates betreffen angebundene Dienste - Interoperabilität bleibt eingeschränkt, da BundID unterstützte Prozesse vorgibt - Nutzende müssen ein BundID-Konto besitzen - Hohe Komplexität, wenn gleichzeitig die Rolle als Aussteller und als Empfänger von Daten	+ Anbindung mit Wallet-Adapter erhöht Usability; weniger Systemwechsel nötig + Wallet-Adapter erleichtert Anbindung an die EUDI-Wallet und reduziert Eigenentwicklungsaufwände - Integrationsaufwand durch Zusatzkomponente, inkl. Adapter-Anbindung & Datenanpassungen - Techn. Zusatzkomponente Adapter erhöht Komplexität, Adapter-Betrieb, Überwachung und Sicherung - Zentral betriebener Adapter schafft "Single Point of Failure" für Datenschutz und Datensicherheit; theoretisch zentrale Überwachung von scheinbar dezentralen Nutzeraktionen möglich	- Direktintegration hat die beste Usability; weniger zusätzliche Systemwechsel und Redirects nötig - Optimale Anpassung an Fachverfahren (Nachnutzung weiterer Nachweise möglich; da keine Intermediäre) - Hoher initialer Aufwand für die Integration, Implementierung und Testing, inkl. neue SST, Validierung, Security-Mechanismen, Zertifikats-Handling - Betriebs- und Wartungsaufwände entstehen, z. B. Monitoring, Updates - Vollständige technische (Prüf-) Verantwortung liegt bei fachl. zuständiger Stelle



	eingegenommen werden soll - -		
Fachlich	+ Auswahl möglich aus versch. Ident-Prozessen der BundID (u. a. EUDI-Wallet) für Behörden (Ausweis, Elster, Nutzender/Passwort) + Stammdatenbereitstellung unterstützt bestehende Fachlogiken, z. B. via SAML Response - Gestaltungsspielraum bleibt begrenzt, da BundID Prozesse vorgibt - Roadmap-Priorisierung steuert Feature-Inhalte, da BundID fachl. Erweiterungen selektiert	+ Adapterkonfiguration steuert Umsetzung flexibler, mögliche Anpassungen an Fachprozesse + Adapterintegration ermöglicht einfache Kommunikation zur EUDI-Wallet (Präsentation, Validierung & Ausstellung) - Klare Governance zwischen Adapter-Betreiber und Fachressorts nötig für fachprozessspezifische Anforderungen	+ Fachstellen steuern Umsetzung flexibel, präzise Anpassungen an Fachprozesse (selektive Attributsfreigabe) + Direktintegration ermöglicht einfache Nutzung von künftigen EUDI-Funktionen
Organisatorisch	+ Zentrale Relying-Party reduziert Aufwand für einzelne Stellen (keine Einzelregistrierung für PID und Ausstellung über ZBP) + Betriebskosten sinken & Anbindung vereinfacht durch	+ Zentral betriebener Adapter erlaubt föderale Skaleneffekte (geteilte Infrastruktur Länder-Kommunen) + Langfristige Standardisierung reduziert Doppelstrukturen (z. B. nicht unzählige versch. Ident-Systeme nötig)	+ Direkte Relying-Party-Rolle stärkt Autonomie, insb. bei größeren & strategischen Akteuren + Langfristige Standardisierung reduziert Doppelstrukturen (z. B. nicht unzählige versch. Ident-Systeme nötig)



	Nutzung bestehender Infrastruktur, insb. für Kommunen - Releasezyklen begrenzen Handlungsspielraum durch zentrale BundID Roll-outs & Timings - Zentrale Governance mindert lokale Gestaltungsfreiheit, da BundID vorgelagert ist	- Adapter bringt organisatorische Pflichten mit, z. B. Betrieb, Weiterentwicklung, Zertifikate - Abhängigkeit von (zentralem) Adapter kann Autonomie & Fortschrittsfähigkeit verringern (z. B. Erweiterungswünsche Funktionalitäten)	- Organisatorische Pflichten der Direktanbindung erhöhen Last, z. B. Zertifikatsmanagement, Audits, Security, Konformitätsbewertung - Kleinere Stellen benötigen externe Unterstützung, da Ressourcen und Expertise fehlen
--	---	--	--

VII. Anhang: Gegenüberstellung Attribute der eID und nationaler PID

Hinweis: Im besten Fall übermittelt die BundID auf dem gewohnten Weg (SAML-Response) weiterhin den vollständigen, bislang bereitgestellten Datensatz auf Basis der von der EUDI-Wallet gelieferten PID. Der Datensatz der PID kann sich je nach PID-Provider bzw. EU-Mitgliedsland unterscheiden. Hinzu kommt, dass Nutzende der EUDI-Wallet immer die Möglichkeit besitzen, bei der Präsentation der Attribute nur eine Teilmenge der im Request geforderten Attribute an die BundID freizugeben (selektive Offenlegung). Die BundID wird stufenweise dahingehend weiterentwickelt, damit technisch umgehen zu können. Es kann allerdings sein, dass zu wenig Identifikationsdaten übermittelt werden, um die Verfahren erfolgreich zu durchlaufen. In diesem Fall muss ein anderes Identifikationsmittel verwendet werden. Für abgeleitete Vergleichsattribute wie die Alters- oder Wohnortprüfung (in der nachfolgenden Tabelle als „n/a“ markiert) sieht die Durchführungsverordnung (EU) 2024/2977 kein eigenes PID-Attribut vor; eine Bereitstellung über Selective Disclosure ist technisch denkbar, wird von der nationalen EUDI-Wallet nach aktuellem Stand jedoch nicht unterstützt.



Attribute aus § 18 Absatz 3 des Personalausweisgesetzes	DURCHFÜHRUNGSVERORDNUNG (EU) 2024/2977
Familienname	family_name (obligatorisch)
Geburtsname	family_name_birth (fakultativ)
n/a	given_name_birth (fakultativ)
Vornamen	given_name (obligatorisch)
Doktorgrad	n/a
Tag der Geburt	birth_date (obligatorisch)
Ort der Geburt	birth_place (obligatorisch)
Anschrift	resident_address (fakultativ)
n/a	resident_country (fakultativ)
n/a	resident_state (fakultativ)
n/a	resident_city (fakultativ)
n/a	resident_postal_code (fakultativ)
n/a	resident_street (fakultativ)
n/a	resident_house_number (fakultativ)
Laut amtlichen Gemeindeverzeichnis verwendeter eindeutiger Gemeindeschlüssel	n/a
n/a	issuing_authority (obligatorisch)



n/a	issuing_country (obligatorisch)
Abkürzung für die Staatsangehörigkeit	nationality (obligatorisch)
Dokumentenart	n/a
letzter Tag der Gültigkeitsdauer	expiry_date (obligatorisch)
dienste- und kartenspezifisches Kennzeichen	n/a
Abkürzung „D“ für Bundesrepublik Deutschland	issuing_jurisdiction (fakultativ)
Angabe, ob ein bestimmtes Alter über- oder unterschritten wird	n/a
Angabe, ob ein Wohnort dem abgefragten Wohnort entspricht	n/a
Ordensname, Künstlername	n/a
n/a	personal_administrative_number (fakultativ)
n/a	portrait (fakultativ)
n/a	sex (fakultativ)
n/a	email_address (fakultativ)
n/a	mobile_phone_number (fakultativ)
n/a	location_status (fakultativ)



VIII. Anhang: Anforderungen an die öffentliche Stelle bei BundID Anbindung

- Kurzfristige Erfüllung rechtl. Umsetzungsfrist zur Identifizierung/ Authentifizierung über die EUDI-Wallet:
 1. Falls der Weg der Anbindung an die EUDI-Wallet über die BundID gewählt wird, muss die Anbindung an die BundID vorgenommen werden, sofern noch keine Anbindung an die BundID besteht.
 2. Die öffentliche Stelle muss die ausgewählten Authentifizierungsmittel um das neue Zugangsmittel „eudi“ erweitern, sofern explizit einzelne Zugangsmittel ausgewählt wurden.
- Optional: Nachweisausstellung über das ZBP in die EUDI-Wallet:
 3. Es muss entschieden werden, welche Nachweise künftig digital in die EUDI-Wallet ausgestellt werden sollen.
 4. Die Anbindung an das ZBP muss via REST-Schnittstelle vorgenommen werden, sofern noch keine Anbindung an das ZBP besteht.
 5. Implementierung der entsprechenden Erweiterungen der ZBP-Schnittstellen muss erfolgen – detaillierte Informationen folgen zu gegebener Zeit mit der ZBP-Schnittstellen-Spezifikation.
 6. Für diese Nachweise muss die öffentliche Stelle
 - ein minimales Set an Attributen definieren (nur die zwingend erforderlichen Attributinformationen sowohl nach dem Datenminimierungsgrundsatz der DSGVO als auch aus der eIDAS-/EUDI-Logik der selektiven Offenlegung)
 - die Semantik sowie die Metadaten der Nachweise abstimmen und festlegen.
 7. Bestimmte Informationen müssen dazu zukünftig in das BundID SSP eingepflegt werden. Weitere Informationen folgen zu gegebener Zeit.
 8. Unstrukturierte Informationen müssen in strukturierte Daten (maschinenlesbar, JSON) überführt werden.
 9. Die öffentliche Stelle muss eine Berechtigung an das BMDS zur Ausstellung von Nachweisen durch die BundID im Namen der öffentlichen Stelle vrs. über das SSP der BundID erteilen.
 10. Die Beantragung von Registrierungszertifikaten muss über das SSP der BundID erfolgen.

IX. Anhang: Kriterien zur Nachweispriorisierung

Auszug aus relevanten Kriterien für die Entscheidung zur Umsetzung eines Verwaltungsnachweises in der EUDI-Wallet:



- **Rechtliche Machbarkeit**

Bestehende rechtliche Zulässigkeit der digitalen Ausstellung sowie Umfang möglicher Rechtsänderungen. Nachweise mit geringem Anpassungsbedarf können schneller umgesetzt werden.

- **Gesellschaftliche Relevanz und Betroffenenzahl**

Anzahl der Bürgerinnen und Bürger, die einen Nachweis besitzen, benötigen oder regelmäßig verwenden. Nachweise mit hoher Reichweite schaffen frühzeitig einen spürbaren Mehrwert für breite Nutzergruppen.

- **Verbreitung in Verwaltungsverfahren (Nachnutzung)**

Anzahl der Verwaltungsleistungen, in denen ein Nachweis heute vorgelegt werden muss. Nachweise, die in vielen Verfahren benötigt werden, ermöglichen besonders hohe Effizienzgewinne und Wiederverwendungseffekte.

- **Nachweisintensität und heutiger Medienbruch**

Umfang der heutigen manuellen Prüfung, papiergebundenen Bearbeitung und Nachweisanforderungen. Besonders geeignet sind Nachweise, die häufig eingereicht, geprüft oder erneut angefordert werden.

- **Organisatorische Umsetzbarkeit**

Verfügbarkeit der erforderlichen Daten, Registeranbindung, Anzahl beteiligter Stellen sowie bestehende Abhängigkeiten von weiteren Nachweisen oder Vorbedingungen.

- **Technische Wallet-Readiness**

Digitalisierungsgrad der Nachweise, Strukturierungsgrad der Daten sowie vorhandene Register- und Systemlandschaften. Bereits strukturierte oder registergestützte Nachweise eignen sich typischerweise besser für eine frühe Umsetzung.

- **Bundesweite Nachnutzbarkeit und EfA-Potenzial**

Möglichkeit, entwickelte Lösungen über Länder- und Kommunalgrenzen hinweg wiederzuverwenden und Skaleneffekte zu erzielen. Verfahren mit hoher Nachnutzbarkeit sollten bevorzugt betrachtet werden.

- **Relevanz über die Verwaltung hinaus**

Bedeutung eines Nachweises in privatwirtschaftlichen Prozessen, beispielsweise gegenüber Arbeitgebern, Banken, Versicherungen oder Bildungseinrichtungen. Nachweise mit hoher Verwendung in Verwaltung und Wirtschaft können zusätzliche Mehrwerte entfalten.

Stammen die Nachweise aus der Privatwirtschaft, ist zu bewerten, ob die Bereitstellung über die EUDI-Wallet einen ausreichenden Mehrwert gegenüber bestehenden Verfahren bietet oder ob Fachgesetze und laufende Vorhaben bereits andere Lösungswege vorsehen. So sieht das Bundesmeldegesetz bei der elektronischen Wohnsitzanmeldung vor, dass Vermieter die Daten unmittelbar bei der Meldebehörde bestätigen und ein Zuordnungsmerkmal erhalten; alternativ käme die Ausstellung einer



Wohnungsgeberbestätigung durch den Vermieter in die EUDI-Wallet in Betracht, was die Erfüllung der EAA-Provider Anforderungen voraussetzt. In diesen Fällen empfiehlt sich eine Meldung an das BMDS und die SPRIND, um die Use-Case-Planung abzustimmen.