IT-PLANUNGSRAT

Berlin
17.06.2026

Verwaltungs-anbindung EUDI-Wallet

Konzept zum Zielbild und Umsetzungsoptionen für die öffentliche Verwaltung an die EUDI-Wallet

BMDS | DS II 7

Inhaltsverzeichnis

Management Summary

Die eIDAS-Verordnung (EU) 2024/1183 verpflichtet alle EU-Mitgliedstaaten, bis spätestens 24.12.2026 eine staatlich anerkannte European Digital Identity Wallet (EUDI-Wallet) bereitzustellen; die Nutzung durch Bürgerinnen und Bürger ist freiwillig. Mit dem Go-Live der staatlichen EUDI-Wallet im Januar 2027 müssen öffentliche Stellen die EUDI-Wallet in digitalen Verwaltungsverfahren als Identifizierungs- und Authentifizierungsmittel akzeptieren, sofern in den jeweiligen Diensten eine starke Nutzerauthentifizierung erforderlich ist. Eine Verpflichtung für die Verwaltung zur Ausstellung oder Entgegennahme von Nachweisen der EUDI-Wallet besteht hingegen nicht. Vor diesem rechtlichen Hintergrund beschreibt das vorliegende Konzept das Zielbild, wie die EUDI-Wallet in Verwaltungsverfahren eingebunden werden kann. Es verfolgt einen zweistufigen Ansatz, der kurzfristig die fristgerechte Erfüllung der Mindestanforderungen sicherstellt und mittel- bis langfristig ein integriertes Zielbild mit direkter Verwaltungsanbindung etabliert. Eine native Einbindung der EUDI-Wallet wird perspektivisch präferiert, da je nach Verwaltungsverfahren zusätzliche Automatisierungs- oder Prozessvorteile durch eine direkte Integration der EUDI-Wallet entstehen. Voraussetzung sind dafür unter anderem die technische Befähigung von Onlinediensten und Fachverfahren.

Kurzfristig wird die rechtskonforme Identifizierung und Authentifizierung über die EUDI-Wallet durch die weiterentwickelte BundID sichergestellt, die geplant ab dem Januar 2027 eine indirekte Anbindung an die EUDI-Wallet für angeschlossene Dienste ermöglicht. Ergänzend können ausgewählte Verwaltungsnachweise über das ZBP in die EUDI-Wallet ausgestellt werden. Diese Lösungen werden derzeit mit der Landeshauptstadt Dresden und der Sächsischen Staatskanzlei pilotiert und bundesweit nachnutzbar ausgestaltet. Die BundID erfüllt die Anforderungen des OZG und bleibt für Verfahren mit rechtssicherer Bescheidzustellung sowie bidirektionaler Kommunikation bestehen, da die EUDI-Wallet kein Verwaltungs- oder Zustellpostfach ersetzt.

Zur direkten Anbindung an die EUDI-Wallet geht das Konzept auf die Vorhaben des Bundes zur Sicherstellung des mittel- bis langfristigen Zielbildes ein. Durch den Bund wird ein Produkt des IT-Planungsrates zum Wallet-Adapter weiterentwickelt und voraussichtlich bis Januar 2027 als modulare Softwarekomponente bereitgestellt. Dieser Wallet-Adapter wird zur Erleichterung der direkten Anbindung bereitgestellt. Die Verantwortung für die technische Weiterentwicklung für spezifische Verwaltungsverfahren sowie für den Betrieb liegen bei den Ländern bzw.

den jeweils fachlich zuständigen Stellen. Dieser Wallet-Adapter wird zur Ermöglichung des Abrufs von Nachweisen aus Registern über die NOOTS-Infrastruktur in die EUDI-Wallet nachgenutzt, zum NOOTS-spezifischen Issuing-Dienst weiterentwickelt und produktiv eingesetzt. In Zusammenarbeit mit der FITKO und BVA wird ein MVP umgesetzt, das insbesondere für sektorübergreifende Prozesse zwischen Verwaltung und Privatwirtschaft geeignet ist.
Insgesamt schafft das Konzept einen Rahmen für die schrittweise Einbindung der EUDI-Wallet in Verwaltungsverfahren unter Betrachtung unterschiedlicher Anbindungsoptionen sowie Anforderungen an öffentliche Stellen. Es beschreibt das Zielbild, um eine weitgehende Nutzung der EUDI-Wallet für die öffentliche Verwaltung sicherzustellen und so den Weg für eine zukunftsfähige digitale Verwaltung zu ebnen.

1 Einleitung und Kontext

Die eIDAS-Verordnung (EU) Nr. 910/2014, zuletzt geändert durch 2024/1183 (eIDAS-VO) schafft einen verbindlichen Rahmen für ein interoperables digitales Identitätsökosystem mit der EUDI-Wallet im Zentrum. Die EUDI-Wallet als zentrales Element ermöglicht es Bürgerinnen und Bürgern, Identitätsdaten sowie weitere Nachweise digital, sicher, sektorübergreifend und EU-weit zu nutzen. Damit kann der Einsatz der EUDI-Wallet vor allem auch Verwaltungsprozesse effizienter, medienbruchfrei und nutzendenzentrierter gestalten.
Das vorliegende Dokument geht darauf ein, wie die EUDI-Wallet mehrwertstiftend für die öffentliche Verwaltung nutzbar gemacht werden kann und welche Verpflichtungen sich für öffentliche Stellen laut der eIDAS-VO ergeben. Es basiert auf den aktuellen Erkenntnissen des Bundesministeriums für Digitales und Staatsmodernisierung (BMDS), welche im Rahmen der nationalen Umsetzung der eIDAS-VO gesammelt wurden. Im Folgenden werden verschiedene Umsetzungsoptionen vorgestellt und bewertet, die aufzeigen, wie die Anforderungen der eIDAS-VO zentral oder dezentral von der öffentlichen Verwaltung erfüllt werden können.
Der Bund, insbesondere das BMDS, unterstützt diesen Transformationsprozess durch die Bereitstellung zentraler Infrastrukturkomponenten und übergreifender Orientierung, während die konkrete fachliche und technische Umsetzung in der Verantwortung der Länder und Kommunen sowie der Bundesverwaltung liegt. Eine enge Zusammenarbeit ist somit zentral.

1.1 EUDI-Wallet

Bis zum 24.12.2026 sind alle Mitgliedstaaten verpflichtet, eine staatlich anerkannte EUDI-Wallet bereitzustellen. Diese ermöglicht es den Nutzenden, insbesondere ihre Personenidentifikationsdaten zum Zweck der Identifikation und Authentifizierung und digitale Nachweise (laut eIDAS-VO werden Nachweise auch als „elektronische Attributsbescheinigungen" bezeichnet) sicher anzufordern, zu erhalten, zu speichern, auszuwählen, zu kombinieren und weiterzugeben (vgl. Art. 5a Abs. 4 lit. a eIDAS-VO Nr. 910/2014). Diese digitalen Nachweise sind etwa der Führerschein, Hochschul- und Ausbildungsnachweise, Vereins- oder Mitgliedschaftsbestätigungen sowie Tickets. Diese Attributsbescheinigungen enthalten Attribute, die u.a. aus authentischen Quellen wie Registern, Hochschulverwaltungen oder anderen fachlichen Datenbeständen stammen, welche Merkmale einer Person in strukturierter Form bestätigen, und sind nicht automatisch mit Bescheiden gemäß §35 VwVfG gleichzusetzen. Die EUDI-Wallet ist kein Postfach für rechtssichere Bescheidzustellung und eine bidirektionale Kommunikation, wie beispielsweise das ZBP der BundID.

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

Die EUDI-Wallet ist sowohl für Remote-Interaktionen über Onlineanwendungen als auch für Vor-Ort-Situationen im Sinne des Proximity-Sharing ausgelegt. Proximity-Sharing ermöglicht dabei einfache Vor-Ort-Nachweisprüfungen, etwa wenn im Supermarkt ein Altersnachweis direkt an der Kasse über das Scannen eines QR-Codes bestätigt wird. Ebenso kann beim Museumseintritt ein auf der EUDI-Wallet gespeicherter Sozialpass vor Ort durch das Museum gescannt und bestätigt werden. Die staatliche EUDI-Wallet wird nur als App angeboten, um höchste Sicherheitsanforderungen zu erfüllen und Sicherheitsfunktionen des Smartphones verwenden zu können. Für die Nutzung wird daher ein Smartphone mit dem Betriebssystem iOS (Apple) oder Android (Google) benötigt. Die Bereitstellung einer browserbasierten EUDI-Wallet ist zum aktuellen Zeitpunkt nicht vorgesehen.

Kriterium	Präsenz-Verfahren (Vor-Ort / Proximity Flow)	Online-Verfahren (Remote Flow)
Art der Interaktion	Persönliche Interaktion vor Ort (Präsenzsituation)	Digitale Interaktion im Rahmen eines Online-Verfahrens
Zweck/Anwendungsfall	Direkte Vorlage von Nachweisen vor Ort, z. B. über NFC oder Bluetooth; eine Internetverbindung ist nicht zwingend erforderlich, z. B. bei Kontrollen sowie Zutritts- oder Berechtigungsprüfungen	Übermittlung von Nachweisen zur Weiterverarbeitung in Online-Anträgen, digitalen Verwaltungsleistungen und Fachverfahren

Tabelle 2: Abgrenzung der Nutzung der EUDI-Wallet in Präsenz und Online Verfahren

Die erste Version der EUDI-Wallet mit der Möglichkeit zur Nachweisverwaltung von einem Identitätsnachweis (PID; Person Identification Data) mit Identitätsdaten wie Name oder Geburtsdatum (vgl. German PID Rulebook[1]) und weiteren Nachweisen wird voraussichtlich bis zum Januar 2027 verfügbar sein. Weitere Funktionalitäten wie die Erstellung von QES (qualified electronic signatures) für Nutzenden der EUDI-Wallet und Zahlungsautorisierung werden ab 2027 sukzessive ergänzt. Öffentliche Stellen oder Organisationen (sogenannte Relying Parties) können Nachweise in der EUDI-Wallet anfordern, prüfen und nutzen.

Die eIDAS-VO verpflichtet öffentliche Stellen bis zum 24.12.2026 dazu, die EUDI-Wallet als Identifizierungs- und Authentifizierungsmittel in digitalen Prozessen zu akzeptieren, sofern in den jeweiligen Diensten eine starke Nutzerauthentifizierung erforderlich ist (vgl. Art. 5f Abs. 1 eIDAS-VO 910/2014), welches mit einem Vertrauensniveau hoch gleichzusetzen ist. Eine Pflicht zur Ausstellung von Nachweisen in die EUDI-Wallet ergibt sich hingegen nicht. Genauso ist die Nutzung der EUDI-Wallet durch Bürgerinnen und Bürger freiwillig und nicht verpflichtend. Für die in Anhang VI der eIDAS-VO aufgeführten Attribute muss jeder Mitgliedstaat einen Verifikationsmechanismus (vgl. Kapitel 4) bereitstellen, der es Vertrauensdiensteanbietern ermöglicht, die fachliche Verifikation von Attributen gegenüber der jeweils zuständigen authentischen Quelle, das heißt Register oder Datenquellen wie Hochschulen oder Schulverwaltungen, zu prüfen (vgl. Art. 45e Abs. 1 eIDAS-VO Nr. 910/2014).

[1] https://bmi.usercontent.opencode.de/eudi-wallet/eidas-2.0-architekturkonzept/content/ecosystem-architecture/PID/german-pid-rulebook/

1.2 EUDI-Wallet-Ökosystem

Die EUDI-Wallet ist in ein europaweit einheitlich vorgegebenes Identitäts- und Nachweisökosystem eingebettet, das die technischen, organisatorischen und rechtlichen Grundlagen für das sichere Anfordern, Erhalten, Speichern, Auswählen, Kombinieren und Weitergeben (vgl. Art. 5a Abs. 4 eIDAS-VO Nr. 910/2014) digitaler Identitäts- und Attributsdaten definiert. Die funktionalen Rollen innerhalb des EUDI-Wallet-Ökosystems zum Nachweisaustausch im engeren Sinne sind klar abgegrenzt: Eine Relying Party kann Aussteller (Issuer), Prüfer (Verifier), oder beides sein. Als Aussteller ((Q/Pub-)EAA-Provider) stellt sie Nachweise mit den erforderlichen kryptografischen Sicherungen in Form von (qualifizierten) elektronischen Attributsbescheinigungen ((Q/Pub-)EAA) aus. In der Rolle des Verifiers prüfen Relying Parties die Authentizität und Gültigkeit dieser Nachweise. Die Rolle des Nachweisinhabers wird durch die EUDI-Wallet ausgeübt, in welcher die Nachweise gespeichert und bei Bedarf präsentiert werden.

Der Lebenszyklus eines Nachweises folgt einem durchgängigen Ablauf: Er beginnt bei der authentischen Quelle – wie Registern oder Datenbeständen, welche Attribute liefern, auf deren Grundlage verifizierbare Nachweise erzeugt werden –, führt über die Ausstellung und Siegelung/Signatur durch eine berechtigte Stelle zur Speicherung in der EUDI-Wallet und endet mit der selektiven Vorlage gegenüber einer Relying Party, die die Validität des Nachweises anhand gemeinsamer europäischer Vertrauensanker überprüft. Gemeinsame technische Grundlagen – darunter abgestimmte Zertifikatsanforderungen, Trust-Listen, Statusmechanismen und interoperable Protokolle zur Übertragung strukturierter Nachweisdaten – sichern die EU-weite Nutzbarkeit dieser Nachweise. Damit entsteht ein einheitliches Ökosystem, das die grenzüberschreitende Verwendung digitaler Identitäts- und Attributsdaten ermöglicht und zugleich die Basis für medienbruchfreie, moderne Verwaltungsprozesse schafft.

Der Begriff „EUDI-Wallet" bezeichnet im nachfolgenden Dokument sowohl EUDI-Wallet Lösungen verschiedener Anbieter bzw. Nationalstaaten als auch das gesamte EUDI-Wallet-Ökosystem einschließlich der zugehörigen Vertrauensinfrastruktur und weiterer Komponenten, da sich die Anbindung der Verwaltung nicht nur auf die EUDI-Wallet, sondern auf das gesamte EUDI-Wallet-Ökosystem bezieht.

1.3 Funktionalitäten der EUDI-Wallet

Die EUDI-Wallet eröffnet der öffentlichen Verwaltung vielfältige Einsatzmöglichkeiten, die über Identifizierung hinausgehen und wesentliche Bausteine eines modernen, interoperablen

digitalen Verwaltungshandelns darstellen. Die Nutzung der EUDI-Wallet kann den Aufwand für Identitäts- und Nachweisprüfungen deutlich reduzieren, da diese digital, medienbruchfrei und EU-weit interoperabel erfolgen. Darüber hinaus sinkt der administrative Aufwand für das manuelle Anfordern, Prüfen und Archivieren von Nachweisen, wodurch Ressourcen freigesetzt und die Servicequalität für Bürgerinnen und Bürger erhöht werden. Damit unterstützt die EUDI-Wallet sowohl die Automatisierung administrativer Prüfprozesse als auch die medienbruchfreie Umsetzung komplexer Verwaltungsverfahren.

Die Einsatzmöglichkeiten lassen sich in drei übergeordnete Anwendungsbereiche gliedern:

- Funktionalität 1: Sichere Identifizierung von Nutzenden mit der EUDI-Wallet
- Funktionalität 2: Ausstellung von Nachweisen in die EUDI-Wallet
- Funktionalität 3: Entgegennahme von Nachweisen aus der EUDI-Wallet

Nach aktuellem Planungsstand wird der Go-Live der EUDI-Wallet im Januar 2027 entsprechend der Regulatorik im EUDI-Wallet-Ökosystem zunächst nur Authentifizierungen auf hohem Vertrauensniveau bei Nutzung auf demselben Endgerät (same-device) ermöglichen, da hierfür bereits die technischen und sicherheitstechnischen Voraussetzungen für ein hohes Vertrauensniveau gemäß eIDAS-Verordnung vorliegen. Eine geräteübergreifende Nutzung (cross-device) wird erst in einer späteren Ausbaustufe möglich sein, sobald hierfür die notwendigen technischen Grundlagen zur Gewährleistung des hohen Vertrauensniveaus geschaffen sind.

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

Funktionalität 1 stellt eine verbindliche Anforderung im Sinne der eIDAS-Verordnung für digitale Antragsverfahren dar, bei denen eine Authentifizierung mit hohem Vertrauensniveau erforderlich ist. Dies impliziert jedoch keine Verpflichtung zur Akzeptanz der EUDI-Wallet in physischer Präsenz, also etwa zur Identifizierung vor Ort bei einer Verwaltungsstelle.

Nach Abschluss des nationalen Onboarding-Prozesses für die EUDI-Wallet, der derzeit durch das BMDS vorbereitet wird, verfügt der Nutzende über einen staatlich ausgestellten digitalen Identitätsnachweis in Form der PID, der in der EUDI-Wallet gespeichert ist. Die PID wird durch den PID-Provider (Bundesdruckerei) ausgestellt, kryptographisch für eine Identifizierung mit hohem Vertrauensniveau signiert. Im Rahmen eines Identifizierungs- oder Authentifizierungsvorgangs fordert eine Relying Party (Verifier) die für den jeweiligen Zweck erforderlichen PID über standardisierte Protokolle aus der Wallet an; dies erfolgt ausschließlich mit ausdrücklicher Zustimmung der nutzenden Person. Die Relying Party prüft anschließend die

Authentizität der PID, insbesondere durch die Validierung des Siegels sowie die Prüfung des Gültigkeits- und Widerrufsstatus. Nur bei gültiger und nicht widerrufener PID gilt die Identifizierung als erfolgreich und kann als rechtssichere Grundlage für die Fortführung des Verwaltungsprozesses dienen.

Funktionalität 2: Ausstellung von Nachweisen in die EUDI-Wallet

Die EUDI-Wallet dient als digitaler Nachweisordner, in dem behördlich bestätigte Attribute gespeichert werden können. Eine ausstellende Stelle tritt dabei als Relying Party (Issuer) auf, die verifizierbare Attributsbescheinigungen sicher in die EUDI-Wallet ausstellt. Mögliche Anwendungsfälle sind die Ausstellung eines digitalen Studierendenausweises durch eine Hochschule oder eines digitalen Gewerbescheins durch das Gewerbeamt.

Das Konzept orientiert sich an den aktuellen technischen Möglichkeiten der nationalen EUDI-Wallet und sieht zunächst eine issuer-initiierte Ausstellung vor, bei der der Nachweis bei der zuständigen öffentlichen Stelle beantragt und z. B. im Rahmen eines Online-Antragsverfahrens ausgestellt wird. Perspektivisch ist auch eine wallet-initiierte Ausstellung vorgesehen, bei der der gewünschte Nachweis direkt aus der EUDI-Wallet angefordert werden kann. Die Ausstellung in die EUDI-Wallet ist als ergänzendes Angebot zur bisherigen Ausstellung in eine Postfachlösung (z.B. dem ZBP der BundID) anzusehen und ersetzt nicht eine rechtssichere Zustellung von Bescheiden. Für die öffentliche Verwaltung bedeutet dies, dass Nachweise, die bislang häufig in Papierform oder als PDF ausgestellt werden, künftig digital, über strukturierte, gesiegelte und verifizierbare Datenformate (u. a. SD-JWT VC) in die EUDI-Wallet der Bürgerinnen und Bürger ausgegeben werden können. Eine kryptographische Siegelung ist notwendig zur Identifizierung des Issuers (sowie eine eindeutige Zuordnung zur fachlich zuständigen Stelle, falls diese nicht identisch ist) und stellt sicher, dass das signierte Dokument nachträglich nicht verändert wurde.

Für die 1. Ausbaustufe des EUDI-Wallet-Ökosystems ist die Ausstellung von Verwaltungsnachweisen als elektronische Attributsbescheinigungen (EAA) durch EAA-Provider vorgesehen. EAAs können von unterschiedlichen Stellen bereitgestellt werden und unterliegen nicht den Anforderungen von qualifizierten elektronischen Attributsbescheinigungen (QEAAs). Die Siegelung kann in diesem Fall durch einen nicht-qualifizierten Vertrauensdiensteanbieter (TSP) erfolgen. Dabei steht es dem EAA-Provider frei, eine Fernsiegelung durchführen zu lassen oder

sich die benötigten Dienste einzukaufen und in der eigenen Umgebung zu nutzen, um Nachweise selbst zu siegeln.
Für weitere Ausbaustufen ab 2027 ist die Ausstellung qualifizierter elektronischer Attributsbescheinigungen (QEAAs) durch qualifizierte Vertrauensdiensteanbieter (engl. QTSP) mit fortgeschrittener oder qualifizierter Siegelung vorgesehen (siehe Kapitel 4 „Nachweisausstellung und Verifikation“).

Funktionalität 3: Entgegennahme von Nachweisen aus der EUDI-Wallet
Die Funktionalität 3 beschreibt die Entgegennahme bzw. Präsentation der in der EUDI-Wallet gespeicherten Attributsbescheinigungen, die sowohl in Online-Verfahren gegenüber Onlinediensten bzw. Portalen als auch die vor Ort erfolgen kann.
Bei Online-Verfahren (Remote Flow) erfolgt die Entgegennahme vollständig digital. Der Onlinedienst stellt im Rahmen der Antragstellung eine technische Anfrage an die EUDI-Wallet der antragstellenden Person, in der definiert ist, welche Attributsbescheinigungen für das jeweilige Verfahren erforderlich sind. Die EUDI-Wallet prüft die Berechtigung des anfragenden Onlinedienstes als Relying Party, informiert die nutzende Person über Zweck und Umfang der Anfrage und holt deren Zustimmung ein. Nach Freigabe werden die benötigten Attributsbescheinigungen selektiv und zweckgebunden an den Onlinedienst übermittelt und für die weitere Bearbeitung des Antrags verwendet. Die Einbindung der Nachweise erfolgt dabei medienbruchfrei innerhalb des digitalen Verfahrens.
Alternativ können Nachweise auch im Rahmen einer Vor-Ort-Prüfung vorgezeigt werden, zum Beispiel bei einer Ticketkontrolle im Museum. In diesem Fall erfolgt das Präsentieren über einen QR-Code in der EUDI-Wallet gegenüber der Akzeptanzstelle (z.B. dem Museum) über einen sogenannten Proximity Flow – ähnlich wie beim Vorzeigen eines Flugtickets in einer Wallet am Flughafen. Die nutzende Person bestätigt die Anfrage direkt in ihrer EUDI-Wallet und gibt die erforderlichen Attribute frei. Die Übermittlung erfolgt unmittelbar und kontrolliert, ohne dass papierbasierte Nachweise oder Dateiuploads erforderlich sind. Diese öffentlichen Stellen müssen als Akzeptanzstellen für die EUDI-Wallet in der Lage sein, die in der EUDI-Wallet vorgezeigten Nachweise zu prüfen. Hierfür wird die Bereitstellung von Prüfkomponenten durch den Bund geprüft. Voraussichtlich soll im ersten Schritt hierfür eine Anwendung für mobile Endgeräte bereitgestellt werden. Dieses Dokument fokussiert sich im Rahmen der Verwaltungsanbindung auf den Online-Flow. Der Proximity-Flow und die damit verbundenen fachlichen,

organisatorischen sowie technischen Anforderungen an Akzeptanzstellen werden in diesem Konzept nicht genauer betrachtet.
Beide Varianten ermöglichen es der öffentlichen Verwaltung, bereits vorhandene und verifizierte digitale Nachweise effizient in Verwaltungsverfahren einzubinden. Während der Online-Flow insbesondere für vollständig digitale Services geeignet ist, unterstützt der Proximity-Flow eine medienbruchfreie Nutzung der EUDI-Wallet auch in Präsenzsituationen. Die Entgegennahme von Nachweisen aus der EUDI-Wallet stellt ein optionales Angebot dar und ist nach eIDAS VO nicht verpflichtend durch die öffentlichen Stellen umzusetzen, birgt im Ende-zu-Ende Prozess jedoch großes Potential, um in Zukunft Prozesse weiter zu automatisieren.

1.4 Referenzen

Das EUDI-Wallet-Ökosystem basiert auf einer Vielzahl rechtlicher, technischer und strategischer Grundlagen, die im Folgenden referenziert werden. Die aufgeführten Dokumente dienen der Einordnung der konzeptionellen Entscheidungen und bilden die Grundlage für die Umsetzung.

eIDAS-VO 910/2014

Am 20. Mai 2024 trat die Novellierung der "Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, zuletzt geändert durch Verordnung (EU) Nr. 2024/1183", kurz eIDAS 2.0, in Kraft. Sie ersetzt und erweitert die bisherige Verordnung eIDAS-VO Nr. 910/2014 und stellt den zentralen Rechtsrahmen für das EUDI-Wallet-Ökosystem dar. Die eIDAS-VO verpflichtet die Mitgliedstaaten zur Bereitstellung einer digitalen Identität für natürliche und juristische Personen.

Durchführungsverordnungen (DVO)

Die im Rahmen der eIDAS-VO erlassenen Durchführungs- und delegierten Rechtsakte sind rechtsverbindlich und konkretisieren die technischen, funktionalen sowie organisatorischen Anforderungen an das EUDI-Wallet-System und werden schrittweise verabschiedet bzw. angekündigt.

Architektur und Referenzrahmen (ARF, Version 2.8.0)

Das ARF enthält eine Reihe von Anforderungen an die Architektur, gemeinsamer Standards und technischer Spezifikationen und wird empfohlen für die Entwicklung der Referenzimplementierung der EUDI-Wallet Lösung zu nutzen. Der ARF selbst besitzt jedoch keine rechtliche Befugnis und legt die verbindlichen rechtlichen Anforderungen für EUDI-Wallets nicht im Voraus fest.

Blueprint für das deutsche EUDI-Wallet Ökosystem

Der Blueprint wurde von der SPRIND und dem BMI (jetzt: BMDS) im Rahmen eines öffentlichen Architekturprozesses entwickelt. Dieser beschreibt die technischen und organisatorischen Grundlagen für die nationale Umsetzung der EUDI-Wallet und den Aufbau des staatlichen EUDI-Wallet-Ökosystems.

National and European Once-Only-Technical-System (NOOTS/ EU-OOTS)

Das NOOTS wird die technische Infrastruktur für den sicheren behördenübergreifenden Datenaustausch zwischen Bund, Ländern und Kommunen schaffen. Ziel ist es, Verwaltungsdaten aus Registern nur einmalig zu erheben und mehrfach, im Sinne des Once-Only-Prinzips, nutzbar zu machen. Perspektivisch ist eine Anbindung an das europäische Once-Only Technical System (EU-OOTS) vorgesehen, um den grenzüberschreitenden Datenaustausch zu ermöglichen.

Internationale Standards

Die Ausgestaltung des EUDI-Wallet-Ökosystems basiert auf international etablierten Standards, die Sicherheit, Interoperabilität und Vertrauenswürdigkeit digitaler Identitäten und Nachweise gewährleisten. Neben europäischen Vorgaben kommen dabei auch internationale technische Spezifikationen zum Einsatz.

Eine wichtige Rolle spielen die Standards des European Telecommunications Standards Institute (ETSI), insbesondere in Bezug auf Sicherheitsanforderungen, Zertifizierungs- und Vertrauensmechanismen für elektronische Identifizierungs- und Vertrauensdienste. Ergänzend werden Protokoll- und Datenstandards internationaler Organisationen wie der OpenID Foundation (OIDF) (z. B. OpenID4VCI, OpenID4VP) und der Internet Engineering Task Force (IETF) (z. B. SD-JWT-VC) genutzt. Zudem verweisen einschlägige europäische Spezifikationen auf Normen

der ISO/IEC-Familie, wodurch eine international anschlussfähige und konsistente Umsetzung unterstützt wird.

2 Zielbild Verwaltungsanbindung

2.1 Prämissen

Prämisse	Beschreibung
EUDI-Wallet als zentrale Verwaltungskomponente etablieren	EUDI-Wallet als eine zentrale Komponente der öffentlichen Verwaltung anerkennen, über die Identitäts- und Attributsbescheinigungen sicher und EU-interoperabel bereitgestellt und verarbeitet werden können.
Niedrigschwellige Anbindung erleichtern	Zugangshürden minimieren, um die Anbindung an das EUDI-Wallet-Ökosystem für alle Akteure, insbesondere der öffentlichen Verwaltungen, kurzfristig niedrigschwellig zu gestalten.
Bestehende Infrastrukturen integrieren	Zentrale Verwaltungsinfrastrukturen wie BundID und NOOTS kurzfristig nachnutzen und auf Synergiepotenziale setzen, u.a. aus der OZG-, SDG-Umsetzung und der Registermodernisierung, um die Erfüllung der Anforderungen der eIDAS-VO zu gewährleisten.
Zentrale Umsetzung anstreben, soweit realisierbar	Zentrale Bereitstellung von Komponenten zur Nachnutzung entwickeln, um direkte Anbindung an die EUDI-Wallet mittel- bis langfristig zu ermöglichen.
Dezentrale Umsetzung ermöglichen	Fachlich zuständige Stellen befähigen, Anforderungen, die nicht zentral umgesetzt werden, eigenständig zu erfüllen und passende Lösungen selbst zu entwickeln.

Tabelle 3: Prämissen für das Zielbild Verwaltungsanbindung

2.2 Kurzfristiges sowie mittel- bis langfristiges Zielbild

Im Rahmen der Entwicklung des EUDI-Wallet-Ökosystems hat der Bund ein Zielbild für die Anbindung der öffentlichen Verwaltung an die EUDI-Wallet erarbeitet. Mittel- bis langfristig stellt die direkte Anbindung an die EUDI-Wallet das Zielbild dar, da sie im Hinblick auf die Nutzendenführung aufgrund geringer Medienbrüche und Systemwechsel Vorteile bietet. Zugleich verbleibt die Hoheit über die Datenverarbeitung durchgehend bei den beteiligten Stellen. Aus datenschutzrechtlicher Sicht ist der Ansatz vorteilhaft, da die Datenübertragung Ende-zu-Ende verschlüsselt erfolgt. Die EUDI-Wallet ist in die Antragsprozesse integriert,

um Nachweise (PID und weitere) gegenüber dem Onlinedienst zu präsentieren und Nachweise direkt in die EUDI-Wallet auszustellen. Das Automatisierungspotenzial wird dabei insbesondere dadurch ermöglicht, dass strukturierte und verifizierte Nachweise unmittelbar im Fachverfahren weiterverarbeitet werden können, sodass fachliche Prüfungen und Entscheidungen regelbasiert und automatisiert erfolgen können, ohne zusätzliche manuelle Zwischenschritte oder vorgelagerte Vermittlungs- oder Postfachlogiken. Dies setzt voraus, dass Onlinedienste und Fachverfahren technisch in der Lage sind, die Kommunikation mit der EUDI-Wallet auf Basis moderner Standards und in strukturierter Datenform zu bewerkstelligen.

Kurzfristig steht die Erfüllung der gesetzlichen Verpflichtungen im Vordergrund, konkret die Akzeptanz der PID in digitalen Prozessen, sofern eine starke Nutzerauthentifizierung auf Vertrauensniveau hoch erforderlich ist. Um Rechtskonformität sicherzustellen und Zeit für den schrittweisen Aufbau dieses Zielbildes zu gewinnen, ermöglicht das BMDS durch die Weiterentwicklung der BundID eine voraussichtlich ab Januar 2027 produktiv nutzbare Einstiegslösung. Die Entgegennahme der PID zur Ident- und Authentifizierung wird über die indirekte Anbindung an die BundID sichergestellt. Damit werden Länder und Kommunen initial organisatorisch und technisch entlastet. Außerdem wird über die Anbindung an das ZBP die Ausstellung insbesondere kommunaler Nachweise ermöglicht; diese Ausstellung wird aktuell im Pilotvorhaben mit der Landeshauptstadt Dresden und der Sächsischen Staatskanzlei anhand von zwei Anwendungsfällen[2] bis voraussichtlich zum Januar 2027 produktiv umgesetzt. In das ZBP ausgestellte Nachweise können auf Wunsch der Nutzenden in die EUDI-Wallet übertragen werden („Push"). Voraussetzung ist die Anbindung der Onlinedienste und Fachverfahren an die BundID sowie für Ausstellungszwecke die Anbindung an das ZBP. Es ist zu berücksichtigen, dass für Verwaltungsverfahren, insbesondere mit Bescheidzustellung und der Anforderung einer bidirektionalen Kommunikation zwischen Verwaltung und Nutzenden, die BundID zukünftig weiterhin eine zentrale Rolle einnimmt.

Zur technischen Erleichterung der direkten Anbindung an die EUDI-Wallet wird ein Produkt des IT-Planungsrates zum Wallet-Adapter weiterentwickelt und voraussichtlich bis Januar 2027 als modulare Softwarekomponente bereitgestellt. Ein möglicher zentraler Betrieb auf Landesebene bietet den Vorteil der Vermeidung von Mehrfachstrukturen, die organisatorische Umsetzung liegt jedoch in der Verantwortung der Länder.

[2] „Ausstellung des Dresden-Pass" und „Ausstellung der sächsischen Ehrenamtskarte"

Ergänzend wird ein zentraler Issuer- und Verifier- Dienst zur flächendeckenden Ausstellung von Verwaltungsnachweisen angeboten, dessen Nachnutzung perspektivisch über eine Verwaltungsvereinbarung zwischen Bund und Ländern geregelt wird. Für die in Anhang VI der eIDAS-VO aufgeführten Attribute muss durch die EU-Mitgliedsstaaten ein Verifikationsmechanismus auf Verlangen Nutzender für QTSPs bereitgestellt werden. Für diese fachliche Verifikation von Attributswerten gegenüber der jeweils zuständigen authentischen Quelle, das heißt Register oder Datenbeständen, welche Attribute liefern, ermöglich der zentrale Verifier-Dienst die Kommunikation zwischen QTSPs und Authentischen Quellen (vgl. Kapitel 4.4).
Darüber hinaus wird die Anbindung an die NOOTS-Infrastruktur zur Ausstellung von Nachweisen aus an NOOTS angebundenen Registern sichergestellt. Die Form des direkten Nachweisabrufs ermöglicht es, nicht-antragsbezogene Nachweise wie etwa Wohnsitz-, Ausbildungs- oder steuerliche Basisnachweise für die EUDI-Wallet und damit den sektorübergreifenden Nachweisaustausch nutzbar zu machen. Dafür wir der Wallet-Adapter – ein Produkt des IT-Planungsrates – nachgenutzt und produktiv zum NOOTS-spezifischer Issuing-Dienst[3] weiterentwickelt. In Zusammenarbeit mit der FITKO und dem BVA wird ein MVP umgesetzt, um voraussichtlich bis Januar 2027 den Nachweisabruf aus einem Register in die EUDI-Wallet über die NOOTS-Infrastruktur zu erproben. Hinweis: Eine Bereitstellung von Nachweisen aus der EUDI-Wallet über das NOOTS (EUDI-Wallet als „Data Provider") ist weder vorgesehen noch rechtlich möglich.
Damit wird eine vollständige Integration der EUDI-Wallet in Verwaltungsverfahren ermöglicht – sowohl für antragsbezogene als auch für nicht-antragsbezogene Nachweise.

2.3 Geltungsbereich des Konzepts zur Verwaltungsanbindung

Für das Konzept werden folgende Aspekte nicht detailliert betrachtet:

- die Entwicklung der staatlichen EUDI-Wallet, die lediglich als relevante Rahmenbedingung berücksichtigt, jedoch nicht vertiefend behandelt wird
- sowie die Ausstellung der PID, einschließlich der zugehörigen Widerrufsprozesse

[3] In der ersten Ausbaustufe im Sinne eines MVP

Bereitstellung und Betrieb der staatlichen EUDI-Wallet als mobile Applikation (iOS und Android) sowie die Möglichkeit der Ausstellung der PID über einen PID-Provider soll durch den Bund bis Januar 2027 sichergestellt werden.

3 Anbindungsoptionen

3.1 Indirekte Anbindung an die EUDI-Wallet über BundID/ZBP

Die BundID wird produktiv weiterentwickelt. Ziel ist es, Januar 2027 die Funktionalität 1 „Sichere Identifizierung von Nutzenden mit der EUDI-Wallet" umzusetzen und damit eine einheitliche Identifizierung und Authentifizierung für alle an die BundID angebundenen Dienste und Brückenköpfe zu ermöglichen. Zusätzlich wird Funktionalität 2 ebenfalls bis Januar 2027 mindestens anhand von zwei konkreten Anwendungsfällen mit der Landeshauptstadt Dresden umgesetzt (Ausstellung des Dresden-Passes sowie der Sächsischen Ehrenamtskarte). Die dabei gewonnenen Erkenntnisse und technischen Lösungen sollen als Blaupause dienen und von allen öffentlichen Stellen genutzt werden können, die Nachweise über das ZBP in die EUDI-Wallet ausstellen wollen.

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

Die BundID erfüllt seit der OZG-Novelle 2024 als einheitliches Nutzerkonto die Aufgabe der Identifizierung und Authentifizierung der Bürger gegenüber der öffentlichen Verwaltung. Aus diesem Grund wird die BundID – ergänzend u.a. zur eID – die EUDI-Wallet als weiteres Identifizierungsmittel voraussichtlich ab Januar 2027 produktiv anbieten. Damit erfüllen alle bereits an die BundID angebundenen öffentlichen Stellen automatisch die verpflichtende Anforderung der eIDAS-VO. Das BMDS als fachverantwortliche Stelle der BundID handelt hierbei in der Rolle einer Relying Party und bezieht im Vorfeld ein Zugriffszertifikat und Registrierungszertifikate, welche für die technische Kommunikation zwischen den Teilnehmenden im EUDI-Wallet-Ökosystem benötigt werden. Die Zertifikate werden von der national zuständigen Stelle (= Registrar), nach der Registrierung der Relying Party, ausgestellt. Die Relying Party stellt die sichere Speicherung des privaten Schlüssels des Zugriffszertifikats sicher. Das Registrierungszertifikat ist nicht schlüsselgebunden und öffentlich einsehbar. Stellen Bürgerinnen und Bürger ihre Identitätsdaten aus der EUDI-Wallet bereit, werden diese durch die BundID (das BMDS

ist als fachlich zuständige Stelle als Relying Party registriert) in Echtzeit technisch geprüft[4] und zur Bestätigung der Identität genutzt. Die BundID gleicht die Angaben mit den vorhandenen Nutzerdaten ab und stellt der anfragenden Behörde die für den jeweiligen Verwaltungsprozess benötigten Informationen bereit. Wenn die Authentifizierung via BundID-Konto erfolgt, wird das Postkorbhandle automatisch dem angebundenen Dienst bzw. Fachverfahren übergeben. Auch weitere Funktionalitäten der BundID wie bspw. die Nutzung der Bidirektionaltität im Postfach sind so direkt nutzbar. Weiterführende technische Details zur indirekten Anbindung über die BundID sind in Anhang II Indirekte Anbindung an die EUDI-Wallet beschrieben.

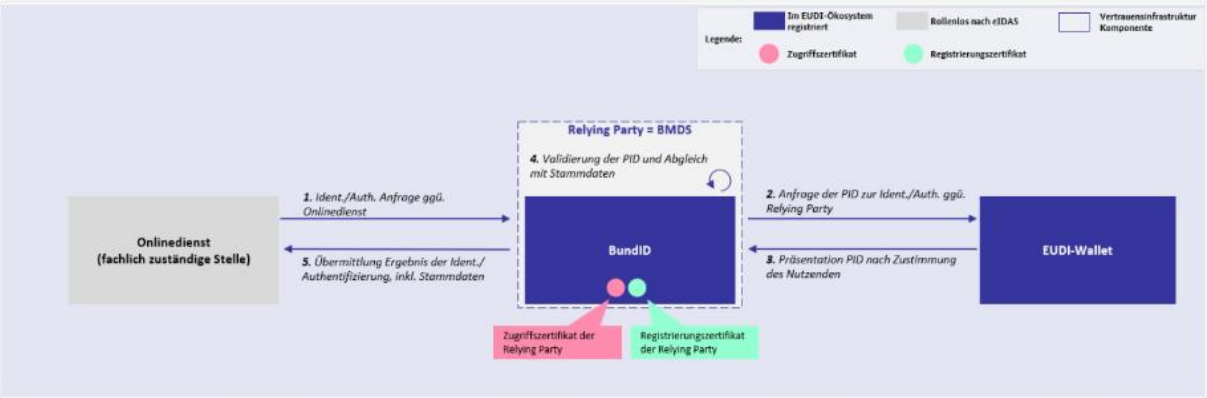

Abbildung 1: Identifizierung von Nutzenden über die BundID mit der EUDI-Wallet (aktueller Arbeitsstand)

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

Öffentliche Stellen, die bereits an das ZBP angebunden sind, können darüber Nachweise in die EUDI-Wallet ausstellen. Dazu ist eine Anpassung an der Schnittstelle nötig, um die für den Nachweis notwendigen Daten als strukturierten Datensatz im JSON-Format an das ZBP zu übermitteln. Durch Nutzung der Postfachfunktionalität bleibt die rechtssichere Zustellung von Bescheiden in das ZBP gewährleistet. In das ZBP zugestellte Nachweise können auch in die EUDI-Wallet ausgestellt werden. Möchten Bürgerinnen und Bürger einen im ZBP hinterlegten Nachweis zusätzlich in ihrer EUDI-Wallet speichern, kann dieser Prozess direkt aus dem ZBP heraus angestoßen werden. Das BMDS übernimmt in der Rolle des EAA-Providers im Auftrag der fachlich zuständigen Stellen die technische Bereitstellung und Siegelung der Nachweise für die EUDI-Wallet. Die im ZBP vorliegenden Nachweise, welche durch die fachlich zuständige Stelle in maschinen- und menschenlesbare Form zugestellt werden, werden durch die

[4] Überprüfung des PID-Providers, des Widerrufstatus der PID, der Echtheit der Signatur/Siegel, des Device und User Binding.

BundID entsprechend in passende Datenstrukturen konvertiert. Die Daten verlassen die vielfach abgesicherte Infrastruktur des ITZBund an dieser Stelle nicht. Zudem ist die gesamte Postfachkommunikation wie gehabt über die Netze des Bundes abgesichert. Das BMDS übernimmt als EAA-Provider die Ausstellung technisch über die BundID-Infrastruktur und stellt im Namen von fachlich zuständigen Stellen EAAs mit einem fortgeschrittenen elektronischen Siegel (FES) unter Einbindung eines QTSP aus. Für die weitere Ausbaustufe wird planmäßig für die Ausstellung von QEAAs ein qualifizierter Fernsiegeldienst eines QTSPs eingebunden, sodass die Anforderungen der eIDAS-Verordnung vollständig erfüllt werden.

Hinweis: Sofern als Voraussetzung für die Ausstellung eines Nachweises in der EUDI-Wallet im Antragsprozess weitere Unterlagen erforderlich sind (z. B. der Nachweis über den Erhalt von Wohngeld für die Ausstellung eines Sozialpasses), können diese weiterhin über die bestehenden Einreichprozesse des jeweiligen Dienstes bzw. Fachverfahrens übermittelt werden. Ein vorheriges Vorliegen dieser Nachweise in der EUDI-Wallet ist gemäß eIDAS-Verordnung nicht zwangsweise erforderlich; perspektivisch ist jedoch vorgesehen, entsprechende Nachweise auch direkt aus der EUDI-Wallet verwenden zu können.

Weiterführende technische Details zur indirekten Anbindung über die BundID sind in Anhang II Indirekte Anbindung an die EUDI-Wallet beschrieben.

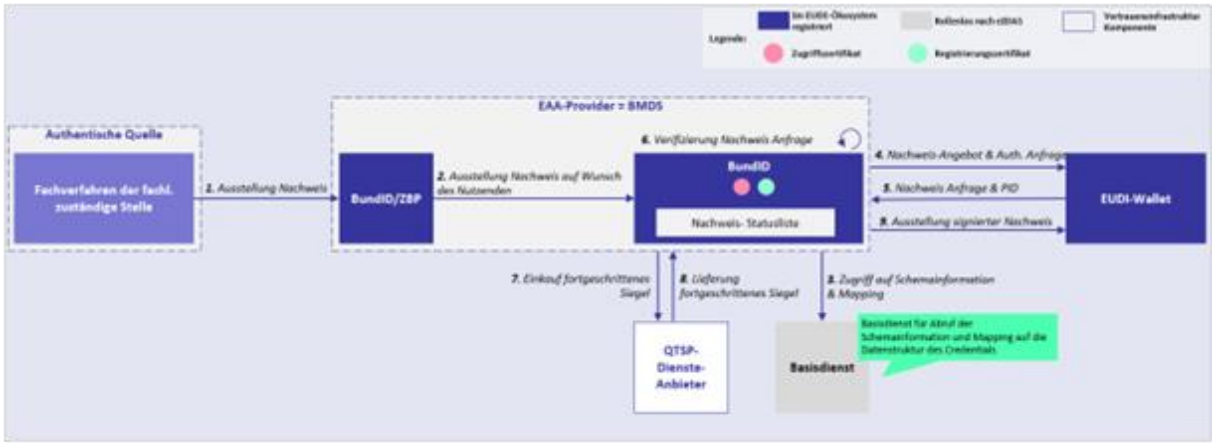

Abbildung 2: Ausstellung von Nachweisen aus dem ZBP in die EUDI-Wallet (aktueller Arbeitsstand)

Nach aktuellem Sachstand ergeben sich folgende Anforderungen für die fachlich zuständigen Stellen, wenn sie die Anbindung an die EUDI-Wallet über die BundID umsetzen wollen:

- Technische Anbindung an das ZBP und Registrierung über das BundID Self-Service-Portal (SSP)
- Bereitstellung menschenlesbarer Daten (z.B. PDF)
- Bereitstellung strukturierter Daten (maschinenlesbar, z.B. JSON)
- Definition und Bereitstellung der Nachweisschemata für die Nachweise, welche als EAAs ausgestellt werden sollen[5]; Attestation Rulebooks[6] als ergänzende Richtlinien zur Definition der Schemata. Aufbau und Bereitstellung der Rulebooks sind aktuell in Arbeit.
- Registrierung als Relying Party bei der national zuständigen Stelle (Registrar). Erhalt eines Zugriffszertifikats optional. Abhängig von intendierten Anwendungsfällen der fachlich zuständigen Stelle bzw. Einbindung und Abstimmung mit dem beauftragten Vermittler (Intermediary), in diesem Fall der BundID.

Laut aktuellem Stand der Umsetzung ist eine Registrierung der fachlich zuständigen Stelle im EUDI-Wallet-Ökosystem als Relying Party erforderlich. Allerdings ist die Beantragung von Zugriffs- und Registrierungszertifikate nicht zwingend notwendig. Die Beantragung der nötigen Registrierungszertifikate kann über den beauftragen Vermittler im Auftrag der fachlich zuständigen Stelle erfolgen. Dazu werden aktuell verschiedene Optionen evaluiert.

Funktionalität 3: Entgegennahme von Nachweisen über die BundID aus der EUDI-Wallet

Ziel ist es, im Zuge der Funktionalität 3, in der EUDI-Wallet gespeicherte Nachweise im Rahmen eines Antragsverfahrens über die BundID gegenüber dem Onlinedienst zu präsentieren. Die konkrete technische Ausgestaltung der Umsetzungsoption über die BundID und die Anforderungen an fachlich zuständige Stellen werden aktuell im laufenden BMDS-Vorhaben zur „Erprobung der Verwaltungsanbindung der EUDI-Wallet" gemeinsam mit der Landeshauptstadt Dresden erhoben und praxisnah validiert. Diese Funktionalität wird nicht bis zum Januar 2027 durch die BundID sichergestellt, da aktuell von wesentlichen Aufwänden seitens BundID ausgegangen wird. Eine direkte Anbindung an die EUDI-Wallet wird für die Entgegennahme von Nachweisen innerhalb der EUDI-Wallet, die der öffentlichen Verwaltung nicht

[5] Definition der Nachweisschemata „Dresden Pass" und „Sächsische Ehrenamtskarte" erfolgt im Rahmen der Pilotierung mit LH Dresden und der Sächsischen Staatskanzlei und wird als Referenz für weitere Nachweise nachnutzbar zur Verfügung gestellt werden; Bestehende Synergien zwischen DAMAS und EUDI-Wallet-Ökosystem werden in der aktuellen DAMAS Konzeption berücksichtigt

[6] https://github.com/cre8/catalog-of-attestations/blob/main/rulebooks/gym-membership-card/1.0.0.md

vorliegen laut aktuellen Erkenntnissen empfohlen. Die rechtlichen Fragestellungen welche Rolle nach eIDAS-VO die BundID bzw. das BMDS als deren fachverantwortliche Stelle in diesem Szenario einnehmen darf, befinden sich aktuell in Klärung durch das BMDS. In Abbildung 3 wird beispielhaft dargestellt, wie die fachlich zuständige Stelle in der Rolle einer Relying Party Nachweise aus der EUDI-Wallet über die BundID in der Rolle eines Vermittlers (Intermediary) entgegennehmen kann.

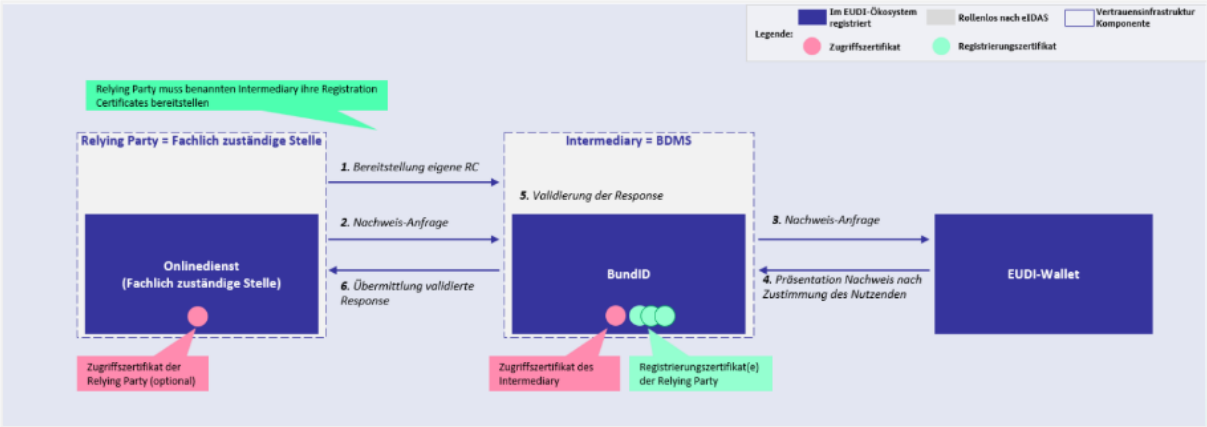

Abbildung 3: Entgegennahme weiterer Attributsbescheinigungen über BundID aus der EUDI-Wallet (aktueller Arbeitsstand)

3.2 Direkte Anbindung an die EUDI-Wallet (mit und ohne Wallet-Adapter)

Für öffentlich-rechtliche Organisationen mit hohem Digitalisierungs- und Reifegrad, wie etwa bundesweit tätige Träger mit eigenen leistungsfähigen IT-Strukturen sowie für zentrale Portale wie das Bundesportal und EfA-Onlinedienste, wird vor allem dann eine direkte Anbindung an die EUDI-Wallet empfohlen, wenn eine rechtssicheren Bescheidzustellung und bidirektionaler Kommunikation über die BundID/ZBP nicht erforderlich sind, unter anderem aufgrund eigenständiger Postfach-Infrastrukturen.

Im Fall von EfA-Onlinediensten, welche bereits an die BundID angebunden sind, wird jedoch eine direkte Anbindung an die EUDI-Wallet empfohlen. Dadurch können Identifizierungs-, Präsentations- und Verifikationsflüsse einmalig implementiert und anschließend nach dem EfA-Prinzip bundesweit nachgenutzt werden. Die fachliche Umsetzung konkreter Anwendungsfälle erfolgt durch die jeweils fachlich zuständigen Stellen bzw. betriebsverantwortlichen Stellen. Eine Nachnutzung der BundID ist grundsätzlich möglich, wird im Hinblick auf die Nutzendenfreundlichkeit aufgrund notwendigerweise erforderliche zusätzliche Interaktionsschritte sowie der Sicherstellung der Entgegennahme von weiteren Nachweisen aus der EUDI-

Wallet jedoch nicht empfohlen. Da die Onlinedienste bzw. Portale direkt mit der EUDI-Wallet kommunizieren, wird bei der Identifizierung bzw. Authentifizierung mit der PID nach aktuellen Umsetzungsstand kein Postfach-Handle und keine Antrags-ID an die fachlich zuständigen Stellen übermittelt, mit welchen sie z.B. das ZBP oder die Statusmonitor Funktion nutzen könnten. Der Bund sowie das Projekt „ZaPuK" prüfen, inwieweit perspektivisch eine Zustellung von Bescheiden in das ZBP auch ohne vorherige Beantragung mit der BundID möglich gemacht werden kann.

Zur Unterstützung der direkten Anbindung können die fachlich zuständigen Stellen den vom Bund zentral weiterentwickelten Wallet-Adapter – ein Produkt des IT-PLR – nutzen. Dieser kann als modulare Softwarekomponente nachgenutzt und bei Bedarf für spezifische Verwaltungsverfahren technisch angepasst werden. Dieser vereinfacht die technische Einbindung der EUDI-Wallet und stellt eine einheitliche technische Grundlage bereit. Der Betrieb dieser Komponente kann entweder zentral als Service oder dezentral durch die jeweilige Stelle bzw. deren Dienstleister erfolgen. Weiterführende technische Details zur direkten Anbindung sind in Anhang III Direkte Anbindung an die EUDI-Wallet bei Betrieb eines Wallet-Adapters beschrieben.

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

Im Vergleich zur indirekten Anbindung an die EUDI-Wallet über die BundID agiert die fachlich zuständige Stelle des Verwaltungsdienstes (u.a. EfA-Onlinedienst oder -portal) bzw. die betriebsverantwortliche Stelle im Kontext von EfA-Onlinediensten als Relying Party (Verifier), und ist als solche beim deutschen Registrar registriert (Art. 5b Abs. 1 und 3 eIDAS-VO). Sie stellt zudem die sichere Speicherung des privaten Schlüssels des Zugriffszertifikats sicher. Das Registrierungszertifikat ist nicht schlüsselgebunden und öffentlich einsehbar. Die fachlich zuständigen Stellen kommunizieren unmittelbar mit der EUDI-Wallet der Nutzenden. Der Verwaltungsdienst stellt eine Anfrage zur Identifizierung und Authentifizierung an die EUDI-Wallet. Nach Freigabe der PID durch den Nutzenden der EUDI-Wallet werden die Daten durch den Wallet Adapter verifiziert[7] und an den Onlinedienst bzw. -portal übergeben. Im Unterschied zur indirekten Anbindung über die BundID werden keine zusätzlichen Informationen wie das Postfach-Handle der BundID übermittelt.

[7] Technische Spezifikationen gem. ETSI EN 319 401 V3.1.1 einhalten

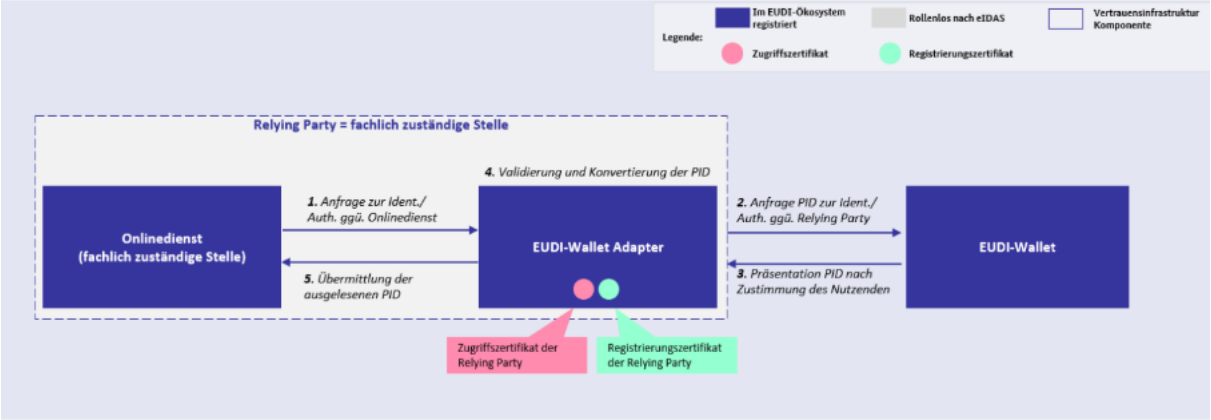

Abbildung 4: Direkte Identifizierung von Nutzenden mit der EUDI-Wallet; Wallet-Adapter im Eigenbetrieb (aktueller Arbeitsstand)

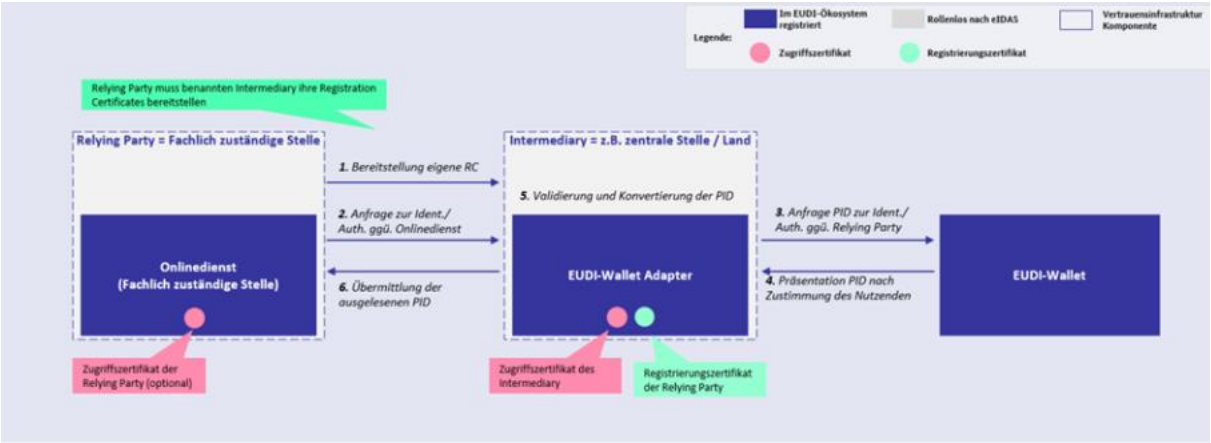

Abbildung 5: Direkte Identifizierung von Nutzenden mit der EUDI-Wallet; Wallet-Adapter über zentrale Stelle angebunden (aktueller Arbeitsstand)

Nach aktuellem Sachstand ergeben sich folgende Anforderungen für die fachlich zuständigen Stellen, welche einen Wallet-Adapter betreiben oder welche eine Wallet-Adapter nutzen, der zentral durch ein Bundesland oder eine Kommune betrieben wird[8]:

[8] Für die Bereitstellung eines zentral betriebenen Wallet-Adapters müssen u.a. sicherheitsrelevante Aspekte, wie Zugangssicherung für die anbindenden Stellen, berücksichtig werden

- Registrierung als Relying Party einschließlich der Speicherung von Zertifikaten (ggf. unterstützt durch Wallet-Adapter); Erhalt eines Zugriffszertifikats optional. Abhängig von intendierten Anwendungsfällen der fachlich zuständigen Stelle bzw. Einbindung und Abstimmung mit dem beauftragten Vermittler (Intermediary)
- Integration und ggf. Betrieb des Wallet-Adapters, u.a. techn. Eingliederung in bestehende Verwaltungsprozesse
- Sichere Verwaltung von privaten Schlüsseln der Zertifikate (ggf. Zertifikatsmanagement durch Wallet-Adapter)
- Übermittlung Authentifizierungsanfrage an die Wallet-Adapter Komponente
- Erhalt PID über den Wallet-Adapter und Verarbeitung im Antragsverfahren; Validierung/Prüfung der PID durch Wallet-Adapter
- Verarbeitung von Fehlermeldungen des Wallet-Adapters
- Datenkonvertierung zur Weiterverarbeitung der Daten durch fachlich zuständige Stellen (optional)
- Anpassung der Nutzeroberfläche u.a. des Onlinedienstes zur Integration der EUDI-Wallet als ergänzendes Identifizierungs-/Authentifizierungsmittel

Alternativ können öffentliche Stellen ebenso ohne den Betrieb eines Wallet-Adapters die EUDI-Wallet anbinden. Nach aktuellem Sachstand ergeben sich folgende Anforderungen für die fachlich zuständigen Stellen, ohne den Betrieb eines Wallet-Adapters:

- Registrierung als Relying Party, einschließlich der Speicherung von Zertifikaten
- Direkte Anbindung an die EUDI-Wallet, unter anderem durch Integration einer neuen Schnittstelle
- Sichere Verwaltung von privaten Schlüsseln der Zertifikate
- Versand Authentifizierungsanfrage an die EUDI-Wallet gemäß vorgegebenem Standard
- Erhalt der PID und Validierung/Prüfung der PID sowie Verarbeitung im Antragsverfahren
- Abruf und Aktualisierung der benötigten Trusted Lists
- Verarbeitung von Fehlermeldungen der EUDI-Wallet
- Datenkonvertierung zur Weiterverarbeitung der Daten durch fachlich zuständige Stellen (optional)

- Anpassung der Nutzeroberfläche u.a. des Onlinedienstes zur Integration der EUDI-Wallet als ergänzendes Identitäts-/Authentifizierungsmittel

Funktionalität 2: Zustellung von Nachweisen über die EUDI-Wallet

Fachlich zuständige Stellen können Nachweise direkt in die EUDI-Wallet der Nutzenden ausstellen. Um die Ausstellung technisch zu vereinfachen, kann ebenfalls ein Wallet-Adapter in durch die fachlich zuständige Stelle betrieben werden. Die Ausstellung eines EAAs erfolgt durch einen sogenannten EAA-Provider. Diese Rolle nach eIDAS muss nicht zwingend von der fachlich zuständigen Stelle selbst erfüllt werden, sondern kann auch an externe Dienste ausgelagert werden, die im Auftrag der fachlich zuständigen Stelle ausstellen. Dadurch entstehen für die jeweiligen Stellen sowohl technische als auch organisatorische Anforderungen.

In einem idealtypischen Ablauf kann die fachlich zuständige Stelle den Gesamtprozess von Antragseingang bis hin zur Nachweiserzeugung automatisiert durchführen, das setzt jedoch voraus, dass alle erforderlichen Unterlagen als EAAs in der EUDI-Wallet vorliegen. Der synchrone Prozess startet im Onlinedienst mit der Beantragung einer Verwaltungsleistung. Nutzende ident- und authentifizieren mit der PID und übertragen weitere für den Antrag benötigten Nachweise welche in der EUDI-Wallet vorliegen, an den Onlinedienst. Nachweise werden durch die Relying Party verifiziert[9]. Zusätzlich werden ggf. fachliche Prüfungen durchgeführt, zum Beispiel eine Altersvalidierung. Auf Grundlage dieser Prüfungen wird der Nachweis als Resultat des Verwaltungsvorgangsautomatisiert durch die fachlich zuständige Stelle bzw. verwaltungsinterne Dienstleister erstellt und der Vorgang dokumentiert. Anschließend werden die strukturierten Nachweisdaten der EUDI-Wallet zugestellt, Bedingung ist die vorherige aktiver Zustimmung des Nutzenden. Durch die synchrone Ausstellung des Nachweises in die EUDI-Wallet des Nutzenden entfällt die Notwendigkeit die Nachweisdaten über einen längeren Zeitraum zu persistieren.

Bei der Integration eines Wallet-Adapter generiert dieser eine Landing-Page, zu der der Nutzende weitergeleitet wird. Die Ausstellung des Nachweises in die EUDI-Wallet kann anschließend durch den Nutzenden auf dieser Landing-Page ausgelöst werden. Die EUDI-Wallet wird auf dem mobilen Endgerät (iOS und Android) des Nutzenden gestartet, prüft die Echtheit des Siegels und Gültigkeit der Anfrage, informiert den Nutzenden über das Ergebnis und stößt erst

[9] Prüfung des Providers gegen Trusted List, des Ablaufdatum und Widerruf des Nachweises, der Echtheit der Signatur/Siegel, des Device und User Binding, der Einhaltung der Schemadefinition des Nachweises

nach Zustimmung des Nutzenden die Anfrage zur Ausstellung in die EUDI-Wallet beim Wallet-Adapter an.

Der Wallet-Adapter prüft ebenfalls die Echtheit des Siegels und Gültigkeit der Anfrage aus der EUDI-Wallet und erstellt anschließend, unter Einbeziehung eines QTSP mittels fortgeschrittener elektronischer Siegelung (FES), einen signierten und validierten Nachweis (gemäß Schemadefinition), welcher an die EUDI-Wallet des Nutzenden ausgestellt wird.

Die asynchrone Ausstellung durch die fachlich zuständige Stelle mittels Wallet-Adapter, d.h. mit Verzögerung zwischen Eingang der Nachweisanfrage und Ausstellung durch die fachlich zuständige Stelle in die EUDI-Wallet, wird im Rahmen der Pilotierung mit Landeshauptstadt Dresden nicht getestet, ist aber mit dem Wallet-Adapter technisch möglich.

Weiterführende technische Details zur direkten Anbindung sind in Anhang III Direkte Anbindung an die EUDI-Wallet bei Betrieb eines Wallet-Adapters beschrieben.

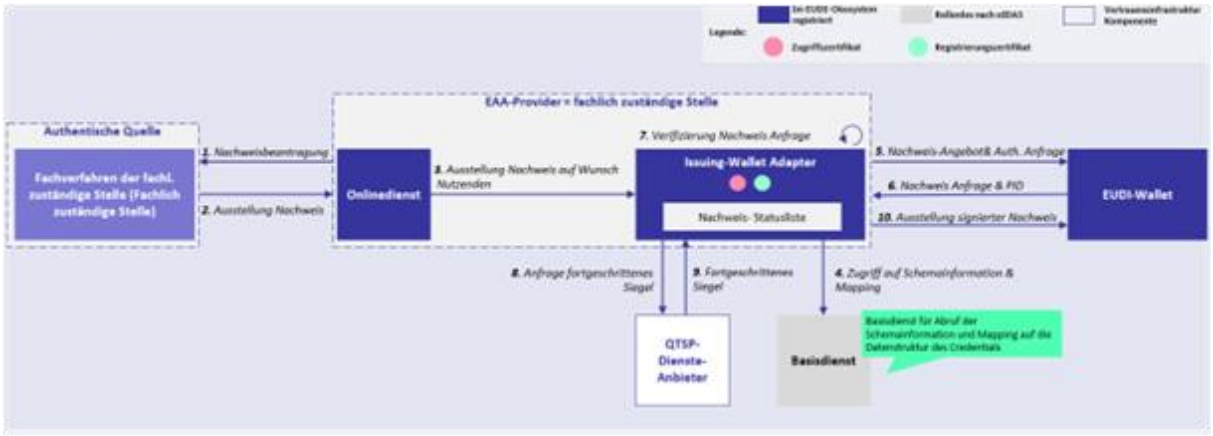

Abbildung 6: Direkte Ausstellung von Nachweisen in die EUDI-Wallet; Wallet-Adapter (Issuing) im Eigenbetrieb (aktueller Arbeitsstand)

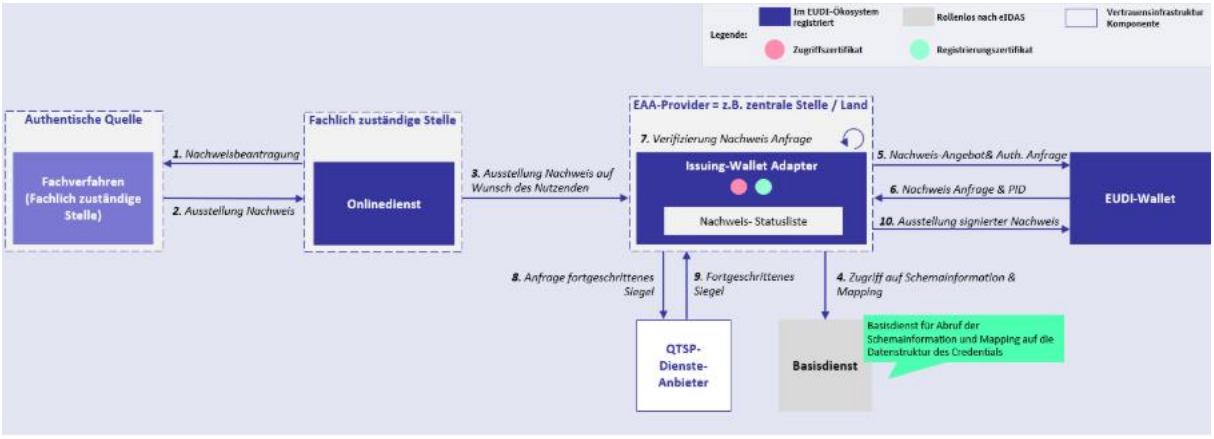

Abbildung 7: Direkte Ausstellung von Nachweisen in die EUDI-Wallet; Wallet-Adapter über zentrale Stelle angebunden (aktueller Arbeitsstand)

Nach aktuellem Sachstand ergeben sich folgende Anforderungen für die fachlich zuständigen Stellen, welche einen Wallet-Adapter betreiben oder welche eine Wallet-Adapter nutzen, der zentral durch ein Bundesland oder eine Kommune betrieben wird:

- Registrierung als Relying Party (EAA-Provider[10]), einschließlich der Speicherung von Zertifikaten unterstützt durch Wallet-Adapter
- Integration und ggf. Betrieb des Wallet-Adapters zur techn. Unterstützung der Ausstellung und EUDI-Wallet-Anbindung
- Sichere Verwaltung von privaten Schlüsseln der Zertifikate (ggf. Zertifikatsmanagement durch Wallet-Adapter)
- Automatisierte Verarbeitung der Nachweisanfrage und Bereitstellung der strukturierten Daten, um den synchronen Ausstellungsprozess zu gewährleisten
- Versand strukturierter Daten an den Wallet-Adapter und Weiterleitung zur Landing-Page des Wallet-Adapters
- Beauftragung eines qualifizierten Vertrauensdiensteanbieters (Fernsiegelung) oder Einkauf eines Dienstes zur elektronischen Siegelung für die fortgeschrittene Siegelung des Nachweises
- Verarbeitung von Fehlermeldungen des Wallet-Adapters

[10] Technische Spezifikationen gem. ETSI EN 319 401 V3.1.1 einhalten

Alternativ können öffentliche Stellen ebenso ohne den Betrieb eines Wallet-Adapters die EUDI-Wallet anbinden. Nach aktuellem Sachstand ergeben sich folgende Anforderungen für die fachlich zuständigen Stellen, ohne den Betrieb eines Wallet-Adapters:

- Registrierung als Relying Party (EAA-Provider), einschließlich der Speicherung von Zertifikaten
- Sichere Verwaltung von privaten Schlüsseln der Zertifikate
- Nachweisabruf, Erstellung des Nachweis Offer und Kommunikation zur EUDI-Wallet, d.h. Prüfung Identität des Antragstellenden, Überprüfung PID, Übereinstimmung der PID und den Daten im angefragten Nachweis, Gültigkeit der EUDI-Wallet Instanz und des EUDI-Wallet Providers
- Generierung des auszustellenden Nachweises in strukturierten Daten gemäß Schemadefinition
- Integration eines qualifizierten Vertrauensdiensteanbieters (Fernsiegelung) oder Einkauf eines Dienstes zur elektronischen Siegelung für die fortgeschrittene Siegelung des Nachweises
- Bereitstellung des Nachweises und Übermittlung an die EUDI-Wallet
- Verarbeitung von Fehlermeldungen der EUDI-Wallet
- Verarbeitung von Fehlermeldungen des einbezogenen QTSP

Funktionalität 3: Entgegennahme von Nachweisen aus der EUDI-Wallet

Bei der direkten Anbindung an die EUDI-Wallet bedeutet Szenario 3 konkret, dass z.B. ein Onlinedienst im Rahmen der Antragstellung eine Anfrage (auch Request) an die EUDI-Wallet eines Nutzenden stellt, ob ein bestimmter (oder mehrere) Nachweis(e), der oder die erforderlich ist/sind, in der spezifischen EUDI-Wallet des Antragstellenden vorhanden sind. Der Relying Party wird der Zugriff auf die EUDI-Wallet ausschließlich über ein gültiges Registrierungszertifikat ermöglicht, welches dokumentiert, welche Attribute von der Relying Party angefordert werden dürfen und zu welchem Zweck.

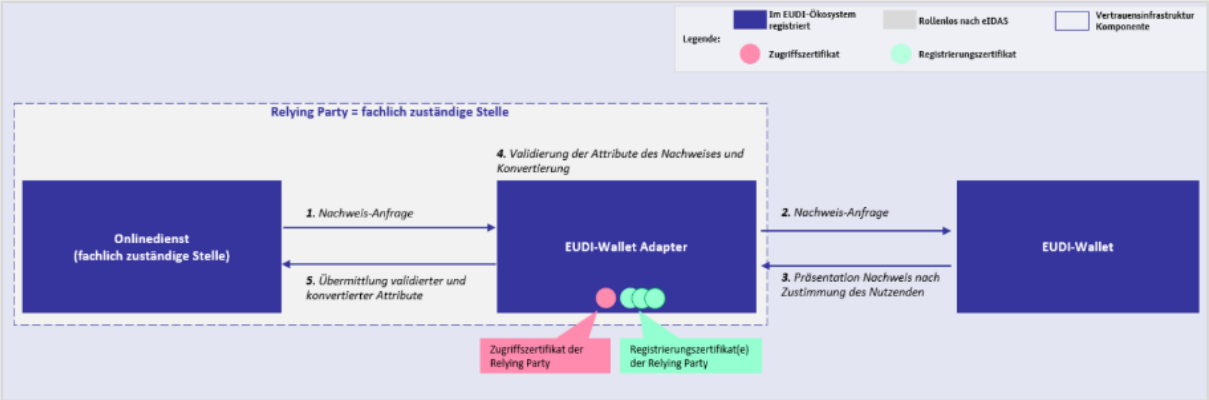

Abbildung 8: Direkte Entgegennahme weiterer Attributsbescheinigungen aus der EUDI-Wallet; Wallet-Adapter im Eigenbetrieb (aktueller Arbeitsstand)

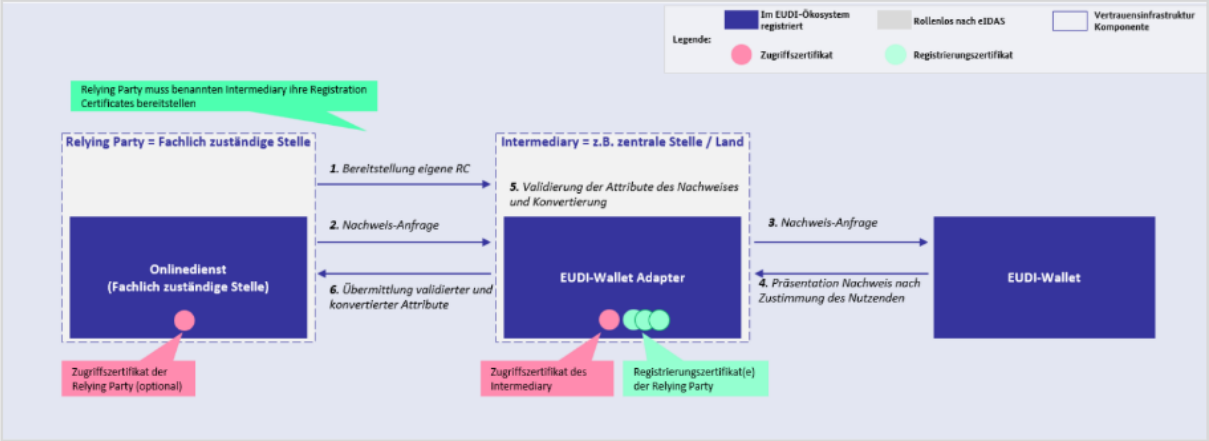

Abbildung 9: Direkte Entgegennahme weiterer Attributsbescheinigungen aus der EUDI-Wallet; Wallet Adapter über zentrale Stelle angebunden (aktueller Arbeitsstand)

Nach aktuellem Sachstand ergeben sich für die fachlich zuständigen Stellen, welche einen Wallet-Adapter betreiben oder welche einen Wallet-Adapter nutzen, der zentral durch ein Bundesland oder eine Kommune betrieben wird, neben den Anforderungen von Funktionalität 1 (Entgegennahme der PID) folgende zusätzliche Anforderungen:

- Beantragung von je einem Registrierungszertifikat pro Anwendungsfall bei der dafür national zuständigen Stelle (= Registrar), einschließlich deren sicheren Speicherung.

Die Beantragung kann dabei je nach Abstimmung mit dem Vermittler direkt durch die Relying Party selbst oder im Auftrag durch den Vermittler erfolgen

- Übermittlung Nachweis Anfrage über den Wallet-Adapter an die EUDI-Wallet (falls die Relying Party die Registrierungszertifikate selbst beantragt hat)
- Erhalt des Nachweises über den Wallet-Adapter und Verarbeitung im Antragsverfahren
- Verarbeitung von Fehlermeldungen des Wallet-Adapters

Nach aktuellem Sachstand ergeben sich für die fachlich zuständigen Stellen, welche keinen Wallet-Adapter betreiben, neben den Anforderungen von Funktionalität 1 (Entgegennahme der PID) folgende zusätzliche Anforderungen:

- Beantragung von je einem Registrierungszertifikat pro Anwendungsfall bei der national zuständigen Stelle (= Registrar), einschließlich deren sicheren Speicherung
- Versand einer Nachweis Anfrage an die EUDI-Wallet
- Erhalt des Nachweises der EUDI-Wallet und Validierung des Nachweises sowie Verarbeitung
- Verarbeitung von Fehlermeldungen der EUDI-Wallet

3.3 Nachweisabruf in die EUDI-Wallet über NOOTS-Infrastruktur

Mittel- bis langfristig sollen Attributsbescheinigungen auf Anfrage der Nutzenden synchron und medienbruchfrei aus (Fach-)Registern oder Datenbeständen, welche an die NOOTS-Infrastruktur angebunden sind für die EUDI-Wallet bereitgestellt werden. Dieser Weg stellt aus Sicht des BMDS den effizientesten und effektivsten Weg der Nachweisausstellung in die EUDI-Wallet für nicht-antragsbezogene Prozesse dar – sowohl für die Nutzenden als auch für die Verwaltung, da durch die Registeranbindung nicht nur die Ausstellung in die EUDI-Wallet, sondern auch gleichzeitig das Once-Only-Prinzip für die behördenübergreifende Kommunikation sichergestellt wird. NOOTS ist eine sichere Transport- und Vermittlungsinfrastruktur, die durch den NOOTS-Staatsvertrag als Verwaltungsstandard festgelegt ist und über die angebundene Register Nachweise und Daten sicher bereitstellen. Registertypen, deren Daten im Rahmen der Registermodernisierung und zur Umsetzung des Once-Only-Prinzips genutzt werden sollen, sind zur Anbindung an das NOOTS verpflichtet. Durch die Anbindung der EUDI-Wallet an die

NOOTS-Infrastruktur zur Bereitstellung von Registerdaten können Aufwände für öffentliche Stellen reduziert werden.

Anforderung an die fachlich zuständigen Stellen ist die Anbindung von Registern an die NOOTS-Infrastruktur. Vor diesem Hintergrund ist es aus Sicht des Bundes essenziell, dass die vorgesehene Anbindung der (Fach-)Register an das NOOTS unvermindert fortgesetzt wird. Die gezielte Verzahnung mit dem Programm der Registermodernisierung und NOOTS wird durch das BVA sichergestellt. Ein gemeinsames Vorhaben zwischen BMDS, BVA und FITKO zur Anbindung der Register an die EUDI-Wallet über die NOOTS-Intrastruktur initiiert. Dafür wird der Wallet-Adapter nachgenutzt, zum NOOTS-spezifischen Issuer-Dienst weiterentwickelt und produktiv eingesetzt. Die Ausgestaltung, einschließlich der Nutzung von Synergien zu DAMAS und NOOTS, wird derzeit gemeinsam mit BVA und FITKO erarbeitet; Detailinformationen zu Datenformaten und Strukturen der Registermodernisierung werden sukzessive geteilt. Nach aktueller Planung soll ein erster Use Case bis zum Januar 2027 im Rahmen eines MVP umgesetzt werden. Dafür wird voraussichtlich für die erste Ausbaustufe des MVP eine Benutzeroberfläche durch das BVA als EAA-Provider bereitgestellt, um ein issuer-initiiertes Kommunikationsszenario für die Ausstellung zu ermöglichen.

3.4 Gegenüberstellung der Anbindungsmöglichkeiten (Funktionalitäts-übergreifend)

Dimension	Indirekte Anbindung über die BundID	Direkte Anbindung an die EUDI-Wallet mit Wallet-Adapter	Direkte Anbindung an die EUDI-Wallet ohne Wallet-Adapter
Technisch	+ Schnittstellennutzung im Identifizierungs-/Authentifizierungsfall reduziert Integrationsaufwand aufgrund Nutzung der BundID + Sicherheitsinfrastruktur senkt techn. Risiken aufgrund bestehender BundID-Mechanismen (Postfachhandle, rechtl. Absicherung) + Änderungen an Spezifikationen und Regularien werden zentral	+ Anbindung mit Wallet-Adapter erhöht Usability; weniger Systemwechsel nötig + Wallet-Adapter erleichtert Anbindung an die EUDI-Wallet und reduziert Eigenentwicklungsaufwände + Änderungen an Spezifikationen und Regularien werden zentral geprüft, Anpassungen implementiert und so Interoperabilität sichergestellt	+ Direktintegration hat die beste Usability; keine zusätzlichen Systemwechsel und Redirects nötig + Optimale Anpassung an Fachverfahren möglich - Hoher initialer Aufwand nötig für die Integration, Implementierung und Testing, inkl. neue Schnittstelle (SST), Validierung, Security-Mechanismen, Zertifikats-Handling

	geprüft, Anpassungen implementiert und so Interoperabilität sichergestellt + Sicherheit ist zentralisiert durch spezialisierten Anbieter der Anbindungslösung gegeben + Übermittlung des Postfach-Handle und der Antrags-ID an die fachlich zuständigen Stellen, wodurch das ZBP sowie die Statusmonitor Funktion genutzt werden kann - Integrationsaufwand durch Schnittstellenwechsel (zu OIDC) für Entgegennahme weiterer Nachweise nötig (Funktionalität 3) - Systemkopplung erhöht Abhängigkeit; BundID-Updates betreffen angebundene Dienste - Flexibilität ist geringer, da unterstützte Prozesse durch die BundID vorgegeben sind - Hohe Komplexität entsteht, wenn Rollen Aussteller und Empfänger von Daten gleichzeitig eingenommen werden - Zentraler Betrieb schafft "Single Point of	+ Einbindung des Wallet-Adapters als Eigenbetrieb oder als Dienst möglich + Sicherheit ist zentralisiert durch spezialisierten Anbieter der Anbindungslösung gegeben - Integrationsaufwand entsteht durch Anbindung des Wallet-Adapters - Techn. Zusatzkomponente Adapter erhöht Komplexität, Adapter-Betrieb, Überwachung und Sicherung (bei dezentralem Betrieb des Wallet-Adapters durch die fachlich zuständige Stelle) - Wenn zentral betrieben: Adapter schafft "Single Point of Failure" für Datenschutz und Datensicherheit - Keine Übermittlung des Postfach-Handle oder der Antrags-ID an die fachlich zuständigen Stellen, wodurch weder das ZBP noch die Statusmonitor Funktion genutzt werden kann	- Regelmäßige selbstständige Prüfung auf Änderungen der Spezifikationen (u.a. OpenID4VP, OpenId4VCI, Haip) und Regularien sowie Anpassungen der SST durch die Onlinedienste notwendig - Betriebs- und Wartungsaufwände entstehen, z. B. Monitoring, Updates - Vollständige technische (Prüf-) Verantwortung liegt bei fachl. zuständiger Stelle - Mehrfachimplementierung derselben Logik zur Nachweiskonvertierung in EUDI-Wallet konforme Formate und -protokolle nötig, da Logik ggf. pro Onlinedienst und Nachweistyp implementiert wird - Keine Übermittlung des Postfach-Handle oder der Antrags-ID an die fachlich zuständigen Stellen, wodurch weder das ZBP noch die Statusmonitor Funktion genutzt werden kann

	Failure" für Datenschutz und Datensicherheit		
Fachlich	+ Auswahl möglich aus versch. Ident-Prozessen der BundID (u. a. EUDI-Wallet) für Behörden (Ausweis, Elster, Nutzender /Passwort) + Gastzugangslogik kann weiterhin genutzt werden + Stammdatenbereitstellung unterstützt bestehende Fachlogiken, z. B. via SAML-Response + Rechtssichere Zustellung von Bescheiden durch Nutzung des ZBP sichergestellt + Nahtlose Nutzung der antragsbezogenen beidseitigen Behördenkommunikation (Bidirektionalität) - Roadmap-Priorisierung steuert Feature-Inhalte, da BundID fachl. Erweiterungen selektiert Nutzende müssen ein BundID-Konto besitzen, um das ZBP nutzen zu können	+ Wallet-Adapter bietet zusätzliche Identifizierungsmöglichkeiten via Onlineausweis, Elster (natürliche Personen und Unternehmen), BundID-Identifikation; Auswahl durch Clients steuerbar + Adapterkonfiguration steuert Umsetzung flexibler, mögliche Anpassungen an Fachprozesse + Adapterintegration ermöglicht einfache Kommunikation zur EUDI-Wallet (Präsentation, Validierung & Ausstellung) + Datenminimierung möglich durch selektive Attributsfreigabe + Zusätzliche Funktionen wie QES-Anbringung zukünftig Teil des Wallet-Adapters - Keine rechtssichere Zustellung von Bescheiden durch direkte Nachweisausstellung möglich Keine bidirektionale antragsbezogene Kommunikation zwischen Nutzenden und fachlich zuständigen Stellen möglich, um bspw. Rückfragen zu fehlenden Antragsdaten zu stellen	+ Fachstellen steuern Umsetzung und Integration in bestehende Prozesse flexibel und angepasst an spezifische Verwaltungsprozesse - Keine rechtssichere Zustellung von Bescheiden durch direkte Nachweisausstellung möglich - Keine bidirektionale antragsbezogene Kommunikation zwischen Nutzenden und fachlich zuständigen Stellen möglich, um bspw. Rückfragen zu fehlenden Antragsdaten zu stellen - Keine rechtssichere Zustellung von Bescheiden durch direkte Nachweisausstellung gegeben
Organisatorisch	+ Zentrale Relying-Party reduziert Aufwand für	+ Zentral betriebener Adapter erlaubt föderale	+ Direkte Relying-Party-Rolle stärkt Autonomie,

	einzelne Stellen (keine Einzelregistrierung für PID und Ausstellung über ZBP) + Klare Governance und Priorisierung der Weiterentwicklung durch BMDS gegeben + Betriebskosten geringer & Anbindung vereinfacht durch Nutzung bestehender Infrastruktur, insb. für Kommunen - Releasezyklen begrenzen Handlungsspielraum durch zentrale BundID Roll-outs & Timings; trotz Ankündigung von Wartungsfenstern Prüfung von Datenminimierung durch Aufsichtsbehörden und NGOs schwieriger	Skaleneffekte (geteilte Infrastruktur Länder–Kommunen) + Kontinuierliche Weiterentwicklung + Zertifikatsmanagement und automatisierte Erneuerung durch Wallet-Adapter möglich - Adapter bringt organisatorische Pflichten mit, z. B. Betrieb, Weiterentwicklung, Zertifikate - Abhängigkeit von (zentralem) Adapter hinsichtlich Weiterentwicklungen kann den Handlungsspielraum begrenzen (z. B. Erweiterungswünsche Funktionalitäten) Klare Governance zwischen Adapter-Betreiber und Fachressorts nötig, z.B. Klärung von Verantwortlichkeiten	insb. bei größeren & strategischen Akteuren + Governance der Fachressorts und fachspezifischen Anforderungen nachnutzbar - Organisatorische Pflichten der Direktanbindung erhöhen Last, z. B. Zertifikatsmanagement, Audits, Security, Konformitätsbewertung - Kleinere Stellen benötigen externe Unterstützung, da Ressourcen und Expertise fehlen Hohe Integrations-, Betriebs- und Wartungskosten

Tabelle 4: Gegenüberstellung der Vor- und Nachteile der Anbindungsmöglichkeiten

4 Nachweisausstellung und Verifikation

4.1 Zielbild der flächendeckenden Ausstellung aus Verwaltungssicht

Das Zielbild der flächendeckenden Ausstellung aus Verwaltungssicht beschreibt die Ausstellung von Nachweisen in die EUDI-Wallet als integralen Bestandteil der Verwaltungsverfahren auf Bundes-, Landes- und kommunaler Ebene.

Antragsbezogene Verfahren werden auf Wunsch des Antragstellenden nach Abschluss der fachlichen Prüfung durch die fachlich zuständige Stelle des Nachweises in die EUDI-Wallet ausgestellt (Push-Verfahren). Dies kann entweder (1) indirekt über das ZBP der BundID, (2a) direkt

durch die fachlich zuständige Stelle[11] oder (2b) über den Zentralen Issuer-Dienst (ZID) des Bundes erfolgen (siehe Abbildung 10). Der ZID ist ein zentraler Dienst, der die Rolle eines (Q)EAA-Providers (1. Ausbaustufe EAA-Provider; 2. Ausbaustufe (Q)EAA-Provider) inkl. Siegel-/Signaturprozessen auf Basis eines fortgeschrittenen bzw. qualifizierten elektronischen Siegels übernimmt.

Nicht-antragsbezogene Verfahren werden im Pull-Verfahren über die NOOTS-Infrastruktur bedient. Perspektivisch werden auf Wunsch des Nutzenden der Abruf eines Attributs direkt aus dem an NOOTS angebundenen Register initiiert – ohne vorgelagertes Antragsverfahren (siehe Kapitel 3.3. Nachweisabruf in die EUDI-Wallet über NOOTS-Infrastruktur). Dieses Verfahren eignet sich insbesondere kurzfristig für Nachweise wie Wohnsitz-, Ausbildungs- oder steuerliche Angaben, welche kein Antragsverfahren voraussetzen. Perspektivisch kann die Nachweisbeschaffung über ein Antragsverfahren sowie über den Abruf über die NOOTS-Infrastruktur erfolgen. Hiermit können die Anwendungsfälle mit einem Nachweisabruf aus der NOOTS-Infrastruktur erhöht werden. Durch eine Registeranbindung haben damit fachlich zuständige Stellen die Möglichkeit, Nachweise in die EUDI-Wallet auszustellen sowie gleichzeitig das Once-Only-Prinzip für die Behörde-zu-Behörde Kommunikation umzusetzen.

[11] Die fachlich zuständige Stelle ist in der Rolle der Relying Party (Issuer), konkret (Q)EAA-Provider

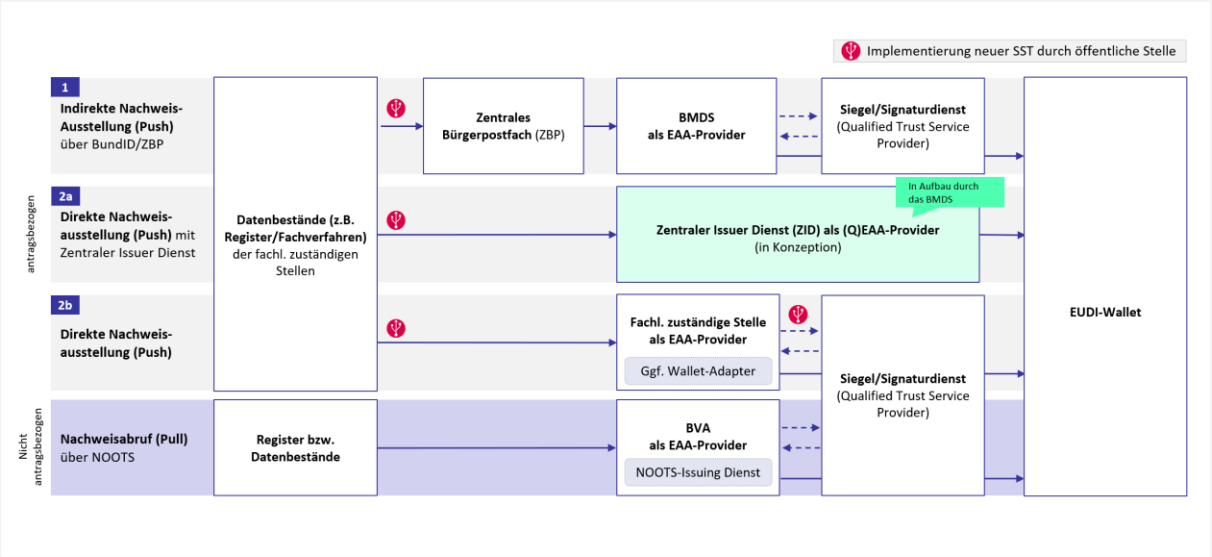

Abbildung 10: Anbindungsoptionen zum Zielbild Nachweisausstellung

4.2 Elektronische Attributsbescheinigungen - EAA, QEAA und Pub-EAA

Eine elektronische Attributsbescheinigung kann sowohl in qualifizierter Form als QEAA durch einen Vertrauensdiensteanbieter als auch nicht qualifiziert als EAA ausgestellt werden. Darüber hinaus gibt es elektronische Attributsbescheinigungen, die von oder im Namen einer für eine authentische Quelle zuständigen öffentlichen Stelle ausgestellt werden (Pub-EAA) (vgl. Art. 4, Nr. 46 eIDAS-VO).

EAAs können von unterschiedlichen Anbietern ausgestellt werden, sofern die technischen Anforderungen zur Anbindung an die EUDI-Wallet eingehalten werden, insbesondere in Bezug auf standardisierte Schnittstellen und unterstützte Datenformate sowie Semantik. EAAs müssen kryptographisch gesichert sein, unterliegen jedoch keinen qualifikationspflichtigen Aufsichts- oder Zertifizierungsverfahren. Sie haben damit keine automatische rechtliche Gleichstellung mit Papiernachweisen. EAAs eignen sich daher vor allem für Anwendungsfälle, bei denen keine hohen Anforderungen an die rechtliche Verbindlichkeit bestehen.

QEAAs dürfen ausschließlich von qualifizierten Vertrauensdiensteanbietern (QEAA-Provider) ausgestellt werden, die von der nationalen Aufsicht der Bundesnetzagentur (BNetzA) benannt und in der nationalen Vertrauensliste[12] geführt werden. Vor der Ausstellung einer QEAA ist eine qualifizierte Identitäts- und Attributsprüfung der betroffenen natürlichen oder juristischen Person erforderlich. Technisch müssen QEAA eine definierte Menge verpflichtender Metadaten enthalten, darunter Angaben zum ausstellenden QTSP, zur Gültigkeitsdauer, zu den bescheinigten Attributen sowie eine qualifizierte elektronische Signatur bzw. Siegel. Aufgrund dieser Eigenschaften besitzen QEAAs die gleiche rechtliche Wirkung wie entsprechende amtlich beglaubigte Papierbescheinigungen und sind insbesondere für rechtlich relevante Verwaltungs- und Geschäftsprozesse vorgesehen (Art. 45b Abs. 2 eIDAS-VO 910/2014).

PuB-EAAs bilden laut der Definition der eIDAS-VO eine eigenständige Kategorie für elektronische Attributsbescheinigungen, die von oder im Namen einer öffentlichen Stelle ausgestellt werden, welche für eine sogenannte authentische Quelle verantwortlich ist (Art. 45f Abs. 3 eIDAS-VO 910/2014), etwa ein amtliches Register oder ein behördliches Fachverfahren. Die Vertrauenswürdigkeit ergibt sich hier weniger aus einer Qualifikation als Vertrauensdiensteanbieter, sondern aus der hoheitlichen Rolle der ausstellenden Stelle und der rechtlich gesicherten Qualität der zugrunde liegenden Daten. Auch PuB-EAAs müssen fest definierte Pflichtinformationen enthalten und qualifiziert signiert oder gesiegelt werden. Sie sind rechtlich QEAAs gleichgestellt und müssen darüber hinaus grenzüberschreitend in allen Mitgliedstaaten anerkannt werden.

Ein Entscheidungsleitfaden[13] zur Unterstützung der Auswahl eines geeigneten Attestierungstyps für einen konkreten Anwendungsfall ist im nationalen Blueprint zu finden.

[12] https://eidas.ec.europa.eu/efda/trust-services/browse/eidas/tls

[13] https://bmi.usercontent.opencode.de/eudi-wallet/eidas-2.0-architekturkonzept/content/ecosystem-architecture/trust/decision-guide/#choosing-the-right-attestation-type

4.3 Anforderungen an Provider

Provider elektronischer Attributsbescheinigungen sind zentrale Akteure im EUDI-Wallet-Ökosystem. Sie sind für die rechtssichere Ausstellung, kryptografische Sicherung und Bereitstellung von Attributen verantwortlich, die in der EUDI-Wallet gespeichert und gegenüber Dritten vorgelegt werden können. Alle bescheinigten Attribute müssen maschinenlesbar, kryptografisch gesichert und eindeutig dem ausstellenden Provider zuordenbar sein. Die einheitliche Identitätsabsicherung von Providern erfolgt über das Zugriffszertifikat, die von einem Registrar ausgegeben werden. Ein Zugriffszertifikat bindet die rechtliche Identität des Providers, legt die technische Rolle im EUDI-Wallet-Ökosystem fest und ermöglichen eine sichere Interaktion mit der EUDI-Wallet. Nicht festgelegt wird durch das Zugriffszertifikat, welchen Beweiswert eine ausgestellte Attestierung hat oder ob er zur Ausstellung bestimmter Attribute berechtigt ist.

EAA-Provider können private oder öffentliche Stellen sein. Mindestanforderungen ergeben sich aus dem Anhang der Durchführungsverordnung (DVO) 2025/2160 sowie aus ETSI 319401 V3.2.1 (2026-01). Sie sind verpflichtet, die technischen Schnittstellen der EUDI-Wallet-Infrastruktur zu implementieren und die Integrität sowie die Authentizität der ausgestellten Bescheinigungen sicherzustellen.

QEAA-Provider müssen durch die zuständige nationale Aufsichtsstelle anerkannt und in der nationalen Vertrauensliste geführt sein. Die Anforderungen an QEAA-Provider sind verbindlich in Anhang V der eIDAS-VO geregelt. Zudem ist jeder Nachweis mit einem qualifizierten elektronischen Siegel zu versehen. Der QEAA-Provider muss darüber hinaus einen Dienst zur Prüfung des Gültigkeits- und Widerrufsstatus bereitstellen. QEAA-Provider sind verpflichtet, vor der Ausstellung einer Bescheinigung die Identität der betroffenen Person oder Organisation sowie die Richtigkeit der zugrunde liegenden Attribute zu prüfen.

Öffentliche Stellen, die für eine authentische Quelle verantwortlich sind (Pub-EAA Provider), können selbst oder im Auftrag Nachweise (Pub-EAAs) ausstellen; diese besitzen dieselbe Rechtswirkung wie QEAA. Öffentliche Stellen, die als Pub-EAA-Provider auftreten, müssen ein Maß an organisatorischer Sicherheit, Zuverlässigkeit und Vertrauenswürdigkeit gewährleisten,

welches dem eines qualifizierten Vertrauensdiensteanbieters entspricht (Art. 45f Abs. 2 eIDAS-VO 910/2014). Die inhaltlichen Mindestanforderungen an Pub-EAA sind in Anhang VII der eIDAS-VO festgelegt. Sie verantworten die Ausstellung qualifizierter Attributsbescheinigungen eigenständig oder unter Einbindung eines qualifizierten Vertrauensdiensteanbieters. Die Mitgliedstaaten sind verpflichtet, diese Stellen zu benennen, ihre Konformität zu prüfen und sie gegenüber der Europäischen Kommission zu melden, damit sie in eine europaweite, maschinenlesbare Liste der Pub-EAA-Anbieter aufgenommen werden.

4.4 Verifikationsmechanismus für QTSPs

Kriterium	Verifikation durch eine Relying Party	Verifikationsmechanismus für QTSPs
Gegenstand	Prüfung des Providers gegen Trusted List, des Ablaufdatum und Widerruf des Nachweises, der Echtheit der Signatur/Siegel, des Device und User Binding, der Einhaltung der Schemadefinition des Nachweises	Prüfung der fachlichen Richtigkeit eines Attributwerts gegenüber einer Authentischen Quelle bzw. national anerkannten Überprüfungsstelle
Akteur	Relying Parties (z.B. Fachverfahren)	Qualifizierte Vertrauensdiensteanbieter (QTSPs) ggf. mit Hilfe zentraler nationaler Überprüfungsstellen, Single Points of Verification (SPoV)
Auslöser	Automatisch bei Entgegennahme eines Nachweises	Ausschließlich auf Veranlassung der nutzenden Person

Tabelle 5: Abgrenzung Begriffe der Verifikation

Im Rahmen der eIDAS-VO sowie der hierzu erlassenen DVO (EU) 2025/1569, sind die Mitgliedstaaten verpflichtet, einen elektronischen, auf Veranlassung der Nutzenden auszulösenden Mechanismus zur Verifikation von Attributwerten bereits ausgestellter Attribute durch QTSPs bereitzustellen. Dieser fachliche Überprüfungsmechanismus muss eine zeitnahe Durchführung ermöglichen, ohne dass eine Echtzeitverifikation vorgeschrieben wäre. Die Mitgliedstaaten können, aber sind nicht verpflichtet dazu, hierfür zentrale nationale Überprüfungsstellen, sogenannte Single-Points-of-Verification (SPoV), einrichten, die als zentrale Schnittstellen gegenüber einem QTSP fungieren. QTSP müssen die Möglichkeit besitzen, die von Nutzenden angefragte Überprüfung von Attributswerten gegenüber einer authentischen Quelle oder einem auf nationaler Ebene anerkannten benannten Dritten durchzuführen. Gegenstand dieser

Überprüfung ist ausschließlich die Bestätigung oder Nicht-Bestätigung von Attributwerten bereits ausgestellter Attribute gemäß Anhang VI; ein inhaltliches Ergebnis wird hierbei nicht übermittelt. Der Überprüfungsmechanismus umfasst somit keine Herausgabe oder inhaltliche Offenlegung des Attributs selbst. Der Einsatzzweck dieses Mechanismus liegt aus Nutzendensicht insbesondere in der reinen Verifikation von Attributwerten bereits ausgestellter Nachweise, vor allem in der fachlichen Korrektheit von Attributen, die in der EUDI-Wallet gespeichert sind. Der Einsatzzweck dieses Mechanismus kann aus Nutzendensicht für die reine Verifikation von Attributwerten bereits ausgestellter Nachweise in der EUDI-Wallet dienen, welcher aus der EUDI-Wallet heraus getriggert wird. Daneben kann der Mechanismus im Ausstellungsprozess qualifizierter Nachweise nachgenutzt werden, etwa wenn ein papierbasierter Nachweis in einen qualifizierten elektronischen Nachweis, d.h. QEAA bzw. Pub-EAA überführt werden soll. In diesem Fall verifiziert ein QTSP die relevanten Attributwerte gegenüber einer authentischen Quelle und stellt sie anschließend als QEAA bzw. Pub-EAA in der EUDI-Wallet der nutzenden Person aus. Beispielsweise wenn ein Bürger oder eine Bürgerin einen vorliegenden Nachweis in Papierform als qualifizierten Nachweis in die EUDI-Wallet ausgestellt bekommen möchte. In diesem Fall kann der QTSP die Attribute aus dem Nachweis in Papierform über den Mechanismus verifizieren und anschließend als QEAA in die EUDI-Wallet des Nutzenden ausstellen.

Für fachlich zuständige Stellen ergeben sich aus diesem Verifikationsmechanismus zusätzliche Anforderungen, die jedoch weitgehend auf bewährten Verfahren einer fachlichen Verifikation aufsetzen. Das BMDS plant hierfür zunächst ein MVP bis Januar 2027 umzusetzen, das grundlegende Verifikationsabläufe bereitstellt und schrittweise erweitert wird. Damit wird eine rechtskonforme Lösung geschaffen, die fachlich zuständige Stellen mit geringem Implementierungsaufwand nachnutzen können und die zugleich eine spätere Skalierung in das vollumfängliche Zielbild ermöglicht.

5 Weiteres Vorgehen und Ausblick

Für den erfolgreichen Roll-out der EUDI-Wallet ist eine früh abgestimmte Zusammenarbeit von Bund, Ländern und Kommunen von zentraler Bedeutung. Vor diesem Hintergrund erprobt das BMDS gemeinsam mit der Landeshauptstadt Dresden, der Sächsischen Staatskanzlei und der BundID die konkrete Anbindung der kommunalen Verwaltung an die EUDI-Wallet. Dabei werden exemplarische kommunale Prozesse betrachtet und daraus resultierende fachliche, technische sowie organisatorische Anforderungen sukzessive identifiziert. Zur Erfüllung der verpflichtenden Anforderungen der eIDAS-Verordnung empfiehlt sich für fachlich zuständige Stellen eine frühzeitige Fokussierung auf die Anbindung der BundID. Es wird empfohlen, frühzeitig zu prüfen, welche Optionen der Ausstellung von Nachweisen (vgl. Abbildung 10) einen Mehrwert bieten. Zudem sollte die Bereitstellung standardisierter, strukturierter und maschinenlesbarer Registerdaten über etablierte Schnittstellen weiterverfolgt werden.

Zur Sicherstellung der Interoperabilität werden zentrale Komponenten durch den Bund bereitgestellt. Dazu zählen die Anbindung der BundID an die EUDI-Wallet, ein nachnutzbarer Wallet-Adapter im Produktportfolio des IT-PLR sowie die Anbindung der EUDI-Wallet an die NOOTS-Infrastruktur. Aktuell wird die Bereitstellung eines zentralen Issuer-Dienstes evaluiert. Grundlage für die Nachnutzung eines solchen zentralen Issuer-Dienst durch die Länder (einschließlich ihrer Kommunen) soll eine Verwaltungsvereinbarung zwischen Bund und Ländern sein, die im nächsten Schritt erarbeitet und abgestimmt werden soll.

Zur Vorbereitung auf das mittel- bis langfristige Zielbild der direkten Anbindung an die EUDI-Wallet dient die von SPRIN-D bereitgestellte Sandbox[14] als offene Test- und Erprobungsumgebung. Diese ist seit Dezember 2025 für Bund, Länder, Kommunen und jeweilige Dienstleister geöffnet, um Anwendungsfälle frühzeitig zu validieren. Eine Teilnahme an der Sandbox ist kostenlos. Die Finanzierung der fachlichen Umsetzung in den Verfahren der Länder und Kommunen obliegt den jeweiligen Ländern und Kommunen. Seit April dieses Jahres ist zudem die

[14] Weitere Informationen zur SPRIN-D Sandbox unter https://eudi-wallet.gov.de/en/ecosystem-knowledge-center

offizielle EUDI-Wallet Webseite[15] online und dient als zentrale Informationsplattform für Bürgerinnen und Bürger, Verwaltungen, Unternehmen und potenzielle Partner.

Der Bund bereitet zudem eine Informations- und Kommunikationskampagne vor, die Transparenz schafft und Bürgerinnen und Bürger umfassend über Nutzen und Anwendung der EUDI-Wallet informiert. Die Umsetzung ist für Ende 2026 sowie für das Jahr 2027 vorgesehen. Ergänzend entsteht über den Orchestrator eine zentrale Anlaufstelle mit Self-Service-Bereich und Supportangeboten für alle Zielgruppen. Darüber hinaus verfolgt der Bund eine gezielte Befähigung von Multiplikatorinnen und Multiplikatoren sowie der Länder, um den Wissenstransfer und eine einheitliche Umsetzung zu fördern. Der Aufbau von Netzwerken (auch Community-Strukturen) zur strukturierten Unterstützung und zum Erfahrungsaustausch sowie die Nutzung von Erkenntnissen aus Pilotprojekten sollen Länder und Kommunen in ihrer Vorbereitung unterstützen und den flächendeckenden Roll-out erleichtern

6 Fazit und Empfehlung

Die EUDI-Wallet bildet mit ihrer Identifizierungs- und Authentifizierungsfunktion sowie den strukturierten, digital nutzbaren und europaweit interoperablen Nachweisen eine zentrale Grundlage für medienbruchfreie und automatisierbare Verwaltungsprozesse. Sie schafft die Voraussetzung für eine skalierbare Infrastruktur, die Abläufe beschleunigt, Redundanzen reduziert und eine konsistente Zusammenarbeit über föderale Ebenen hinweg ermöglicht. Für fachlich zuständige Stellen ergeben sich daraus verbindliche technische und organisatorische Anforderungen. Die EUDI-Wallet ist gemäß eIDAS-Verordnung als Identifizierungs- und Authentifizierungsmittel in allen digitalen Verfahren zu akzeptieren, in denen eine starke Nutzerauthentifizierung zwingend erforderlich ist. Die BundID stellt die rechtskonforme indirekte Anbindung sicher. Das mittel- bis langfristige Zielbild empfiehlt fachlich zuständigen Stellen aus Ländern und Kommunen eine direkte Anbindung der EUDI-Wallet – mit oder ohne Nutzung des Wallet-Adapters – zusätzlich zur Anbindung an die BundID. Die Empfehlung orientiert

[15] Offizielle EUDI-Wallet Webseite unter https://eudi-wallet.gov.de/

sich an den im Konzept beschriebenen Vorteilen, insbesondere im Hinblick auf Nutzendenfreundlichkeit und Automatisierungspotenzialen.

Hieraus resultieren die folgenden Handlungsbedarfe für die öffentliche Verwaltung, die aktuell zu adressieren sind:

- **01 Vorbereitung der Identifizierung und Authentifizierung**
  Onlinedienste, welche eine starke Nutzerauthentifizierung voraussetzen, die mit einem Vertrauensniveau „hoch" gleichzusetzen ist, sind verpflichtend, die EUDI-Wallet als Mittel zur Identifizierung und Authentifizierung einzubinden. In diesem Zusammenhang ist durch Länder und öffentliche Stellen zu prüfen, für welche Onlinedienste diese Verpflichtung zutrifft, und festzustellen, ob bereits eine Anbindung dieser Onlinedienste an die BundID besteht. Soweit eine Anbindung an die BundID besteht oder vorgesehen ist, kann die gesetzliche Verpflichtung vollständig über die indirekte Anbindung an die EUDI-Wallet erfüllt werden. Eine unmittelbare technische Anbindung einzelner Dienste an die EUDI-Wallet ist zur Erfüllung dieser gesetzlichen Pflicht nicht erforderlich.
- **02 Vorbereitung der Nachweisausstellung**
  Es wird Ländern und öffentlichen Stellen auch ohne rechtliche Verpflichtung empfohlen, vorbereitend zu ermitteln, für welche Nachweise eine Ausstellung durch die jeweils fachlich zuständige Stelle in den eigenen Zuständigkeitsbereichen künftig sinnvoll erscheint. In diesem Zusammenhang obliegt es den Ländern und fachlich zuständigen Stellen, ihre Zuständigkeitsbereiche zu analysieren und geeignete Nachweistypen zu identifizieren. Außerdem ist empfohlen festzulegen, ob eine Ausstellung über bestehende Infrastrukturen wie das ZBP, über zentrale Issuer-Dienste oder perspektivisch über direkte Anbindungen erfolgen soll. Die fachlich zuständigen Stellen können die benötigten Nachweisschemata entweder selbst definieren oder auf bereits veröffentlichte Nachweisschemata anderer Stellen zur Nachnutzung zurückgreifen. Hierbei

wird auf die Synergiepotenziale mit der Registermodernisierung verwiesen (vgl. Handlungsbedarf Nr. 05). In diesem Kontext ist ausdrücklich zu berücksichtigen, dass die jeweils anbindende Stelle die Rolle einer Relying Party in der Funktion eines (Q)EAA-Providers bei einer direkten Anbindung an die EUDI-Wallet übernimmt – unabhängig davon, ob diese über einen zentral durch ein Land oder eine zentrale öffentliche Stelle betriebenen Wallet-Adapter oder ohne Nutzung eines Wallet-Adapters erfolgt. Damit geht die Verantwortung einher, die einschlägigen technischen, organisatorischen und rechtlichen Anforderungen der eIDAS-Verordnung zu erfüllen. Diesen Anforderungen sind insbesondere in Bezug auf Registrierung, Zertifikatsmanagement, Ausstellung, Siegelung sowie die Einhaltung der Anforderungen an elektronische Attributsbescheinigungen zu berücksichtigen.

- **03 Vorbereitung der Nachweisentgegennahme**

  Es wird Ländern und öffentlichen Stellen empfohlen, vorbereitend zu ermitteln, bei welchen Onlinediensten zukünftig die Entgegennahme von Nachweisen – insbesondere aus der Privatwirtschaft – über die EUDI-Wallet entgegenzunehmen sind. Sofern öffentliche Stellen Nachweise aus der EUDI-Wallet entgegennehmen, sind sie verpflichtet, deren Echtheit des Siegels und Gültigkeit anhand der im EUDI-Ökosystem vorgesehenen kryptographischen Sicherungen und Vertrauensmechanismen zu prüfen. Der Bund prüft aktuell die Bereitstellung einer Prüfkomponente für die Vor-Ort-Prüfung im Sinne des Proximity-Sharings.

- **04 Weiterentwicklung von Online-Verfahren und Auswahl von Anbindungsoptionen**

  Es ist durch Länder und öffentliche Stellen festzulegen, in welcher Form und in welchen Ausbaustufen die Mehrwerte der EUDI-Wallet in den jeweiligen Online-Verfahren genutzt werden sollen. Hierzu wird ein fachlicher Austausch mit BMDS und SPRIND empfohlen, um gemeinsam Anwendungsfälle zu definieren. Länder sollten gemeinsam mit ausgewählten fachlich zuständigen Stellen eine Erprobung in der

Sandbox mit konkreten Anwendungsfällen v.a. für die frühzeitige Weiterentwicklung von föderal nachnutzbaren Basiskomponenten aktiv fördern.

- **05 Fortführung der Registeranbindung**
  Unabhängig von der EUDI-Wallet verbleibt für die Länder ein zentraler, verpflichtender Aufgabenbereich in der Fortführung der Registeranbindung an die NOOTS-Infrastruktur. Die Anbindung registerführender Stellen an NOOTS ist sowohl Voraussetzung für die Umsetzung des Once-Only-Prinzips als auch für mittel- bis langfristige Szenarien der Nachweisausstellung in die EUDI-Wallet auf Basis registergestützter Daten. Das Konzept stellt klar, dass die Nutzung der EUDI-Wallet die Registermodernisierung nicht ersetzt, sondern auf dieser aufsetzt. Für Länder ergibt sich daher der fortwährende Handlungsbedarf, bestehende Registeranbindungen konsequent weiterzuführen. Mit der Anbindung der Register an NOOTS werden die Vorgaben der Registermodernisierung erfüllt und gleichzeitig die Grundlage geschaffen, Registerdaten direkt zur Ausstellung von Nachweisen in der EUDI-Wallet zu verwenden, da die Anbindung der NOOTS-Infrastruktur an die EUDI-Wallet durch den Bund sichergestellt wird.
- **06 Governance, Betrieb und Nachnutzung zentraler Komponenten**
  Bei der Auswahl von Anbindungsoptionen sind Aspekte wie der Betrieb eines Wallet-Adapters oder weiterer technischer Komponenten, die die Anbindung an die EUDI-Wallet für öffentliche Stellen technisch erleichtern, zu berücksichtigen und zu klären. Dies betrifft insbesondere Fragen der Verantwortlichkeiten, der Betriebsmodelle sowie der Finanzierung, des Monitorings und des Zertifikatsmanagements. Auch diese Aspekte sind nicht rechtlich verpflichtend, jedoch für eine effiziente und föderal anschlussfähige Nutzung der EUDI-Wallet über die reine Mindestanforderung hinaus relevant.
- **07 Vorbereitung von Testaktivitäten in der EUDI-Wallet-Sandbox**
  Geeignete Anwendungsfälle können durch fachlich zuständige Stellen in der EUDI-Wallet-Sandbox erprobt werden, um frühzeitig praxisnahe Erkenntnisse zu gewinnen.

Fachlich zuständige Stellen können insbesondere die Integrationsleitfäden für Relying Parties und/oder EEA Issuer[16] sichten, um die bevorstehenden Integrationsschritte und die Gesamt-Journey nachvollziehen zu können. Ergänzend kann die Readiness Checklist[17] genutzt werden, um den Vorbereitungsgrad der eigenen Organisation strukturiert zu bewerten sowie identifizierte Lücken gezielt zu adressieren. Darüber hinaus empfiehlt sich eine frühzeitige Auseinandersetzung mit den verfügbaren Support-Ressourcen[18], um die Erprobung und spätere Umsetzung effizient zu unterstützen. Dies ist ausschließlich relevant für Stellen, die eine direkte Anbindung an die EUDI-Wallet (mit oder ohne Wallet-Adapter) vorbereiten. Länder sollten eine Erprobung in der Sandbox v.a. für die frühzeitige Weiterentwicklung von föderal nachnutzbaren Basiskomponenten aktiv fördern. Für eine Anbindung über die BundID ist die Nutzung der Sandbox nicht erforderlich. Soweit Wallet-Adapter, Issuer-Dienste oder weitere technische Komponenten zentral durch Länder betrieben oder koordiniert werden sollen, sind frühzeitig Verantwortlichkeiten, Betriebsmodelle sowie Fragen der Finanzierung, des Monitorings und des Zertifikatsmanagements zu klären. Auch diese Aspekte sind nicht rechtlich verpflichtend, jedoch Voraussetzung für eine koordinierte, effiziente und föderal anschlussfähige Nutzung der EUDI-Wallet über die reine Mindestanforderung hinaus.

Die bisherigen Pilotierungen zeigen, dass frühzeitige Use-Case-Definition, Nutzung der Testmöglichkeiten der Sandbox, Klärung rechtlicher Rahmenbedingungen, föderale Koordination, die rechtzeitige Befähigung zentraler Basisdienste sowie durchgehend digital gedachte Ende-zu-Ende-Prozesse entscheidend sind, um die Potenziale der EUDI-Wallet vollständig zu erschließen. Die Umsetzung setzt voraus, dass fachlich zuständige Stellen sowohl technische

[16] Weiterführende Informationen zum Sandbox Onboarding und Integration unter https://bmi.usercontent.opencode.de/eudi-wallet/developer-guide/eaa/onboarding/overview/
[17] Readiness Checkliste unter https://bmi.usercontent.opencode.de/eudi-wallet/developer-guide/rp/Sandbox_Readiness_Checklist/
[18] Verfügbare Sandbox Support Ressourcen unter https://bmi.usercontent.opencode.de/eudi-wallet/developer-guide/Sandbox_Support_Resources_Overview/

Mindestvoraussetzungen als auch organisatorische Zuständigkeiten frühzeitig adressieren und ihre Verfahren systematisch auf die künftige Nutzung der EUDI-Wallet ausrichten.

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

Begriff/Abkürzung	Begriffsbestimmung
ARF	Architecture and Reference Framework
BundID	Zentrale Komponente des Bundes zur sicheren, einfachen und flexiblen Identifizierung und Authentifizierung gegenüber digitalen Verwaltungs-leistungen
DAMAS	Daten- und Nachweismanagement System der öffentlichen Verwaltung
DVO	Durchführungsverordnung / Implementing Act
EAA	Electronic attestation of attributes / Elektronische Attributsbescheinigung
eID	elektronische Identitätsfunktion des Personalausweises
eIDAS	electronic IDentification, Authentication and trust Services / elektronische Identifizierung, Authentifizierung und Vertrauensdienste
eS	Elektronische Signatur/Siegel
EU	European Union / Europäische Union
EUDI	European Digital Identity / Europäische Digitale Identität
EUDI-Wallet	European Digital Identity Wallet / Europäische Digitale Identitätsbrieftasche
EU-OOTS	EU-Once-Only-Technical-System
FES	Fortgeschrittene elektronische Signatur/Siegel
Haip	High Assurance Interoperability Profile
JSON	JavaScript Object Notation
MVP	Minimum Viable Product (dt. „minimal brauchbares oder existenzfähiges Produkt“)
NOOTS	National Once-Only-Technical-System
OIDC	OpenID Connect
OpenID4VP	OpenID for Verifiable Presentations 1.0
OpenID4VCI	OpenID for Verifiable Credential Issuance 1.0
OZG	Onlinezugangsgesetz
PID	Personal Identification Data/ Personenidentifizierungsdaten
Pub-EAA	Elektronische Attributsbescheinigung öffentlicher Stellen / Public Body Electronic Attestation of Attributes
Pub-EAA Provider	Public Body Electronic Attestation of Attributes Provider / Aussteller elektronischer Attributsbescheinigung öffentlicher Stellen

QEAA	Qualified Electronic Attestation of Attributes / Qualifizierte elektronische Attributsbescheinigung
QES	Qualifizierte elektronische Signatur
QTSP	Qualified Trust Service Provider / Qualifizierter Vertrauensdiensteanbieter
RP	Relying Party / vertrauende Partei bzw. Stelle
SAML	Security Assertion Markup Language
SDG	Single Digital Gateway / einheitliches digitales Zugangstor
SD-JWT-VC	Selective Disclosure JSON Web Token – Verifiable Credential
SST	Schnittstelle
ZBP	Zentrales Bürgerpostfach der BundID
ZID	Zentraler Issuer Dienst

7 Anhang

I. Beschreibung relevanter Rollen und Komponenten

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 ist (Art. 3 Abs. 47 eIDAS-VO 910/2014). 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-VO definierte Mindestliste an Attribute müssen elektronisch durch QTSPs überprüfbar sein, sofern sie aus Authentischen Quellen des öffentlichen Sektors stammen (Artikel 45e i. V. m. Anhang VI eIDAS-VO 910/2014).

Relying Party

Relying Parties sind natürliche Personen oder Organisationen, die auf eine elektronische Identifizierung vertrauen – etwa durch eine EUDI-Wallet, andere elektronische Identifizierungsmittel oder Vertrauensdienste (Art. 3 Nr. 6 eIDAS-VO 910/2014). Relying Parties können von EUDI-Wallet-Nutzenden 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 überprüfen (Art. 5a Abs. 5a ii eIDAS-VO 910/2014). Im EUDI-Wallet-Ökosystem kann eine Relying Party zwei unterschiedliche Rollen einnehmen: Als Relying Party (Issuer) stellt diese Nachweise für Wallet-Nutzende bereit, die anschließend in der EUDI-Wallet gespeichert und gegenüber anderen Stellen verwendet werden können. Als Relying Party (Verifier) prüft diese die durch Wallet-Nutzende präsentierte Nachweise auf deren Echtheit des Siegels und Gültigkeit. Beide Rollen unterliegen denselben Registrierungs- und Zertifikatsanforderungen, unterscheiden sich jedoch funktional: Issuer erzeugen und siegeln/signieren Nachweise, während Verifier diese Nachweise im Rahmen eines Prozesses verifizieren, und zweckgebunden nutzen.

Zu Zweck des Onboardings ist eine vorherige Registrierung bei der zuständigen nationalen Registrierungsstelle – dem sogenannten Relying Party Registrar – erforderlich (Art. 5b Abs. 1 und 3 eIDAS-VO 910/2014). Dafür müssen Relying Parties Daten zur Ausstellung eines Zugriffs- und Registrierungszertifikates bereitstellen:

- Das Zugriffszertifikat dient der Authentifizierung der Relying Party gegenüber der EUDI-Wallet. Es wird durch den Relying Party Registrar ausgestellt und enthält die für die technische Identifikation der Relying Party notwendigen Attribute. Die rechtliche Grundlage bildet Anhang IV der DVO 2025/848.
- Das Registrierungszertifikat dient der Transparenz und Nachvollziehbarkeit der Datenverarbeitung durch die Relying Party. Es dokumentiert, welche Attribute von der 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 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. Sie sind zudem öffentlich einsehbar, sodass andere 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 Artikel 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 (Artikel 9 Absatz 1 Buchst. d),

- EUDI-Wallet-Provider (Artikel 5d Absatz 1),
- QEAA-Provider (Artikel 22 Absatz 1),
- Pub-EAA-Provider (Artikel 45f Absatz 3),
- sowie registrierte Relying Parties (Artikel 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 Relying Parties und EUDI-Wallets. Die genaue 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.

Relying Party Registrar

Der Relying Party Registrar ist für die Registrierung und Verwaltung von Relying Parties im EUDI-Wallet-Ökosystem zuständig (Artikel 2, Nr. 5 DVO 2024/2980). Es prüft die Registrierung und stellt das Zugriffs- und Registrierungszertifikat gemäß DVO 2025/848 aus. Die Rolle des Registrars umfasst zudem die technische und organisatorische Prüfung der Angaben der Relying Party, die Zertifikatsverwaltung, sowie Aussetzung und Widerruf (Art. 5b eIDAS-VO; DVO 2025/848).

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 sind (Art. 2 DVO 2024/2977). 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.

Pub-EAA Provider

Pub-EAA Provider sind Behörden (öffentliche Stellen) oder bevollmächtigte Vertreter von Behörden, die selbst oder im Namen einer Authentische Quelle Bescheinigungen ausstellen. Die Berechtigung zur Ausstellung dieser Bescheinigungen setzt eine Konformitätsbewertung durch eine notifizierte Konformitätsbewertungsstelle voraus (Art. 45f. Abs. 1,2 und 6 eIDAS-VO ; DVO 2024/2982). Pub-EAA Provider werden an die EU-Kommission gemeldet, inkl. Angabe der Konformitätsbewertung und werden in einer EU-Vertrauensliste veröffentlicht (Art. 45f. Abs. 3 eIDAS-VO). Zusätzlich sind die Provider mit einem eindeutigen behördlichen Identifier sowie einem gültigen Zugriffs- und Registrierungszertifikat ausgestattet (DVO 2025/848). 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.

Qualifizierter Vertrauensdiensteanbieter (QTSP)

Ein QTSP ist ein zertifizierter Anbieter qualifizierter Vertrauensdienste, der etwa qualifizierte elektronische Signaturen, Siegel oder Zertifikate ausstellt (Art. 3 Abs. 20, Art. 24 ff. eIDAS-VO 910/2014). QTSPs müssen regelmäßig Konformitätsbewertungen durch akkreditierte Stellen durchlaufen und der Aufsichtsstelle Prüfberichte vorlegen (Art. 20 Abs. 1 eIDAS-VO 910/2014). Alle qualifizierten QTSPs mit gültiger Notifizierung werden von den Mitgliedstaaten an die EU-Kommission zu melden und werden in einer EU-Vertrauensliste veröffentlicht (Art. 22 eIDAS-VO 910/2014).

Vermittler

Ein Vermittler (sog. Intermediary) 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 (Art. 5b Abs 10 eIDAS-VO, ARF 3.11). Er übernimmt Aufgaben wie die Weiterleitung von Anfragen, Schnittstellenintegration, Validierung von Attributsbescheinigungen oder Anbindung bestehender Systeme, ohne selbst personenbezogene Attribute zu speichern, auszustellen oder auszuwerten (Art. 5b Abs 10 eIDAS-VO, ARF 3.11). 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 dem im Registrierungszertifikat definierten Attributen an die EUDI-Wallet zu übermitteln.

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 Artikel 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 (SPRIN-D) 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.

Wallet-Adapter

Der Wallet-Adapter übersetzt sowohl die eingehenden als auch die ausgehenden Anfragen/Antworten (d. h. Requests/Responses) zwischen der Relying Party und der EUDI-Wallet. Das bedeutet z.B. die Übersetzung eingehender JSON-Formate der 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.

II. Prozessübersicht „Indirekte Anbindung an die EUDI-Wallet"

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 ermöglicht.
2	Auswahl Identifizierungs- / Authentifizier-ungsmittel	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 (Access Certificate) & Annex V nr. 3 j (Registration Certificate) OpenID4VP: OpenID Digital Credentials Protocols Working Group (Credential=technischer Begriff für Nachweis). (2025, 17. August). *OpenID for Verifiable Presentations 1.0. (Final Status)*. OpenID Foundation. OpenID for Verifiable Presentations 1.0;
4	Bereitstellung Authorization Request durch Link/QR Code	BundID IdP	BundID stellt die Authorization Request für die EUDI-Wallet bereit. Dem Nutzenden wird sowohl ein Link als auch ein QR-Code angezeigt. 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. Im Cross-Device Flow scant der User den QR-Code mit	Referenz: OpenID4VP: OpenID Digital Credentials Protocols Working Group. (2025, 17. August). *OpenID for Verifiable Presentations 1.0. (Final Status)*. 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 für eine

			seinem Handy ab, um die Wallet-Auswahl zu starten (siehe Hinweis).	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: ● Verifikation der Signatur über die Anfrage mithilfe des öffentlichen Schlüssels im Zertifikat ● Validierung der Zertifikat(e) gegen den zuvor bezogenen Trust Anchor ● Prüfung, dass keines der Zertifikate widerrufen ist Die EUDI-Wallet 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). *Selective Disclosure for JWTs (SD-JWT VC) – draft-ietf-oauth-sd-jwt-vc-15*. 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.2.4.0 (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: ● Validierung des PID-Providers gegen Trusted List ● Prüfung der Echtheit und Signatur ● Kontrolle von Device Binding und User Binding ● Prüfung auf Ablaufdatum und Widerruf ● Prüfung der Einhaltung der Schemadefinition für PID-Credentials	Referenzen: PID-Verifizierung eIDAS-VO 910/2014 Artikel 5a
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	Onlinedienst / fachl. zuständige Stelle	Der Onlinedienst der fachlich zuständigen Stelle prüft die empfangenen Daten darauf, ob sie den zu authentifizierenden Nutzenden repräsentieren bzw. nutzt sie zur Identifizierung eines bisher unbekannten Nutzenden. Optional kann der Onlinedienst dem Nutzenden die Response präsentieren und zur Vorausfüllung z.B. eines Onlineformulars im Rahmen einer Antragsstellung nutzen. Der Nutzende kann dieses Formular manuell prüfen, ggf. ergänzen und dann die Daten zur weiteren Verarbeitung für das Antragsverfahren freigeben.	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./Authen-tifizierung des Nutzenden	Onlinedienst	Ist der Prozess erfolgreich, ist der Nutzende für die Nutzung des Services authentifiziert.	

Funktionalität 2: Ausstellung von Nachweisen aus dem 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	z.B. wurde ein Antragsprozess durchlaufen, auf den die Ausstellung eines Nachweises folgt.

			sie/ihn zum Abruf eines Nachweises berechtigt.	
1	Ausstellung des Nachweises in das Zentrale Bürgerpostfach (ZBP)	Fachlich zu-stän-dige 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 Authentifizierungs-verfahren.	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, Wallet-Instance (= hoch), ● ELSTER (= substantiell) ● 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	Das ZBP stellt ein UI-Element bereit, über das der Nutzende die Ausstellung anstoßen kann. Z.B. ein Button “In meine EUDI-Wallet

			(Credential)) in die EUDI-Wallet ausstellen zu lassen	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. Die Credential Offer enthält: • Credential Issuer URL • Identifier des auszustellenden Credentials • Optional: issuance_state Parameter, um den Ausstellungsprozess mit einer bestehenden Web Session zu verknüpfen	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). *OpenID for Verifiable Credential Issuance 1.0 (Final Status)*. OpenID Foundation. OpenID for Verifiable Credential Issuance 1.0
5	Bereitstellung der Credential Offer	BundID als techn. Komponente eines EAA-Providers	Die BundID zeigt dem Nutzenden sowohl einen Link als auch ein QR-Code an. Im Same-Device-Flow klickt der Nutzende auf den Link. Durch das im Link angegebene Protokoll (bspw.: OpenID4VCI oder Haip-vci)	Referenz: OpenID4VCI: OpenID Digital Credentials Protocols Working Group. (2025, 16. September). *OpenID for Verifiable Credential Issuance 1.0 (Final Status)*. OpenID Foundation.

			kann der Browser, die Auswahl der zu verwendenden EUDI-Wallet über die entsprechende API durch den Nutzenden triggern. Im Cross-Device Flow scannt der Nutzende den QR-Code mit seinem Handy ab, um die Wallet-Auswahl zu starten.	OpenID for Verifiable Credential Issuance 1.0
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: ● Verifikation der signierten Metadaten durch Prüfung der Signatur und ● Existenz und Gültigkeit des Registrierungs-zertifikats Die EUDI-Wallet informiert den Nutzenden über das Prüfergebnis und welche Stelle welches Credential anbietet. 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	Referenz: OpenID4VCI: OpenID Digital Credentials Protocols Working Group. (2025, 16. September). *OpenID for Verifiable Credential*

			• fügt die Wallet Unit Attestation (WUA) hinzu • übermittelt die Credential Request an die BundID	*Issuance 1.0 (Final Status)*. OpenID Foundation. OpenID for Verifiable Credential Issuance 1.0
8	Verifizierung des Credential Requests	BundID als techn. Komponente eines EAA-Provider	Die BundID prüft: • die Übereinstimmung von PID Daten des Nutzenden und den Daten im angefragten Credential (siehe Hinweis) • die Gültigkeit des Nachweises (Dresden Pass), indem die Attribute gegen die authentische Quelle geprüft werden, (optional für EAAs, Pflicht bei Pub-EAA und QEAA-Ausstellung) • die Gültigkeit der EUDI-Wallet Unit, anhand der entsprechenden EUDI-Wallet Provider Trust Lists • die Gültigkeit des EUDI-Wallet Providers anhand von Revocation Lists (Optional für Attestation Provider; verpflichtende Prüfung für PID Provider) • die Eigenschaften der WSCA/WSCD anhand der bereitgestellten WUA (Optional, laut ARF Version 2.4.0) • den Schutz von private und public key durch WSCD	Um Missbrauch der Daten zu vermeiden, wird festgelegt, dass auch bei nicht-qualifizierten EAAs die erneute Identifizierung/Authentifizierung des Users durch den Aussteller (Issuer) gefordert wird. Hinweis: Es wird aktuell geprüft, ob der der Abgleich stattdessen über die Login-Session erfolgen kann. Vorausgesetzt der Nutzende hat sich zuvor mit seiner EUDI-Wallet im BundID ZBP angemeldet. IETF OAuth Working Group. (2024, 8. Juli). *Selective Disclosure for JWTs (SD-JWT-VC) – draft-ietf-oauth-sd-jwt-vc-15*. IETF. SD-JWT-based Verifiable Credentials (SD-JWT-VC)

9	Anfügen einer Disclosure Policy	BundID als techn. Komponente eines EAA-Providers	Die BundID fügt optional eine Disclosure Policy an das Credential an, falls dies durch die fachlich zuständige Stelle angefordert wurde.	Funktionalität in erster Ausbaustufe der staatlichen EUDI-Wallet noch nicht unterstützt.
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. Unter Einbeziehung eines QTSP wird der Hash-Wert mit einem fortgeschrittenen Siegel versehen (Hinweis: QTSPs erhalten kein Zugriff auf die Inhaltsdaten des EAAs.)	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 dann im Namen des BMDS vorgehalten wird.
11	Ausstellung des Credentials in die EUDI-Wallet	BundID als techn. Komponente eines EAA Provider	Die BundID erzeugt das SD-JWT VC (Credential) und übermittelt es an die EUDI-Wallet des Nutzenden.	
12	Präsentation des Credentials	EUDI-Wallet	Der EUDI-Wallet präsentiert dem Nutzenden das empfangene Credential. Der Nutzende stimmt der Speicherung zu, woraufhin die EUDI-Wallet das Credential abspeichert.	

III. Prozessübersicht „Direkte Anbindung an die EUDI-Wallet bei Betrieb eines Wallet-Adapters“

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 Onlinedienstes auf, wählt den gewünschten Service aus und startet den Identifizierungs-/ Authentifizierungsprozess.	Bei Anbindung eines Wallet-Adapters: Die fachlich zuständige Stelle ist als Relying Party registriert. Das Registration Certificate wird dem Wallet-Adapter zur Ausübung seiner Rolle als Vermittler (Intermediary) übermittelt. Der Wallet-Adapter hat Zugriff bzw. hält die Registration Certificates der Relying Party. Falls kein Wallet-Adapter verwendet wird, muss die fachlich zuständige Stelle selbst eine neue OpenID4VP Schnittstelle implementieren. Bei Eigenbetrieb eines Wallet-Adapters: 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 Identifizier-ungs-/ Authentifi-zierungsmittel	Online-dienst / Fachl. zu-stän-dige Stelle	Der Onlinedienst der fachlich zuständigen Stelle fordert den Nutzenden zur Authentifizierung auf, z.B. über den Button “Mit EUDI-Wallet	Ohne Wallet-Adapter muss die fachlich zuständige Stelle die Authentifizierungsanfrage an die EUDI-Wallet gemäß OpenID4VP-Standard versenden, inkl.

			anmelden" oder einer sinngemäßen Option. Daraufhin schickt der Onlinedienst die Datenanfrage als OIDC-Request an den Wallet-Adapter gemäß OpenID Connect-Protokoll und leitet den Nutzenden zum Wallet-Adapter weiter.	Signierung der Authorization Request-Daten.
3	Erstellung Authorization Request	Wallet-Adapter	Der Wallet-Adapter: ● erstellt eine Authorization Request gemäß OpenID4VP-Standard. ● präsentiert die Zertifikate ● signiert die Authorization Request mit dem privaten Schlüssel des Access Certificates Der Wallet-Adapter stellt die Authorization Request für die EUDI-Wallet zum Abruf bereit.	Bei Anbindung eines Wallet-Adapters: Der Wallet-Adapter nutzt sein eigenes Access Certificate. Zusätzlich stellt die fachlich zuständige Stelle dem Wallet-Adapter ihre eigenen Registration Certificates zur Verfügung. Bei Eigenbetrieb eines Wallet-Adapters: Bei Eigenbetrieb des Wallet-Adapters ist das Access Certificate sowie die Registration Certificates des Wallet Adapters die der Relying Party. Referenzen: EU 2025/848 Annex IV nr. 3 k (Access Certificate) & Annex V nr. 3 j (Registration Certificate) OpenID4VP: OpenID Digital Credentials Protocols Working Group. (2025, 17. August). *OpenID for Verifiable Presentations 1.0 (Draft 20)*. OpenID Foundation. OpenID for Verifiable Presentations 1.0

4	Bereitstellung Authorization Request durch Link/QR Code	Wallet-Adapter	Der User 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. 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. Im Cross-Device Flow scannt der User den QR-Code mit seinem Handy ab, um die Wallet-Auswahl zu starten.	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). *OpenID for Verifiable Presentations 1.0 (Draft 20)*. OpenID Foundation. OpenID for Verifiable Presentations 1.0
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: • Verifikation der Signatur über die Anfrage mithilfe des öffentlichen Schlüssels im Zertifikat • Validierung der Zertifikat(e) gegen den zuvor bezogenen Trust Anchor.	Referenz: ARF v2.4.0 (e.g 6.6. Trust throughout a PID or an attestation lifecycle)

			• Prüfung, dass keines der Zertifikate widerrufen ist. Die EUDI-Wallet 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). *Selective Disclosure for JWTs (SD-JWT-VC) – draft-ietf-oauth-sd-jwt-vc-04*. 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 den Wallet-Adapter.	Referenzen: ARF v.2.4.0 (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: • Validierung des PID-Providers gegen Trusted List • Prüfung der Echtheit und Signatur • Kontrolle von Device Binding und User Binding • Prüfung auf Ablaufdatum und Widerruf	Referenzen: PID-Verifizierung eIDAS-VO 910/2014 Artikel 5a Nummer 5; ARF v.2.4.0

			• Prüfung der Einhaltung der Schemadefinition für PID-Credentials Anschließend übersetzt der Wallet-Adapter die Response in eine OIDC-Response und sendet die Response an den Onlinedienst der fachlich zuständige Stelle.	
9	Prüfung und Freigabe der Daten	Onlinedienst / fachl. zuständige Stelle	Der Onlinedienst der fachlich zuständigen Stelle prüft die empfangenen Daten darauf, ob sie den zu authentifizierenden Nutzenden repräsentieren bzw. nutzt sie zur Identifizierung eines bisher unbekannten Nutzenden. Optional kann der Onlinedienst dem Nutzenden die Response präsentieren und zur Vorausfüllung z.B. eines Onlineformulars im Rahmen einer Antragsstellung nutzen. Der Nutzende kann dieses Formular manuell prüfen, ggf. ergänzen und dann die Daten zur weiteren Verarbeitung für das Antragsverfahren freigeben.	Wird die Ident./Auth. 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 der PID stammen.
10	Erfolgreiche Ident./Auth. des Nutzenden	Onlinedienst	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; Fachlich zuständige Stelle in der Rolle eines EAA-Providers

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	Bereitstellung des Nachweises	Onlinedienst	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/die 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 den Nachweis Request an die EUDI-Wallet des Nutzenden zu stellen.
2	Datenüber-mittlung	Onlinedienst	Die Daten für den Nachweis werden via Pushed Authorization Request 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. Die Credential Offer enthält: • Credential Issuer URL	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). *OpenID for Verifiable*

			• Identifier des auszustellenden Credentials • Optional: issuance_state Parameter Der Wallet-Adapter antwortet dem Onlinedienst durch Übermittlung der Adresse für die Landing Page (redirect uri).	*Credential Issuance 1.0 (Final Status).* OpenID Foundation. OpenID for Verifiable Credential Issuance 1.0
4	Redirect zur Wallet-Adapter Landing Page	Onlinedienst	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.	Um Missbrauch der Daten zu vermeiden, wurde festgelegt, dass auch bei nicht-qualifizierten EAAs die erneute Identifizierung/Authentifizierung des Users durch den Aussteller (Issuer) gefordert wird. Hierfür ist der Wallet-Adapter selbst als Relying Party registriert, um die PID abrufen zu dürfen. Der strukturierte Datensatz für den Nachweis enthält Identifizierungsdaten für den berechtigten Empfänger. Die Nutzendenidentifizierung findet an dieser Stelle statt, da die Wallet in der aktuellen Version noch nicht den Interactive Authorization Endpoint unterstützt. Nutzendenauthentifizierung und Ausstellung des Nachweises müssen daher unabhängig voneinander und nacheinander geschehen.

				Sobald die Wallet den benötigten Endpunkt unterstützt, wird die Authentisierung des Nutzenden Teil des Ausstellungsprozesses.
5	Bereitstellung der Credential Offer	Wallet-Adapter	Der Wallet-Adapter zeigt dem Nutzenden sowohl einen Link als auch ein QR-Code 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. Im Cross-Device Flow scannt der/die Nutzende den QR-Code mit seinem Handy ab, um die Wallet-Auswahl zu starten.	Referenz: OpenID4VCI: OpenID Digital Credentials Protocols Working Group. (2025, 16. September). *OpenID for Verifiable Credential Issuance 1.0 (Final Status)*. OpenID Foundation. OpenID for Verifiable Credential Issuance 1.0
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: ● Verifikation der signierten Metadaten	Die Credential Issuer's Metadaten beinhalten: - Technische Informationen über den Aussteller - Übersetzungs- und Visualisierungsinformationen für das auszustellende Credential

			durch Prüfung der Signatur und ● der Existenz und Gültigkeit des Registrierungszertifikats Die EUDI-Wallet informiert den Nutzenden über das Prüfergebnis und welche Stelle welches Credential anbietet. Der Nutzende akzeptiert das ihm angebotene Credential.	
7	Erstellung des Credential Request	EUDI-Wallet	Erst nach Zustimmung des Nutzenden startet die EUDI-Wallet den Credential Request. Die EUDI-Wallet: ● erstellt den Credential Request gemäß OpenID4VCI-Standard ● fügt die Wallet Unit Attestation (WUA) hinzu übermittelt die Credential Request an den Wallet-Adapter	Referenzen: EU 2025/848 Annex IV nr. 3 k (Access Certificate) & Annex V nr. 3 j (Registration Certificate) Referenz: OpenID4VCI: OpenID Digital Credentials Protocols Working Group. (2025, 16. September). *OpenID for Verifiable Credential Issuance 1.0 (Final Status).* OpenID Foundation. OpenID for Verifiable Credential Issuance 1.0
8	Verifizierung des Credential Requests	Wallet-Adapter	Der Wallet-Adapter prüft: ● die Gültigkeit des Nachweises (z.B. Dresden Pass), indem die Attribute gegen die authentische Quelle geprüft werden, (optional für EAAs, Pflicht bei Pub-EAA und QEAA-Ausstellung) ● die Gültigkeit der EUDI-Wallet Unit,	Um Missbrauch der Daten zu vermeiden, wird festgelegt, dass auch bei nicht-qualifizierten EAAs die erneute Identifizierung/Authentifizierung des Users durch den Aussteller (Issuer) gefordert wird; IETF OAuth Working Group. (2024, 8. Juli). *Selective Disclosure for JWTs (SD-JWT-VC) – draft-ietf-oauth-sd-jwt-vc-15.*

			anhand der entsprechenden EUDI-Wallet Provider Trust Lists • die Gültigkeit des EUDI-Wallet Providers anhand von Revocation Lists (Optional für Attestation Provider; verpflichtende Prüfung für PID Provider) • die Eigenschaften der WSCA/WSCD anhand der bereitgestellten WUA (Optional, laut ARF Version 2.4.0) • den Schutz von private und public key durch WSCD	IETF. SD-JWT-based Verifiable Credentials (SD-JWT-VC)
9	Anfügen einer Disclosure Policy	Wallet-Adapter	Der Wallet-Adapter fügt optional eine Disclosure Policy an das Credential an, falls dies durch die fachlich zuständige Stelle angefordert wurde.	Funktionalität in erster Ausbaustufe der staatlichen EUDI-Wallet noch nicht unterstützt.
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. 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 Nutzenden	

12	Präsentation des Credentials	EUDI-Wallet	Die EUDI-Wallet präsentiert dem Nutzenden das empfangene Credential.	

IV. Pilotvorhaben zur Verwaltungsanbindung mit Sächsischer Staatskanzlei und Landeshauptstadt Dresden

Das Pilotvorhaben zur Verwaltungsanbindung mit Sächsischer Staatskanzlei und Landeshauptstadt Dresden zeigt sehr deutlich, dass Verwaltungseinheiten frühzeitig auf strukturierte Datenformate und klar abgegrenzte Verantwortlichkeiten ausgerichtet werden müssen. Digitale Nachweise können nur dann effizient verarbeitet werden, wenn alle beteiligten Stellen – von Fachverfahrensbetreibern über Onlinedienste bis hin zu zentralen Basisdiensten – in der Lage sind, fachlich definierte Datensätze konsistent und interoperabel zu erzeugen, zu übertragen und zu empfangen. Dies setzt nicht nur technische Vorbereitung voraus, sondern vor allem ein einheitliches Verständnis darüber, wer in der föderalen Architektur für die Ausstellung von Nachweisen, für ihre inhaltliche Qualität, Struktur sowie Semantik, für die Validierung und für den Betrieb der entsprechenden Systeme verantwortlich ist. Gerade im EUDI-Wallet-Ökosystem ist es essenziell, dass Rollen und Verantwortlichkeiten eindeutig definiert sind – etwa für die Identifizierung und Authentifizierung über die EUDI-Wallet, für die Ausstellung digitaler Nachweise in die Wallet und für die Präsentation solcher Nachweise in Verwaltungsprozessen.

Aktuell werden gemeinsam mit der Landeshauptstadt Dresden, der BundID sowie dem Wallet-Adapter alle drei Funktionalitäten und unterschiedlichen Anbindungsoptionen sowohl produktiv als auch prototypisch erprobt. Ziel ist es, dass die BundID bis zum Januar 2027 die Ident- und Authentifizierung mit der EUDI-Wallet für alle angebundenen Dienste ermöglicht und zugleich die Ausstellung des Dresden-Passes sowie der sächsischen Ehrenamtskarte über das ZBP unterstützt. Perspektivisch können Nachweise, die in menschen- und maschinenlesbarer Form in das ZBP ausgestellt werden in die EUDI-Wallet übermittelt werden. Im Zuge der Pilotierung mit der Landeshauptstadt Dresden entsteht eine Blaupause für die Ausstellung weiterer Nachweise über das ZBP. Darüber hinaus wird der Wallet-Adapter als Produkt des IT-PLR prototypisch weiterentwickelt und zur Nachnutzung bereitgestellt. Der Betrieb erfolgt dezentral und nicht durch den Bund.