Verwaltungsanbindung EUDI-Wallet

Zielbild und Umsetzungsoptionen für die öffentliche Verwaltung

Konzept

Inhaltsverzeichnis

Abkürzungsverzeichnis

Nr.	Begriff / Abkürzung	Begriffsbestimmung
1	ARF	Architecture and Reference Framework
2	DVO	Durchführungsverordnung / Implementing Act
3	EAA	Electronic attestation of attributes / Elektronische Attributsbescheinigung
4	eID	elektronische Identitätsfunktion des Personalausweises
5	eIDAS	electronic IDentification, Authentication and trust Services / elektronische Identifizierung, Authentifizierung und Vertrauensdienste
6	EU	European Union / Europäische Union
7	EUDI	European Digital Identity / Europäische Digitale Identität
8	EUDI-Wallet	European Digital Identity Wallet / Europäische Digitale Identitätsbrieftasche
9	EU-OOTS	EU-Once-Only-Technical-System
10	JSON	JavaScript Object Notation
11	Legal PID	Legal Person Identification Data / Identifizierungsdaten juristischer Personen
12	NOOTS	National Once-Only-Technical-System
13	OIDC	OpenID Connect
14	OpenID4VCI	OpenID for Verifiable Credential Issuance/Verifiable Presentation
15	OZG	Onlinezugangsgesetz
16	PID	Personal Identification Data /Personenidentifizierungsdaten
17	Pub-EAA	Elektronische Attributsbescheinigung öffentlicher Stellen / Public Body Electronic Attestation of Attributes
18	Pub-EAA Provider	Public Body Electronic Attestation of Attributes Provider / Aussteller elektronischer Attributsbescheinigung öffentlicher Stellen
19	QEAA	Qualified Electronic Attestation of Attributes / Qualifizierte elektronische Attributsbescheinigung
20	QTSP	Qualified Trust Service Provider / Qualifizierter Vertrauensdiensteanbieter
21	RP	Relying Party / vertrauende Partei bzw. Stelle
22	SAML-Response	Security Assertion Markup Language Response
23	SDG	Single Digital Gateway / einheitliches digitales Zugangstor
24	SD-JWT-VC	Selective Disclosure JSON Web Token – Verifiable Credential
25	TL	Trusted List / Vertrauensliste (Liste qualifizierter Vertrauensdiensteanbieter je Mitgliedstaat)
26	UX	User Experience / Nutzendenerfahrung
27	Trust Anchor	Vertrauensanker für Zertifikatsprüfung
28	ZBP	Zentrale Bürgerpostfach der BundID

1 Einleitung

Das vorliegende Dokument zur Anbindung der öffentlichen Verwaltung an das EUDI-Ökosystem wurde im Rahmen der nationalen Umsetzung der eIDAS-Verordnung (EU) 2024/1183 (eIDAS-VO) erstellt und basiert auf den aktuellen Erkenntnissen des Bundesministeriums für Digitales und Staatsmodernisierung (BMDS). Im Folgenden werden verschiedene Umsetzungsoptionen vorgestellt, die aufzeigen, wie die Anforderungen der eIDAS-VO zentral oder dezentral von der öffentlichen Verwaltung erfüllt werden können.

Artikel 5f Absatz 1 der eIDAS-VO verpflichtet fachlich zuständige Stellen (z. B. (Fach-)Behörden) spätestens bis zum 24.12.2024 dazu, die EUDI-Wallet zur elektronischen Identifizierung und Authentifizierung in digitalen Antragsprozessen zu akzeptieren, sofern eine „starke Nutzerauthentifizierung“ (vgl. Art. 1, Abs. 51 eIDAS-VO) rechtlich notwendig ist.

Bei der Ausstellung von Nachweisen (sogenannten Attributsbescheinigungen) durch die öffentliche Verwaltung sind die fachlich zuständigen Stellen verpflichtet, zumindest für die in Anhang VI der eIDAS-VO aufgeführten Attribute den Vertrauensdienstanbietern die Möglichkeit zu geben, die Authentizität dieser Attribute anhand der Authentischen Quelle (Details siehe Anhang I), das heißt Register oder Datenquellen wie Hochschulen oder Schulverwaltungen, zu überprüfen (vgl. Art. 45e Abs. 1 eIDAS-VO). Die Ausstellung verifizierbarer Attributsbescheinigungen durch Behörden ist damit implizit vorgesehen. Ob damit eine Umsetzungsverpflichtung bis 24.12.2026 einhergeht, wird derzeit noch rechtlich geprüft.

Im Hinblick auf die Anbindung der öffentlichen Verwaltung an die EUDI-Wallet wurden unterschiedliche Umsetzungsoptionen entwickelt, welche aktuell im Rahmen eines laufenden BMDS-Vorhabens zur „Erprobung der Verwaltungsanbindung der EUDI-Wallet“ gemeinsam mit der Stadt Dresden und dem Land Sachsen getestet und praxisnah validiert werden. Dabei liegt ein besonderer Fokus auf den Mehrwerten, die sich sowohl für die öffentliche Verwaltung als auch für Bürgerinnen und Bürger ergeben.

2 Kontext

2.1 EUDI-Wallet

Bis zum 24.12.2026 sind alle Mitgliedstaaten der EU verpflichtet, eine staatlich anerkannte EUDI-Wallet für natürliche und juristische Personen bereitzustellen. Diese EUDI-Wallet bietet neben der digitalen Identität für natürliche Personen (Person Identification Data, PID) und Organisationen (Legal Person Identification Data, Legal PID) auch die Möglichkeit, sowohl staatliche als auch private Attributsbescheinigungen zu speichern und vorzulegen – beispielsweise Führerscheine, Zeugnisse, Nachweise über Vereinsmitgliedschaften oder Tickets. Darüber hinaus umfasst die EUDI-Wallet Funktionen wie die Verwendung eines Pseudonyms zur Authentifizierung, eine rechtssichere digitale Unterschrift mittels qualifizierter elektronischer Signatur sowie eine Bezahlfunktion. Die EUDI-Wallet ist sowohl für Online-Interaktionen als auch für Vor-Ort-Szenarien („Proximity-Sharing“) konzipiert. Die produktive Bereitstellung der ersten Version der EUDI-Wallet mit der PID-Funktion zur Identifikation und Authentifizierung sowie der Funktion zur Speicherung und Verwaltung von

Attributsbescheinigungen (auch Nachweise) soll bis Ende 2026 erfolgen. Die weiteren Funktionalitäten der EUDI-Wallet werden sukzessive ab 2027 bereitgestellt.

2.2 EUDI-Ökosystem

Die eIDAS-VO schafft einen verbindlichen Rahmen für ein interoperables digitales Identitätsökosystem mit der EUDI-Wallet im Zentrum. Diese EUDI-Wallet dient als zentrale Anwendung, über die sich Bürgerinnen und Bürger sowie Organisationen sicher, datenschutzkonform und nutzendenzentriert digital identifizieren und authentifizieren können. Darüber hinaus ermöglicht das EUDI-Ökosystems die Ausstellung von digital und automatisiert verifizierbaren Attributsbescheinigungen durch elektronische Signaturen und Siegel, die in vielfältigen digitalen Verwaltungs- und Geschäftsprozessen eingesetzt werden können.

Damit diese Funktionen europaweit zuverlässig und einheitlich zur Verfügung stehen, ist die EUDI-Wallet in ein umfassendes digitales Identitätsökosystem eingebettet. Dieses Ökosystem bildet den strukturellen, technischen und rechtlichen Rahmen, innerhalb dessen die EUDI-Wallet betrieben wird. Es legt die Rollen, Abläufe und Schnittstellen fest, die für die Ausstellung, Nutzung und Validierung digitaler Identitäten und weiterer Attributsbescheinigungen erforderlich sind, und schafft damit die Grundlage für ein vertrauenswürdiges digitales Europa. Die EUDI-Wallet bietet damit das Potenzial, den Zugang zu Verwaltungsleistungen europaweit zu automatisieren sowie sicherer und effizienter zu gestalten.

Durch die europaweite Verifizierung elektronischer Attributsbescheinigungen können manuelle Prüfprozesse reduziert, bürokratische Hürden abgebaut und Sachbearbeitende spürbar entlastet werden. Gleichzeitig entsteht die Grundlage für eine grenzüberschreitende Nutzung digitaler Identitäten und digitaler Attributsbescheinigungen aus der Privatwirtschaft und der öffentlichen Verwaltung.

2.3 Referenzen

Das EUDI-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 2024/1183

Die Verordnung (EU) 2024/1183 stellt den zentralen Rechtsrahmen für das EUDI-Wallet-Ökosystem dar. Sie ersetzt und erweitert die bisherige Verordnung (EU) Nr. 910/2014 und 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 2.3.0)

Das ARF enthält eine Reihe Anforderungen an die Architektur, gemeinsamer Standards und technischer Spezifikationen und wird empfohlen für die Entwicklung der Referenzimplementierung der

EUDI-Wallet Lösung genutzt zu werden. 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 deutschen EUDI-Ökosystems.

National und 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.

3 Zielbild Verwaltungsanbindung EUDI-Wallet

Im Rahmen der Entwicklung des EUDI-Ökosystems wurde durch den Bund ein Zielbild für die Anbindung der öffentlichen Verwaltung an die EUDI-Wallet erstellt. Dieses besteht aus übergreifenden Prämissen und betrachtet unterschiedliche Umsetzungsoptionen der Anbindung für fachlich zuständige Stellen an die EUDI-Wallet. Mit dem Zielbild wird eine Blaupause für einen Referenzrahmen mit kohärenter nationaler Umsetzung, effizienten Strukturen und hoher Interoperabilität auf Bundes-, Landes- und kommunaler Ebene geschaffen. So können die Skalierbarkeit und die Akzeptanz der EUDI-Wallet langfristig gesichert und weiter gestärkt werden.

Das Zielbild entspricht den Vorgaben der eIDAS-VO. Dabei werden bestehende nationale, digitale Infrastrukturen sowie laufende Digitalisierungsprogramme systematisch berücksichtigt. Zielgruppe dieses Zielbilds sind fachlich zuständige Stellen auf Bundes-, Landes- und kommunaler Ebene, die verpflichtet sind, den gesetzlichen eIDAS-Vorgaben nachzukommen. Darüber hinaus werden die weiterführenden Nutzungspotenziale der EUDI-Wallet für die öffentliche Verwaltung adressiert.

3.1 Prämissen

Prämisse	Beschreibung
EUDI-Wallet als zentrale Verwaltungskomponente etablieren	EUDI-Wallet als 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-Ökosystem für alle Akteure, insbesondere der öffentlichen Verwaltungen, niedrigschwellig zu gestalten.
Bestehende Infrastrukturen integrieren	Zentrale Verwaltungsinfrastrukturen wie BundID/eOK und NOOTS 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 Anforderungen im größtmöglichen Umfang zentral zu erfüllen.
Dezentrale Umsetzung ermöglichen	Fachlich zuständigen Stellen befähigen, Anforderungen, die nicht zentral umgesetzt werden, eigenständig zu erfüllen und passende Lösungen selbst zu entwickeln.

3.2 Geltungsbereich

Das Konzept betrachtet drei Anwendungsszenarien der EUDI-Wallet für die öffentliche Verwaltung sowie die damit verbundenen Anforderungen an fachlich zuständige Stellen. Es werden jeweils mehrere, i.d.R. drei verschiedene Umsetzungsoptionen je Anwendungsszenario beschrieben. Dabei wird detaillierter auf Umsetzungsoptionen eingegangen, die eine niedrigschwellige Anbindung von Verwaltungsdiensten an die EUDI-Wallet ermöglichen. Die in den Umsetzungsoptionen beschriebenen Rollen werden im Anhang I detailliert dargestellt.

Für das Konzept werden folgende Aspekte nicht detailliert betrachtet:

- die direkte Anbindung von Verwaltungsdienstleistungen an die EUDI-Wallet, da diese auf europäischer Ebene im Rahmen der eIDAS-Verordnung geregelt wird,
- die Umsetzung der deutschen EUDI-Wallet, die lediglich als relevante Rahmenbedingung berücksichtigt, jedoch nicht vertiefend behandelt wird,
- die Ausstellung der digitalen Identität für natürliche Personen (Person Identification Data, PID) und für Organisationen (Legal Person Identification Data, Legal PID), einschließlich der zugehörigen Widerrufsprozesse,
- die Registrierungsprozesse von „Vertrauende Beteiligte“ (sogenannte Relying Parties) einschließlich des Zertifikatsmanagements (Zugriffs- und Registrierungszertifikate) sowie deren Aufnahme in nationale Register.

Eine Relying Party (Details siehe Anhang I) kann sowohl die Funktion des Austellers als auch des Verifiers übernehmen. Als Austeller stellt sie (qualifizierte) elektronische Attributsbescheinigungen aus. Als Verifier prüft sie die Authentizität und Gültigkeit dieser Attributsbescheinigung.

4 Umsetzungsoptionen der Anwendungsszenarien der EUDI-Wallet für die öffentliche Verwaltung

Auf Basis der Anforderungen der eIDAS-VO werden drei Anwendungsszenarien mit Blick auf die Anbindung der öffentlichen Verwaltung an die EUDI-Wallet unterschieden:

- Szenario 1: Entgegennahme der PID zur Identifizierung und Authentifizierung mit der EUDI-Wallet
- Szenario 2: Ausstellung von verifizierbaren Attributsbescheinigungen in die EUDI-Wallet
- Szenario 3: Entgegennahme weiterer Attributsbescheinigungen aus der EUDI-Wallet

Die Szenarien sind nach Umsetzungspflicht priorisiert.

Szenario 1 stellt eine verbindliche Anforderung im Sinne der eIDAS-VO (MUSS-Anforderungen) dar.

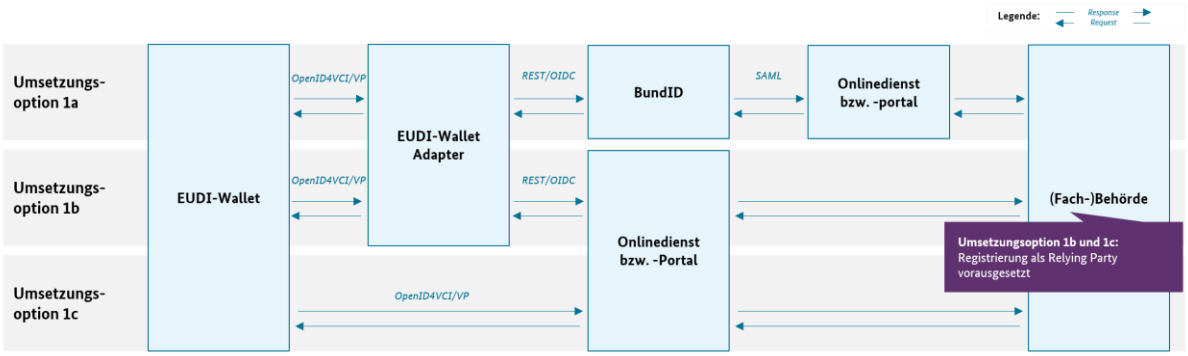
Im Hinblick auf Szenario 2 sind die jeweils fachlich zuständigen Stellen verpflichtet, zumindest für die in Anhang VI der eIDAS-VO aufgeführten Attribute einen Validierungsmechanismus bereitzustellen, der es Vertrauensdiensteanbietern ermöglicht, die Authentizität von Attributen anhand der Authentischen Quelle (d.h. des jeweiligen Registers oder Datenbestands) zu überprüfen. Die Ausstellung verifizierbarer Attributsbescheinigungen durch (Fach-)Behörden ist damit zwar implizit vorgesehen, ob aber auch eine Umsetzungsverpflichtung bis 24.12.2026 einhergeht, wird derzeit noch rechtlich geprüft.

Szenario 3 stellt eine optionale Nutzung der Funktionalitäten der EUDI-Wallet (KANN-Anforderung) dar. Jedes der drei Szenarien wird im Folgenden beschrieben und mögliche Umsetzungsoptionen werden dargestellt. Welche Option gewählt wird, liegt im Ermessen der fachlich zuständigen Stellen und ist abhängig davon, ob die Anforderungen bevorzugt dezentral eigenständig umgesetzt oder zentral bereitgestellte und nachnutzbare Komponenten genutzt werden sollen.

Im Rahmen des BMDS-Vorhabens zur „Erprobung der Verwaltungsanbindung der EUDI-Wallet“ werden aktuell mögliche Umsetzungsoptionen für die Szenarien 1 bis 3 gemeinsam mit der Stadt Dresden und dem Land Sachsen evaluiert und praxisnah validiert.

4.1 Szenario 1: Entgegennahme der PID zur Identifizierung- und Authentifizierung mit der EUDI-Wallet

Im Rahmen des Szenarios 1 wird die PID aus der EUDI-Wallet an den Onlinedienst bzw. das -portal übermittelt, um die Identität der Nutzenden eindeutig zu verifizieren. Für die Anbindung der EUDI-Wallet als Identifizierungs- und Authentifizierungsmittel durch den Verwaltungsdienst (u.a. Onlinedienste, Verwaltungsportale) gibt es drei mögliche Umsetzungsszenarien:



4.1.1 Umsetzungsoption 1a: Indirekte Anbindung über die BundID

Aufgabe der BundID ist zum einen die Bereitstellung eines zentralen Nutzerkontos zur Identifizierung und Authentifizierung von Bürgerinnen und Bürgern gegenüber der Verwaltung. Aus diesem Grund wird die BundID – ergänzend zur eID – die EUDI-Wallet als weiteres Identifizierungsmittel ab 12.24.2026 anbieten. Damit erfüllen alle bereits an die BundID angebundenen Verwaltungsdienste (u.a. Onlinedienste, Verwaltungsportale) automatisch die verpflichtende Anforderung der eIDAS-Verordnung.

Die BundID stellt eine Identifizierungs- bzw. Authentifizierungsanfrage an die EUDI-Wallet des Nutzenden. Ein EUDI-Wallet Adapter (Details siehe Anhang I) soll die Integration erleichtern, indem dieser den sicheren Austausch und die Kommunikation zwischen BundID und EUDI-Wallet ermöglicht. Der Nutzende erhält die Anfrage zur Freigabe der personenidentifizierenden Daten (PID) . Nach aktiver

Freigabe der PID durch Nutzende der EUDI-Wallet werden die Daten an die BundID übergeben. Die BundID als Relying Party prüft die PID auf Echtheit und Gültigkeit, mit Unterstützung des EUDI-Wallet Adapters. Nach erfolgreicher Validierung wird die PID durch den EUDI-Wallet Adapter in ein für die BundID lesbares JSON-Format übersetzt. Auf dieser Grundlage erstellt die BundID eine Identifizierungs- bzw. Authentifizierungsantwort und übermittelt über die bestehende SAML-Schnittstelle den Stammdatensatz an den anfragenden Verwaltungsdienst (u.a. Onlinedienst).

4.1.2 Umsetzungsoption 1b: Indirekte Anbindung über einen zentralen EUDI-Wallet Adapter

Im Vergleich zur Umsetzungsoption 1a agiert die fachlich zuständige Stelle des Verwaltungsdienstes (u.a. Onlinedienst, oder -portal) und nicht mehr die BundID als Relying Party, und ist als solche in der EU-Vertrauensliste registriert (Art. 5b Abs. 1 und 3 eIDAS-VO). Im Kontext von Portalen, Plattformen und/oder EfA-Onlinediensten wird aktuell rechtlich geprüft, welche Organisation im Kontext der eIDAS-Verordnung, als fachlich zuständig Stelle die Registrierung als Relying Party vornehmen muss. Ziel ist es, den Registrierungsprozess zentralisiert und effizient zu gestalten.

Der Verwaltungsdienst stellt eine Identifizierungs- und Authentifizierungsanfrage des Nutzenden an die EUDI-Wallet über einen EUDI-Wallet Adapter. In dieser Umsetzungsoption agiert der EUDI-Wallet Adapter im Auftrag der fachlich zuständigen Stelle als Vermittler.

Nach aktuellem Sachstand ergeben sich folgende Anforderungen für die fachlich zuständigen Stellen:

- Registrierung als Relying Party unter Angabe des EUDI-Wallet-Adapters als Vermittler, einschließlich der Speicherung von Zertifikaten (Zugriffs- und Registrierungszertifikat)
- Anbindung an den EUDI-Wallet-Adapter, unter anderem durch Integration einer neuen OpenID-Connect-Schnittstelle
- Versand einer Authorisierungsanfrage an den EUDI-Wallet-Adapter
- Erhalt der PID als JSON-Response über den EUDI-Wallet-Adapter und deren Verarbeitung; kein Empfang von BundID-Stammdaten als SAML-Response
- UX-Anpassung der Nutzeroberfläche des Verwaltungsdienstes zur Integration der EUDI-Wallet als ergänzendes Identitäts-/Authentifizierungsmittel
- Verarbeitung von Fehlermeldungen durch den EUDI-Wallet-Adapter

4.1.3 Umsetzungsoption 1c: Direkte Anbindung an die EUDI-Wallet

Wie in der Umsetzungsoption 1c agiert die fachlich zuständige Stelle des Verwaltungsdienstes (u.a. Onlinedienst) als Relying Party, nutzt jedoch nicht den EUDI-Wallet Adapter als Vermittler. Die konkrete technische Ausgestaltung der direkten Anbindung an die EUDI-Wallet ist nicht Gegenstand des Konzeptes.

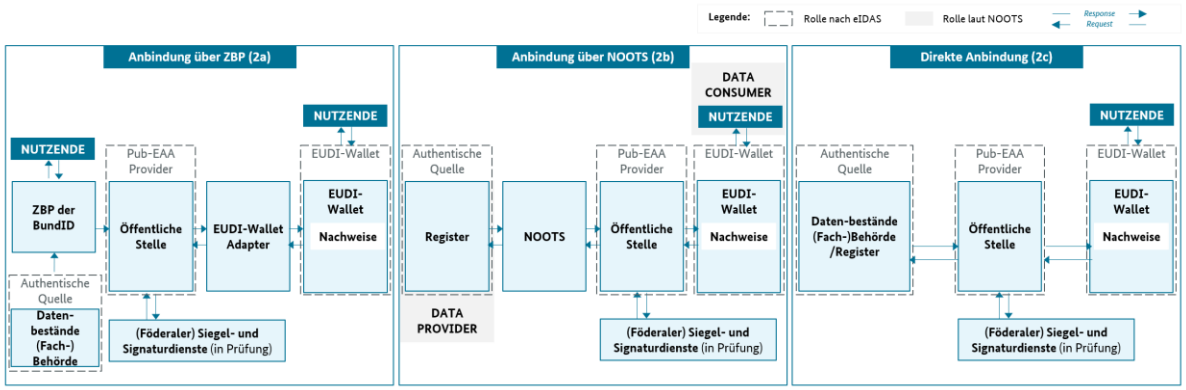
Nach aktuellem Sachstand ergeben sich folgende Anforderungen für die fachlich zuständigen Stellen:

- Registrierung als Relying Party, einschließlich der Speicherung von Zertifikaten (Zugriffs- und Registrierungszertifikat)
- Anbindung an den EUDI-Wallet, unter anderem durch Integration einer neuen OpenID4VCI/VP Schnittstelle
- Versand einer Authorisierungsanfrage an die EUDI-Wallet in SD-JWT-VC Format
- Erhalt der PID als SD-JWT-VC-Response der EUDI-Wallet sowie Validierung auf Echtheit und Gültigkeit der PID (Validierungsprozesse); kein Erhalt BundID Stammdaten als SAML-Response

- UX-Anpassung der Nutzeroberfläche des Verwaltungsdienstes zur Integration der EUDI-Wallet als ergänzendes Identifizierungs-/Authentifizierungsmittel
- Verarbeitung von Fehlermeldungen durch die EUDI-Wallet

4.2 Szenario 2: Ausstellung von verifizierbaren Attributsbescheinigungen in die EUDI-Wallet

Im Rahmen des Anwendungsszenarios 2 werden Attributsbescheinigungen auf Basis von Authentischen Quellen (u.a. Register, Datenbestände der öffentlichen Verwaltung) in die EUDI-Wallet ausgestellt. Voraussetzung dafür ist die Bereitstellung von strukturierten, maschinenlesbaren Daten in einem technisch signierten, überprüfbaren Format (OpenID4VCI). Die technische Signatur und Siegelung kann durch einen (qualifizierten) Vertrauensdiensteanbieter (Details siehe Anhang I) erfolgen, um Rechtsgültigkeit und Nachvollziehbarkeit sicherzustellen (Art. 24 Abs. 1, Art. 45e Abs. 1 eIDAS-VO). Für die Anbindung der EUDI-Wallet gibt es drei mögliche Umsetzungsszenarien:



4.2.1 Umsetzungsoption 2a: Indirekte Anbindung über Postfach- bzw. Kommunikationslösungen

Gemäß eIDAS müssen im EUDI-Wallet Ökosystem drei Rollen bei der Ausstellung von Attributsbescheinigungen zusammenspielen: Die Authentische Quelle, die fachlich für eine Attributsbescheinigung zuständig ist. Der Pub-EAA Provider, eine laut der eIDAS-VO „öffentliche Stelle“ oder bevollmächtigte Vertreter, die selbst oder im Namen einer Authentischen Quelle Attributsbescheinigungen ausstellen. Die EUDI-Wallet des Nutzenden, für den die Attributsbescheinigung auf Antrag ausgestellt werden soll.

Voraussetzung für die Umsetzungsoption 2a ist die Nutzung einer Postfach- bzw. Kommunikationslösung, beispielsweise dem zentralen Bürgerpostfach (ZBP). Bürgerinnen und Bürger können Nachrichten in ihr BundID-Postfach erhalten, etwa Bescheide oder Rückfragen von (Fach-) Behörden. Auf Wunsch der Nutzenden kann die Ausstellung solcher im ZBP vorliegender Bescheide durch einen Mechanismus wie einen QR-Code (cross-device) oder einen Deep-Link (same-device) in die EUDI-Wallet ausgelöst werden. Voraussetzung ist, dass diese Bescheide als menschen- und maschinenlesbare Attributsbescheinigung in Form von strukturierten Datensätzen vorliegen. Das ZBP stellt hierzu einen entsprechenden Funktionsaufruf („Button“) für Nutzende zur Verfügung.

Die technische Umwandlung im ZBP vorliegender Datensätze in eIDAS-konforme Formate kann durch den EUDI-Wallet Adapter unterstützt werden. Der EUDI-Wallet Adapter übernimmt die Umwandlung der Bescheide in eIDAS-konforme Attributsbescheinigungen und die Übersetzung von definierten Datenformaten wie z.B. JSON in OpenID4VCI. Der EUDI-Wallet Adapter agiert dabei im Auftrag des

Pub-EAA Providers (Details siehe Anhang I), der formal die Attributsbescheinigung in die EUDI-Wallet ausstellt.

Eine öffentliche Stelle, die die Rolle des Pub-EAA Providers übernimmt, ist bislang nicht definiert. Um eine niedrigschwellige Ausstellung von Attributsbescheinigungen für fachlich zuständige Stellen zu ermöglichen, wird nach aktuellem Überlegungsstand die Möglichkeit eines zentralen Pub-EAA Providers – ein bevollmächtigter Vertreter der für die Authentischen Quellen zuständigen (Fach-)Behörden – evaluiert. Der (zentrale) Pub-EAA Provider nutzt einen qualifizierten Vertrauensdienst (vgl. Siegel und Signaturdienst) für die qualifizierte Siegelung und Signatur der ausgestellten Attributsbescheinigungen und stellt diese mit Hilfe des EUDI-Wallet Adapters der EUDI-Wallet bereit.

4.2.2 Umsetzungsoption 2b: Indirekte Anbindung über NOOTS

Mittel- bis langfristig sollen Attributsbescheinigungen auf Verlangen des Nutzenden synchron und medienbruchfrei direkt aus (Fach-)Registern oder Datenbeständen über das NOOTS an die EUDI-Wallet bereitgestellt werden. Dieser Weg stellt aus Sicht des Bundes den effizientesten und effektivsten Weg der Nachweisausstellung dar – sowohl für die Nutzenden als auch für die Verwaltung. Diese Umsetzungsoption setzt die Anbindung des NOOTS an die EUDI-Wallet voraus. Die gezielte Verzahnung mit dem Programm der Registermodernisierung und NOOTS wird durch den Bund sichergestellt, um Effizienz, Skalierbarkeit und Anschlussfähigkeit im EUDI-Ökosystem zu gewährleisten. Vor diesem Hintergrund ist es aus Sicht des Bundes essenziell, dass die vorgesehene Anbindung der (Fach-)Register an das NOOTS unvermindert fortgesetzt wird.

4.2.3 Umsetzungsoption 2c: Direkte Anbindung an die EUDI-Wallet

Fachlich zuständige Stellen können in der Rolle eines Pub-EAA Providers außerdem Attributsbescheinigungen direkte in die EUDI-Wallet ausstellen. Die konkrete technische Ausgestaltung dieser Umsetzungsoption und die Anforderungen an fachlich zuständige Stellen werden aktuell im laufenden BMDS-Vorhaben zur „Erprobung der Verwaltungsanbindung der EUDI-Wallet“ gemeinsam mit der Stadt Dresden erhoben und praxisnah validiert. Aus Sicht des Bundes sollen jedoch grundsätzlich alle Nachweise, die direkt über NOOTS aus Registern verfügbar sind auch direkt über NOOTS ausgestellt werden.

4.3 Szenario 3: Entgegennahme weiterer Attributsbescheinigungen aus der EUDI-Wallet

Im Rahmen des Szenarios 3 werden, neben der PID, weitere Attributsbescheinigungen aus der EUDI-Wallet genutzt. Ziel ist es, nutzendenseitig in der EUDI-Wallet gespeicherte Attributsbescheinigungen wie etwa ein digitaler Führerschein oder ein Ausbildungsnachweis im Rahmen eines laufenden Verwaltungsverfahrens einzubringen, z. B. als Ergänzung eines Antrags. Konkret bedeutet dies, dass z.B. ein Onlinedienst im Rahmen der Antragstellung eine (technische) Anfrage an die EUDI-Wallet eines Nutzenden stellt, ob eine bestimmte (oder mehrere) Attributsbescheinigungen, die erforderlich sind, in der spezifischen Wallet des Antragstellenden vorhanden sind.

5 Weiteres Vorgehen und Ausblick

Erfolgsentscheidend für die Umsetzung ist die frühzeitige Einbindung aller föderalen Ebenen. Durch das BMDS-Vorhaben zur „Erprobung der Verwaltungsanbindung der EUDI-Wallet“ gemeinsam mit der

Stadt Dresden, dem Land Sachsen und der BundID werden reale kommunale Verwaltungsprozesse sowie fachliche, technische und organisatorische Anforderungen fortlaufend bis Q2 2026 aufgenommen und validiert. Eine darüber hinausgehende kontinuierliche Einbindung weiterer Kommunen sowie der Länder ist angestrebt. Dabei werden laufende Vorhaben zur Verwaltungsdigitalisierung systematisch berücksichtigt, wie das Vorhaben zur „Zielarchitektur für Postfach- und Kommunikationslösungen“ (ZaPuK).

Zur Sicherstellung der sogenannten „Wallet-readiness“ und Erfüllung der verpflichtenden Anforderungen der eIDAS-Verordnung können fachlich zuständige Stellen die Anbindung an die BundID inkl. ZBP und die Bereitstellung strukturierter, maschinenlesbarer Daten über standardisierte Schnittstellen aus zentralen Registern (vgl. Registeranbindung) priorisieren. Die gezielte Verzahnung mit dem Programm der Registermodernisierung zur Anbindung an NOOTS wird durch den Bund sichergestellt. Ziel ist die Entwicklung einer konsistenten, gemeinsam abgestimmten Zielvorstellung, die verdeutlicht, wie beide Programme zusammenwirken, um Synergien bei der Umsetzung der SDG- und der eIDAS-Verordnung zu realisieren. Dabei wird auch auf eine transparente und einheitliche Verwendung unterschiedlicher, jedoch inhaltlich gleichbedeutender Begrifflichkeiten geachtet, um terminologische Klarheit und Verständlichkeit zu gewährleisten. Eine Anbindung von NOOTS und der BundID an die EUDI-Wallet wird vom Bund sichergestellt.

Aktuell wird validiert, einen EUDI-Wallet-Adapter wie in den oben beschriebenen Optionen als zentral entwickelte und von Bund bereitgestellte Komponente auszugestalten. Dabei ist derzeit noch offen, ob der Betrieb durch den Bund selbst erfolgt oder ob die Komponente zur eigenständigen Nutzung bereitgestellt wird. Als Produkt des IT-Planungsrats könnte er von Ländern, Kommunen und fachlich zuständigen Stellen als Dienst genutzt werden.

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). 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 qualifizierte Vertrauensdiensteanbieter überprüfbar sein, sofern sie aus Authentischen Quellen des öffentlichen Sektors stammen (Artikel 45e i. V. m. Anhang VI eIDAS-VO).

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). Relying Parties können von EUDI-Wallet-Nutzenden sowohl personenidentifizierende Daten (PID) als auch nicht-PID-bezogene Attributsbescheinigungen ((Q)EAAs) anfordern und müssen auch in der Lage sein, deren Echtheit und Gültigkeit zu überprüfen (Art. 5a Abs. 5a ii eIDAS-VO). 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). 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.

Relying Party Registrar

Der Relying Party Registrar ist für die Registrierung und Verwaltung von Relying Parties im EUDI-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). Die registrierten Relying Parties werden durch den Registrar in einer EU-Vertrauensliste geführt (Art. 5a Nr. 18a eIDAS-VO, Art. 5b Abs. 5 eIDAS-VO).

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). 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). QTSPs müssen regelmäßig Konformitätsbewertungen durch akkreditierte Stellen durchlaufen und der Aufsichtsstelle Prüfberichte vorlegen (Art. 20 Abs. 1 eIDAS-VO). 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).

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 Adapter

Der EUDI-Wallet Adapter fungiert als Vermittler (engl. Intermediary) im Namen einer Relying Party. Dabei übersetzt er 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 Signaturen und Zertifikate zur Sicherstellung von Echtheit und Gültigkeit.