SÄCHSISCHE
STAATSKANZLEI

Freistaat
SACHSEN

EUDI-Wallet Integration im Freistaat Sachsen

Entscheidungs- und Umsetzungsgrundlage einer zukünftigen Zielarchitektur



*KI- generiert
d-you-Logo © Bundesrepublik Deutschland,
Bundesministerium für Digitales und Staatsmodernisierung

Inhalt

Vorwort **5**

Management Summary **6**

1. Einleitung und Einordnung des Dokuments **11**

1.1 Auftrag und Adressaten des Dokuments 11

1.2 Umsetzungsrahmen 11

1.3 Ausgangslage und Zielposition im Freistaat Sachsen 12

2. Zielarchitektur **14**

2.1 Architekturüberblick 14

2.1.1 Nachweisformate mdoc und SD-JWT VC 16

2.1.2 Wallet-Landschaft und Interoperabilität 16

2.2 Rollen und Verantwortlichkeiten 17

2.3 Grundsätze für das künftige sächsische Landesangebot 17

2.4 Koordination durch die Sächsische Staatskanzlei 18

2.5 Kernfunktionen 19

2.5.1 Identifizierung und Authentifizierung 19

2.5.2 Entgegennahme und Prüfung von Nachweisen 19

2.5.3 Ausstellung von Nachweisen 20

2.6 Rollen und Verantwortlichkeiten 22

2.7 Zugangswege für Bürgerinnen und Bürger 23

3. Entscheidungsgrundlagen der EUDI-Wallet-Integration **24**

3.1 EUDI-Wallet-Ökosystem im Freistaat Sachsen 24

3.2 Stufen der Einführung 24

3.2.1 Gesetzliche Akzeptanzanforderungen erfüllen 24

3.2.2 Empfang von Nachweisen 24

3.2.3 Ausstellen von Nachweisen 25

3.3 Aufbau einer Strategie und Priorisierung von Anwendungssituationen 26

3.4 Betrieb und Steuerung 27

3.5 Anmeldung und technischer Anschluss im EUDI-Wallet-Ökosystem 28

3.6 Roadmap und Abhängigkeiten 29

4. Abkürzungsverzeichnis **30**

5. Glossar **32**

Abbildungsverzeichnis

Abbildung 1: Strategisches Zielbild der EUDI-Wallet-Integration in Sachsen (Planungsstand) 10
Abbildung 2: Funktionale Zielarchitektur und technische Funktionskette 14
Abbildung 3: Drei Umsetzungswege: BundID/ZBP, direkte Anbindung und ZID/NOOTS (nach BMDS) 15
Abbildung 4: Die Kernfunktionen der EUDI-Wallet-Integration 19
Abbildung 5: Roadmap und Abhängigkeiten (direkte Amt24-Anbindung parallel) 29

Vorwort

Dr. Daniela Dylakiewicz - Amtschefin der Sächsischen Staatskanzlei und Beauftragte für Informationstechnologie (CIO) des Freistaates Sachsen

Die digitale Transformation der öffentlichen Verwaltung befindet sich an einem historischen Wendepunkt. Mit der Novellierung der europäischen eIDAS-Verordnung (eIDAS 2.0) und der Einführung der European Digital Identity Wallet (EUDI-Wallet), in Deutschland als „d-you“ etabliert, überschreiten wir die Grenzen rein nationaler E-Government-Strukturen. Bürgerinnen und Bürger erhalten damit eine sichere, plattformunabhängige und europaweit anerkannte digitale Brieftasche direkt auf ihrem Smartphone.

Für den Freistaat Sachsen erwächst daraus nicht nur eine gesetzliche Akzeptanzpflicht ab Anfang 2027, sondern vor allem die strategische Chance, behördliche Prozesse radikal medienbruchfrei, datensparsam und nutzerzentriert neu zu gestalten.

Der Freistaat Sachsen begegnet dieser europäischen Innovationswelle aus einer Position der Stärke. Mit der ressortübergreifenden Strategie zur digitalen Transformation der Sächsischen Staatsverwaltung hat die Staatsregierung den verbindlichen Rahmen für das Verwaltungshandeln fest verankert. Ein Kernversprechen dieser Transformation ist die Bereitstellung einfacher, durchgängig digitaler Angebote nach dem Prinzip „Digital by Default“. Ein Meilenstein dieser Entwicklung ist die vollständige Harmonisierung unserer Identifikationsinfrastruktur.

Sachsen hat seine landesspezifischen eID-Dienste und Portal-Servicekonten auf dem zentralen Landesportal Amt24 erfolgreich zurückgebaut und vollumfänglich auf die BundID sowie Mein Unternehmenskonto (MUK) umgestellt. Diese Konsolidierung war ein Kraftakt für Land und Kommunen, schafft jedoch genau die Standardisierung, die nun als stabiles Sprungbrett für das EUDI-Ökosystem dient.

Sachsen ist bereit, technologische Standards aktiv mitzugestalten - im Rahmen wegweisender Pilotprojekte, wie bei der Erprobung des Dresden-Passes und der Sächsischen Ehrenamtskarte. Hier testen sächsische Akteure in enger Kooperation mit dem Bund bereits das Zusammenspiel zwischen kommunalen Nachweisen, der BundID und der EUDI-Wallet.

Die vorliegende EUDI-Wallet-Strategie für den Freistaat Sachsen führt diese Vorarbeiten konsequent fort und bettet sie in den nationalen Rahmen ein. Maßgeblich hierfür sind die Beschlüsse des IT-Planungsrates (insbesondere B-2025/36-IT und B-2026/19-IT). Der IT-Planungsrat hat mit dem Konzept zur „Verwaltungsanbindung EUDI-Wallet“ ein klares Zielbild definiert. Die Bundesländer sind nun aufgefordert, die Wallet-Anbindung mit Nachdruck voranzutreiben, wahlweise mittelbar über die bewährte Infrastruktur der BundID oder über direkte, native Schnittstellen, um maximale Automatisierungspotenziale in den Fachverfahren freizusetzen. Zudem sichert der IT-Planungsrat über den Ausbau zentraler Issuer- und Verifier-Dienste im Rahmen des deutschen „D-Stack“ eine hohe föderale Nachnutzbarkeit und Wirtschaftlichkeit.

Diese Strategie dient als digitaler Kompass für unsere Landesverwaltung und die sächsischen Kommunen. Sie zeigt auf, wie wir die EUDI-Wallet nicht bloß als rechtliche Pflichtaufgabe implementieren, sondern sie als Katalysator nutzen, um sächsische Behördengänge sicherer, schneller und souveräner in den Alltag der Menschen zu integrieren.

Management Summary

Der Freistaat Sachsen steht vor der Aufgabe, seine Verwaltungsangebote schrittweise an das europäische EUDI-Wallet-Ökosystem anzubinden. Die zentrale Empfehlung dieses Dokuments lautet, dafür ein gemeinsam nutzbares, durch die Sächsische Staatskanzlei koordiniertes Landesangebot vorzubereiten, das vorhandene Bundesleistungen einbindet und zugleich eigenständige standardkonforme Lösungen zulässt. Die EUDI-Wallet soll einen zusätzlichen freiwilligen Zugang zu Verwaltungsleistungen eröffnen. Sie ersetzt weder bestehende digitale und analoge Zugangswege noch die fachliche Verantwortung der jeweils zuständigen Behörde. Für den Freistaat Sachsen kommt es deshalb darauf an, gemeinsame technische Voraussetzungen zu schaffen, ohne eine flächendeckende Einheitslösung oder eine konkrete Produkt- und Betreiberentscheidung vorwegzunehmen.

Die EUDI-Wallet ist eine digitale Brieftasche, in der Bürgerinnen und Bürger Identitätsdaten und elektronische Nachweise auf ihrem Mobiltelefon verwalten können. Bei einer Verwaltungsleistung können sie gezielt die für den jeweiligen Vorgang benötigten Angaben freigeben. Dazu können beispielsweise Identitätsmerkmale, Berechtigungen oder ausgestellte Bescheinigungen gehören. Der mögliche Nutzen entsteht nicht allein durch die Wallet-App, sondern durch das Zusammenspiel mit Online-Diensten, Fachverfahren, Registern sowie technischen Prüf- und Ausstellungsdiensten. Erst wenn diese Systeme abgestimmt zusammenarbeiten, lassen sich Daten strukturiert übernehmen, manuelle Eingaben verringern und bereits bestätigte Angaben in weiteren Verfahren wiederverwenden. Perspektivisch wird damit eine weitgehende Automatisierung von Verwaltungsverfahren ermöglicht.

Der europäische Rechtsrahmen verpflichtet die Mitgliedstaaten, bis zum 24. Dezember 2026 eine nationale EUDI-Wallet bereitzustellen. Die Veröffentlichung einer deutschen EUDI-Wallet, sie trägt den Namen „d-you“, ist für den 2. Januar 2027 geplant. Die Nutzung durch Bürgerinnen und Bürger bleibt freiwillig. Öffentliche Stellen müssen die Wallet akzeptieren, wenn der Zugang zu einem öffentlichen Online-Dienst eine elektronische Identifizierung und Authentifizierung voraussetzt. Daraus folgt jedoch noch keine allgemeine Pflicht, beliebige Nachweise aus der Wallet entgegenzunehmen oder selbst Nachweise in die Wallet auszustellen. Welche Funktionen tatsächlich benötigt werden, muss für jeden Verwaltungsprozess anhand seiner Rechtsgrundlage, seines Datenbedarfs und der beabsichtigten fachlichen Wirkung entschieden werden.

In Deutschland werden wesentliche Grundlagen zentral durch den Bund vorbereitet. Dazu gehören die staatliche EUDI-Wallet-App d-you, die vorgesehene Wallet-Unterstützung der BundID, der EUDI-Wallet Hub DE für Registrierung und Onboarding, eine Verifier-App für die Prüfung von Nachweisen sowie der Zentrale Issuing-Dienst für die registerbasierte Ausstellung über die Infrastruktur des National Once-Only Technical System (NOOTS). Diese Komponenten befinden sich in unterschiedlichen Planungs- und Entwicklungsständen. Für die sächsische Umsetzung sind deshalb nur bestätigte Funktionen, verfügbare Test- und Produktivumgebungen sowie belastbare Anschlussbedingungen einzuplanen. Zieltermine und angekündigte Leistungsumfänge des Bundes sind als Planungsstände zu behandeln und vor einer produktiven Nutzung erneut zu prüfen.

Kernbotschaft:

Ab Ende 2026 muss die Wallet akzeptiert werden, während Umfang und Termine der Bundesleistungen noch weitestgehend Planungsstand sind. Sachsen sollte deshalb jetzt vorbereiten, was es selbst steuern kann, und den Rest an bestätigte Bundesleistungen koppeln.

Das sächsische Zielbild ordnet die bundesweiten Komponenten in die bestehende Verwaltungslandschaft ein. Ausgangspunkt sind Amt24 und weitere Online-Dienste sowie die dahinterliegenden Fachverfahren und Register. Strategisch soll Amt24 direkt an das EUDI-Wallet-Ökosystem angebunden werden, damit die Wallet-basierte Identifikation in Amt24 neben der BundID als Alternative angeboten werden kann. Die Zielarchitektur unterscheidet drei Anbindungswege: die mittelbare Anbindung über BundID und Zentrales Bürgerpostfach, die direkte Anbindung mit oder ohne technische Vermittlungsfunktion sowie die registerbasierte Ausstellung über den Zentralen Issuing-Dienst und NOOTS. Die direkte Amt24-Anbindung schafft zunächst eine Plattformfähigkeit; die Aktivierung weiterer Wallet-Funktionen wird je Online-Dienst und Anwendungsfall geprüft. Die Wege stehen nicht in einem einfachen Entweder-oder-Verhältnis. Sie erfüllen unterschiedliche Aufgaben und können je nach Anwendungsfall aufeinander aufbauen.

Eine zentrale Vermittlungsfunktion kann ein EUDI-Wallet-Adapter übernehmen. Er stellt die standardisierten Wallet-Protokolle über Schnittstellen bereit, an die sich Online-Dienste, Fachverfahren sowie Prüf- und Ausstellungsdienste anschließen können. Die fachlich zuständige Stelle legt fest, welche Nachweise und Attribute benötigt werden, in welchem Umfang eine selektive Offenlegung möglich ist und welche Folge ein Prüfergebnis im Verfahren auslöst. Der Adapter setzt diese Anforderungen technisch um. Er kann Nachweis- und Präsentationsschemata bereitstellen, angeschlossene Systeme über etablierte Schnittstellen anbinden und den technischen Betrieb durch Konfigurations- und Überwachungsfunktionen unterstützen. Fachverfahren und Register bleiben dabei die fachlich führenden Systeme.

Für Vertrauen und Rechtssicherheit genügt es nicht, Daten lediglich aus einer Wallet zu übernehmen. Beim Empfang muss geprüft werden, wer den Nachweis ausgestellt hat, ob seine kryptografische Absicherung gültig ist, ob das erwartete Schema verwendet wird und ob der Nachweis noch gilt oder widerrufen wurde. Bei der Ausstellung sind Datenquelle, Ausstellungsbefugnis, Nachweisschema, Signatur oder Siegel sowie Regeln für Gültigkeit, Status und Widerruf festzulegen. Je nach Nachweistyp können öffentliche Stellen, technische Issuer-Dienste und qualifizierte Vertrauensdiensteanbieter unterschiedliche Aufgaben übernehmen. Die fachliche und rechtliche Verantwortung verbleibt bei der zuständigen Organisation, auch wenn technische Leistungen zentral bereitgestellt oder beauftragt werden.

Für das Landesangebot gelten fünf Leitlinien. Gemeinsame technische Leistungen sollen dort gebündelt werden, wo viele Stellen davon profitieren. Fachverfahren und zuständige Stellen behalten die Verantwortung für Rechtsgrundlage, Datenqualität und fachliche Entscheidung. Bereits vorhandene Bundes- und föderale Leistungen sollen nachgenutzt werden, sofern sie die sächsischen Anforderungen erfüllen. Nur wo für einen nachgewiesenen Bedarf keine geeignete Lösung von Bund oder anderen Ländern verfügbar ist, wird eine eigene sächsische Entwicklung geprüft. Standardisierte Schnittstellen und unabhängige Nachweis- und Präsentationsschemata sollen dauerhafte Abhängigkeiten von einzelnen Anbietern vermeiden. Schließlich müssen alternative digitale und analoge Zugangswege erhalten bleiben, damit die freiwillige Nutzung der Wallet nicht zu einem Ausschluss von Personen ohne EUDI-Wallet oder geeignetes Endgerät führt.

Die Sächsische Staatskanzlei übernimmt in diesem Zielbild vor allem eine strategische, koordinierende und unterstützende Rolle. Sie kann gemeinsame Anforderungen bündeln, die Verbindung zu Bundesleistungen herstellen, Orientierung für Amt24 und weitere Online-Dienste geben und ein freiwillig nutzbares Landesangebot organisieren. Landesbehörden, Kommunen und andere öffentliche Stellen entscheiden weiterhin selbst über ihre Anwendungsfälle, die erforderlichen Daten, die Rechtsgrundlage und die fachliche Verarbeitung. Das Landesangebot soll den Einstieg erleichtern und wiederverwendbare technische Bausteine bereitstellen. Landes- und Kommunalstellen unterscheiden sich deutlich in ihren technischen Voraussetzungen. Das Landesangebot soll deshalb insbesondere Kommunen den Einstieg erleichtern, etwa durch Leitfäden, standardisierte Prozessmuster, technische Blaupausen und Unterstützung bei Einführung und Betrieb. Die Nutzung dieses Angebotes bleibt für jede Kommune freiwillig. Es überträgt keine gesetzlichen Zuständigkeiten und verpflichtet keine Organisation, ausschließlich einen zentralen Weg zu nutzen.

Kernbotschaft:

Sachsen nutzt Bundesleistungen nach, wo sie verfügbar sind und den sächsischen Anforderungen genügen. Die Staatskanzlei koordiniert ein freiwilliges Landesangebot, das insbesondere Kommunen den Einstieg erleichtert; die fachliche Verantwortung bleibt bei der zuständigen Stelle.

Die Einführung sollte in drei Stufen erfolgen. In der ersten Stufe werden die gesetzlichen Akzeptanzanforderungen für Identifizierung und Authentifizierung erfüllt. Amt24 soll hierfür direkt an das EUDI-Wallet-Ökosystem angebunden werden, sodass die Wallet-basierte Identifikation neben der BundID als Alternative angeboten werden kann. Soweit eine BundID-Anbindung verbindlich vorgegeben ist, ist sie umzusetzen. Die direkte Anbindung schafft eine Plattformfähigkeit; die Freischaltung erfolgt für die jeweiligen Online-Dienste nach fachlicher, rechtlicher und technischer Prüfung. Aussagen zu Aufwand und Geschwindigkeit der Anbindungswege setzen erfolgreich abgeschlossene Integrations- und Interoperabilitätstests voraus.

In der zweiten Stufe wird der Empfang strukturierter Nachweise in Amt24 und weiteren Online-Diensten realisiert. Eine Akzeptanzstelle der Wallet fordert nur die für ihren Vorgang benötigten Angaben an, für die zuvor eine Berechtigung zentral beantragt wurde. Die nutzende Person sieht den Zweck der Anfrage und entscheidet über die Freigabe. Ein technischer Verifier prüft Aussteller, seine Signatur oder sein Siegel, Schema, Gültigkeit und Status. Anschließend werden die freigegebenen Daten und das Prüfergebnis strukturiert an den Online-Dienst und in der Folge an das Fachverfahren übergeben. Für digitale Verfahren ist eine integrierte Prüfung grundsätzlich vorteilhaft, weil Daten ohne Medienbruch weiterverarbeitet werden können. Für mobile und Vor-Ort-Situationen bleibt eine geeignete Verifier-App wichtig.

Die dritte Stufe umfasst die Ausstellung von Nachweisen in die EUDI-Wallet. Geeignete Dokumente, welche im Rahmen eines Verwaltungsverfahrens entstehen, können von der zuständigen Stelle oder mit Hilfe eines separaten Dienstes als elektronischer Nachweis ausgegeben werden. Registerbasierte Nachweise sollen perspektivisch über den Zentralen Issuing-Dienst aus Registern erzeugt werden, die an NOOTS angeschlossen sind. Eine parallele sächsische Struktur für Abruf und Ausstellung aus Registern ist neben dem zentralen Dienst nicht vorgesehen. Vor der Umsetzung ist für jeden Nachweistyp zu prüfen, ob bereits ein geeignetes Rulebook sowie ein nutzbares Nachweisschema vorliegen. Bestehende Strukturen sollen nachgenutzt werden, um eine Interoperabilität gewährleisten zu können.

Anwendungsfälle sollten nicht allein danach ausgewählt werden, ob eine technische Anbindung grundsätzlich möglich ist. Neben verbindlich vorgeschriebenen Umsetzungen sollten insbesondere Anwendungsfälle berücksichtigt werden, die einen besonderen Mehrwert für die Bürgerinnen und Bürger bieten.

Für Bürgerinnen und Bürger kann die Wallet Verwaltungsverfahren vereinfachen, wenn sie bestätigte Angaben nicht wiederholt eingeben oder Bescheinigungen erneut als Datei oder auf Papier vorlegen müssen. Der Vorteil hängt jedoch vom konkreten Verfahren ab. Eine zusätzliche technische Lösung ohne abgestimmten Prozess schafft noch keinen Mehrwert. Notwendig sind eine verständliche und barrierefreie Nutzerführung, transparente Datenanfragen, Datensparsamkeit sowie geregelte Wege für abgebrochene Vorgänge, Verlust oder Neueinrichtung einer Wallet. Wer die Wallet nicht nutzen möchte oder kann, muss weiterhin einen geeigneten Zugang zur Verwaltungsleistung erhalten.

Kernbotschaft:

> **Nicht was technisch möglich ist, sondern was den Menschen und Verfahren nützt, bestimmt die Reihenfolge: Anwendungsfälle werden nach verbindlicher Vorgabe und nach Mehrwert für Bürgerinnen und Bürger priorisiert, nicht nach Anschlussfähigkeit.**

Für Betrieb und Steuerung verschiedener Komponenten des EUDI-Wallet-Ökosystems wird ein zentraler Landesbetrieb, beispielsweise als Bestandteil der Basiskomponenten, als mögliches Zielmodell geprüft. Betreiber, Leistungsumfang und Finanzierung sind noch festzulegen; eine künftige Betriebsorganisation könnte ausgewählte gemeinsame Dienste bereitstellen und deren technischen Regelbetrieb verantworten.

Die Roadmap unterscheidet zwischen Vorbereitungen, die der Freistaat Sachsen selbst steuern kann, und Schritten, die von angebotenen Diensten des Bundes abhängen. Die jeweils fachlich verantwortlichen Stellen können bereits jetzt neben der verpflichtenden Identifizierung und Authentifizierung über die EUDI-Wallet mögliche Anwendungsfälle im eigenen Zuständigkeitsbereich erfassen.

Für die weitere Entscheidung ergibt sich damit eine klare Richtung: Alle Akteure im Freistaat Sachsen sollten die gesetzlich notwendige Akzeptanz der EUDI-Wallet vorbereiten, anschließend den Empfang strukturierter Nachweise in ausgewählten Verfahren erproben und die Ausstellung dort erschließen, wo ein belastbarer Wiederverwendungsnutzen besteht. Die Sächsische Staatskanzlei sollte diese Entwicklung koordinieren, gemeinsame Anforderungen bündeln und ein freiwillig nutzbares Landesangebot konkretisieren. Offen bleiben insbesondere Betreiber- und Finanzierungsmodell, Umfang und Nachnutzungsbedingungen zentraler Dienste sowie die Auswahl der ersten Anwendungsfälle. Diese Fragen sollten anhand vorbereiteter Pilotfälle und bestätigter Bundesleistungen entschieden werden, ohne fachliche Zuständigkeiten zu verlagern oder vermeidbare Parallelstrukturen aufzubauen.

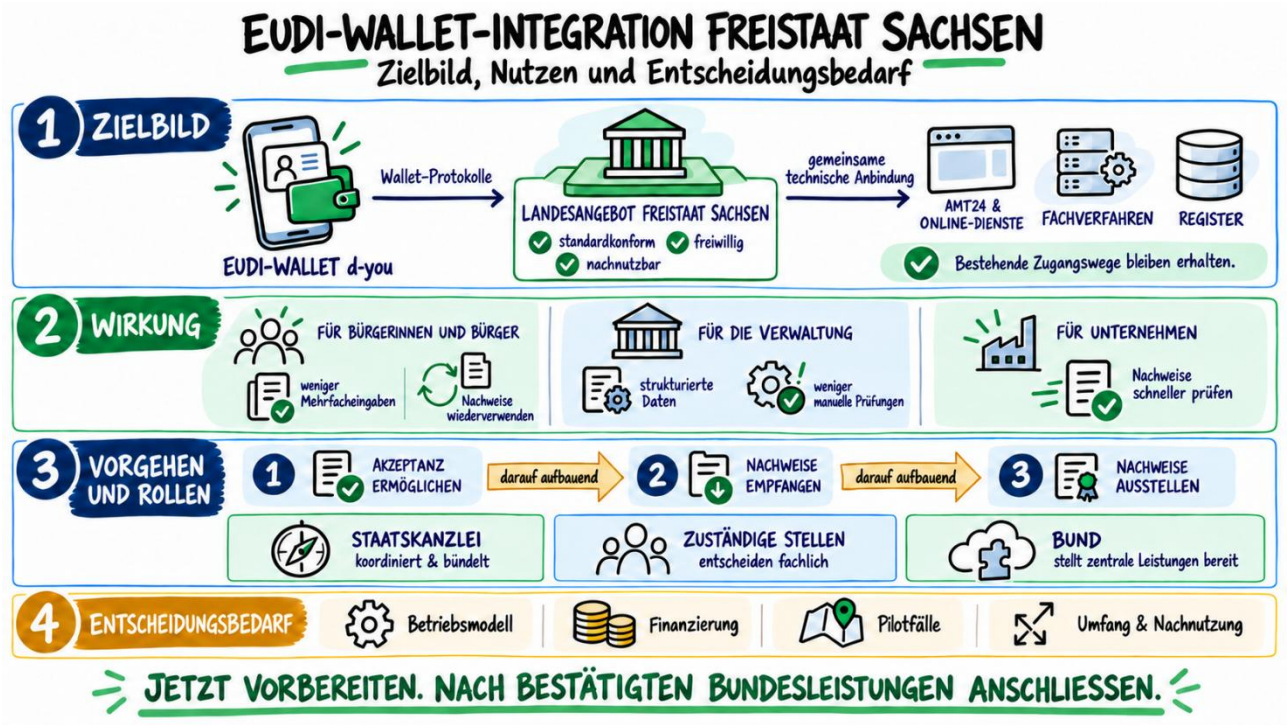


Abbildung 1: Strategisches Zielbild der EUDI-Wallet-Integration in Sachsen (Planungsstand)

1. Einleitung und Einordnung des Dokuments

1.1 Auftrag und Adressaten des Dokuments

Das Dokument erläutert aus Sicht der Sächsischen Staatskanzlei, warum der Freistaat Sachsen ein eigenes Zielbild benötigt und wofür es eingesetzt werden soll. Adressaten sind die Ressorts, kommunale Spitzenverbände und fachlich zuständige Stellen sowie deren IT- und Verfahrensverantwortliche.

Kernaussagen:

- Das Dokument übersetzt den europäischen und bundesweiten Rahmen in ein umsetzbares Zielbild für den Freistaat Sachsen.
- Es dient als fachliche und technische Orientierung. Es ersetzt keine Entscheidung über einzelne Fachverfahren, Nachweistypen oder Beschaffungsvorhaben.
- Es beschreibt die Rolle der Sächsischen Staatskanzlei bei der strategischen Einordnung, Koordination und Unterstützung der Verwaltungsanbindung sowie die Voraussetzungen für die Nutzung eines möglichen Landesangebots.
- Es soll öffentlichen Stellen im Freistaat Sachsen als Orientierung dienen, nachnutzbare Lösungswege aufzeigen und Impulse für eigene Umsetzungsvorhaben geben.

Aus diesem Zweck folgt zunächst die Einordnung in den europäischen und föderalen Umsetzungsrahmen. Darauf aufbauend werden die sächsische Ausgangslage und die daraus abgeleitete Zielposition beschrieben.

1.2 Umsetzungsrahmen

Gemäß der Verordnung (EU) Nr. 910/2014 in der geltenden Fassung müssen die Mitgliedstaaten bis zum 24. Dezember 2026 mindestens eine EUDI-Wallet bereitstellen. Bürgerinnen und Bürger entscheiden freiwillig über ihre Nutzung. Die europäischen Durchführungsrechtsakte konkretisieren unter anderem Registrierung, Schnittstellen, Nachweisformate sowie Vertrauens- und Widerrufsmechanismen. Der Entwurf eines Digitalen-Identitäten-Gesetzes (DIdG) befindet sich mit Stand 8. Oktober 2026 im Gesetzgebungsverfahren und ist bisher nicht als geltendes Recht zu behandeln.

Wird für den Zugang zu einem von einer öffentlichen Stelle erbrachten Online-Dienst eine elektronische Identifizierung und Authentifizierung verlangt, so ist auch die EUDI-Wallet zu akzeptieren. Im BMDS-Rahmen für die Verwaltungsanbindung, der in Kapitel 2.1 für den Freistaat Sachsen konkretisiert wird, beschreibt der Bund drei Wege: mittelbar über BundID und Zentrales Bürgerpostfach, direkt mit oder ohne Wallet-Adapter sowie für den Abruf und die Ausstellung registerbasierter Nachweise über den Zentralen Issuing-Dienst und NOOTS. Eine allgemeine Pflicht für die öffentliche Verwaltung, Nachweise auszustellen oder andere Nachweise über die Personenidentifikationsdaten hinaus aus der Wallet entgegenzunehmen, folgt daraus nicht. Gleichwohl kann die freiwillige Ausstellung und Entgegennahme geeigneter Nachweise medienbruchfreie Prozesse ermöglichen und Verwaltungsverfahren beschleunigen.

Der Bund entwickelt und plant zentrale Komponenten und Dienste, darunter die staatliche EUDI-Wallet und den EUDI-Wallet Hub DE. Die IT-Planungsratsbeschlüsse B-2026/18-IT und B-2026/19-IT ordnen dem Bund unter anderem Verantwortung und Finanzierung für zentrale Leistungen zu und bitten ihn um einen zentralen Issuer- und Verifier-Dienst sowie einen Vorschlag für Verwaltungsvereinbarung und Finanzierung. Zugleich sehen die Beschlüsse für Länder und Kommunen Anschluss, Flächendeckung, Nutzung und abgestimmte Meilensteinplanungen vor. Die direkte Amt24-Anbindung ist davon funktional abzugrenzen und soll nicht unnötig vom noch unbestätigten Umfang zentraler Bundesleistungen abhängig gemacht werden. Welche Bundesleistung zu welchem Zeitpunkt produktiv und nachnutzbar bereitsteht, bleibt als Planungsstand zu behandeln.

Die Umsetzung im Freistaat Sachsen wird im Einklang mit der Deutschland-Architektur und dem D-Stack weiterentwickelt. Daraus folgt die Nachnutzung geeigneter gemeinsamer Komponenten, ohne eine konkrete Produkt- oder Betreiberentscheidung für das Landesangebot vorwegzunehmen. Bestehende Komponenten, Zuständigkeiten und technische Ausgangsbedingungen im Freistaat Sachsen müssen dabei berücksichtigt werden.

1.3 Ausgangslage und Zielposition im Freistaat Sachsen

Der Bund verantwortet die Entwicklung und Orchestrierung der staatlichen EUDI-Wallet sowie die bundesweiten Grundlagen für Registrierung, Zertifikate und Vertrauensinfrastruktur. Zu den bundesweit geplanten Leistungen gehören außerdem eine Verifier-App, der EUDI-Wallet Hub DE und der Zentrale Issuing-Dienst. Die Registermodernisierung und NOOTS werden als eigener Bundesstrang fortgeführt. Politische und architektonische Festlegungen erfolgen im europäischen und föderalen Rahmen, während der Freistaat Sachsen sie für seine Verwaltungslandschaft umsetzt.

Der Freistaat Sachsen verfügt mit Amt24 bereits über eine breite digitale Ausgangsbasis. Mehr als 162.600 Personen nutzen über 3.900 Verwaltungsleistungen staatlicher und kommunaler Behörden in Amt24 (Stand Juni 2026).

Daneben sind 288 Online-Anträge aktiv. Ihr Flächenrollout soll die Bereitstellung in allen 418 sächsischen Städten und Gemeinden ermöglichen. Für die Amt24-Onlineanträge ist die Umstellung vom bisherigen Servicekonto auf BundID beziehungsweise Mein Unternehmenskonto zum 31.12.2026 eingeplant.

Für Amt24 liegen Projektleitung und redaktionelle Betreuung bei der Sächsischen Staatskanzlei, Betrieb und Support beim Staatsbetrieb Sächsische Informatik Dienste. Diese Angaben beschreiben Reichweite und organisatorische Ausgangslage, belegen aber noch keine EUDI-Wallet-Readiness. Strategisch soll Amt24 zusätzlich direkt an das EUDI-Wallet-Ökosystem angebunden werden. Dadurch entsteht eine Plattformfähigkeit für die Wallet-basierte Identifikation neben der BundID; die Aktivierung und weitere Verarbeitung bleiben für jeden Online-Dienst gesondert zu prüfen.

Für den Freistaat Sachsen liegt es nahe, die direkte Anbindung von Amt24 an das EUDI-Wallet-Ökosystem vorzunehmen und weitere Online-Dienste anwendungsfallbezogen einzubeziehen. Zugleich unterscheiden sich Landes- und Kommunalstellen deutlich in ihren technischen Voraussetzungen und im Stand ihrer BundID-, Fachverfahrens- und Registeranbindung.

Die Sächsische Staatskanzlei verfolgt das Ziel, einen zentral koordinierten und niedrigschwelligen Zugang zur EUDI-Wallet zu ermöglichen. Die direkte Amt24-Anbindung bildet dafür einen strategischen Baustein. Ein darüberhinausgehendes Landesangebot soll gemeinsame technische Anforderungen bündeln, Amt24 und weitere Online-Dienste unterstützen und verfügbare Bundesleistungen nachnutzen. Betreiber, Leistungsumfang und Finanzierung sind gesondert festzulegen. Das Angebot soll Landes- und

Kommunalstellen freiwillig zur Verfügung stehen und ist nicht als zwingende flächendeckende Einheitsintegration angelegt.

Jede Organisation kann ihre eigene standardkonforme Integrationsstrategie festlegen. Sie bleibt für ihren Anwendungsfall, ihre Daten und ihre fachlichen Entscheidungen verantwortlich. Das Landesangebot schafft eine nachnutzbare Option und Unterstützung. Es ersetzt weder die Zuständigkeit der jeweiligen Stelle noch die Möglichkeit einer eigenen direkten Anbindung. Gleichwohl sind die insbesondere für die Kommunen in Sachsen zentral bereitgestellten kostenfreien Amt24 Online-Antragsverfahren mit Wallet-Anbindung aus Kosten- und Effizienzgründen konsequent nachzunutzen (Sächsisches EfA-Prinzip).

2. Zielarchitektur

2.1 Architekturüberblick

Die sächsische Zielarchitektur konkretisiert den BMDS-Rahmen als Zusammenspiel von EUDI-Wallet, einer technischen Vermittlungsfunktion, Online-Diensten, Fachverfahren, Verifier-Funktionen und der registerbasierten Ausstellung über ZID und NOOTS. Amt24 soll direkt angebunden werden, damit die Wallet-basierte Identifikation neben der BundID als Alternative angeboten werden kann. Die technische Vermittlungsfunktion übersetzt die standardisierten Wallet-Protokolle für die angeschlossenen Dienste, ohne eine konkrete Produktentscheidung vorwegzunehmen.

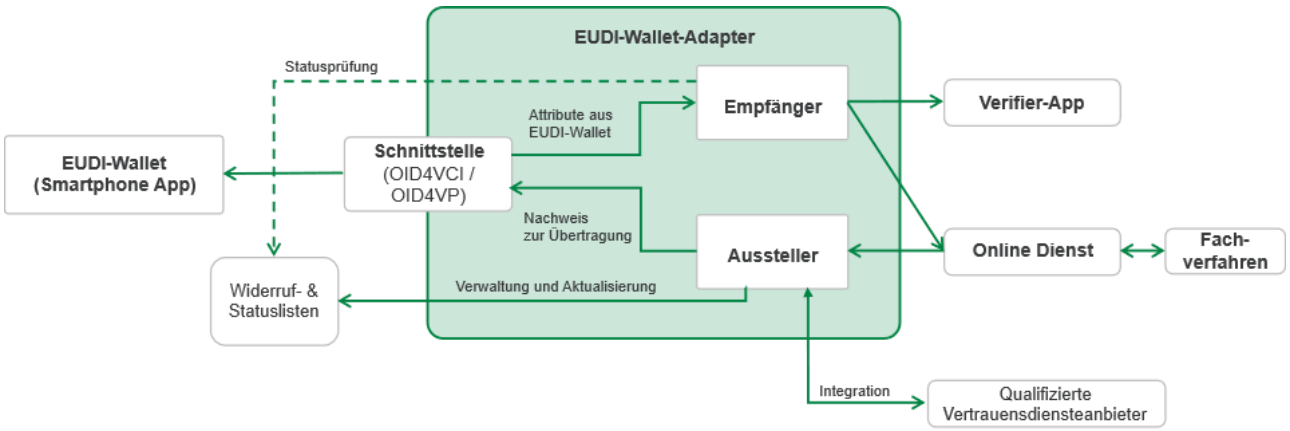


Abbildung 2: Funktionale Zielarchitektur und technische Funktionskette

Zur Wallet-Seite nutzt die Architektur OpenID for Verifiable Presentations (OID4VP) für die Präsentation und OpenID for Verifiable Credential Issuance (OID4VCI) für die Ausstellung von Nachweisen. Empfänger- beziehungsweise Verifier-Dienste nehmen freigegebene Identitäts- und Nachweisdaten entgegen und liefern strukturierte Prüfergebnisse an nachgelagerte Prozesse und Systeme. Aussteller- beziehungsweise Issuer-Dienste erzeugen aus freigegebenen Daten einen signierten oder gesiegelten Nachweis und übertragen ihn an die Wallet.

Der Wallet-Adapter übersetzt die standardisierten Wallet-Protokolle in Schnittstellen, die von Online-Diensten und Ausstellerdiensten verarbeitet werden können. Zwischen dem Adapter und diesen nachgelagerten Systemen werden ausschließlich die für den jeweiligen Vorgang erforderlichen Fachdaten sowie strukturierte Prüf- oder Ausstellungsinformationen ausgetauscht. Wallet-spezifische Protokolldetails verbleiben im Adapter. Welche Nachweise und Attribute in welchem Detailgrad benötigt werden, wird für den jeweiligen Anwendungsfall fachlich festgelegt. Dazu gehört auch die Entscheidung, ob und in welchem Umfang selektive Offenlegung genutzt werden soll. Auf dieser fachlichen Grundlage können Nachweis- und Präsentationsschemata im Adapter hinterlegt und über standardisierte Schnittstellen den angeschlossenen Systemen verfügbar gemacht werden. Ein optionales Dashboard kann Betreiber bei der technischen Konfiguration, der Überwachung des Betriebsstatus und der Nachvollziehbarkeit von Anfragen unterstützen. Der Adapter setzt diese Datenanforderung technisch um und kann gegenüber den angeschlossenen Systemen etablierte Schnittstellenprotokolle wie REST bereitstellen. Die Wallet wählt auf dieser Grundlage geeignete Nachweise aus und ermöglicht der nutzenden Person, nur die angeforderten Attribute freizugeben und nicht den gesamten Nachweis. Fachverfahren und Register bleiben die fachlich führenden Systeme.

Vertrauensdiensteanbieter stellen je nach Nachweistyp qualifizierte Signatur-, Siegel- oder Attributsdienste bereit. Status- und Widerrufslisten ermöglichen dem Verifier, die fortbestehende Gültigkeit von Nachweisen zu prüfen. Maßgeblich sind die für den jeweiligen Nachweistyp vorgesehenen Statusmechanismen, Rulebooks und Vertrauenslisten. Die Abbildung fasst dieses Zusammenspiel zusammen, die folgenden Abschnitte erläutern die einzelnen Schnittstellen.

Das Konzept des BMDS beschreibt drei Wege für die Verwaltungsanbindung: die mittelbare Anbindung über BundID und Zentrales Bürgerpostfach, die direkte Anbindung mit oder ohne Wallet-Adapter sowie die registerbasierte Ausstellung über den Zentralen Issuing-Dienst und NOOTS. Diese Wege erfüllen unterschiedliche Funktionen und bilden gemeinsam den Rahmen für die sächsische Zielarchitektur.

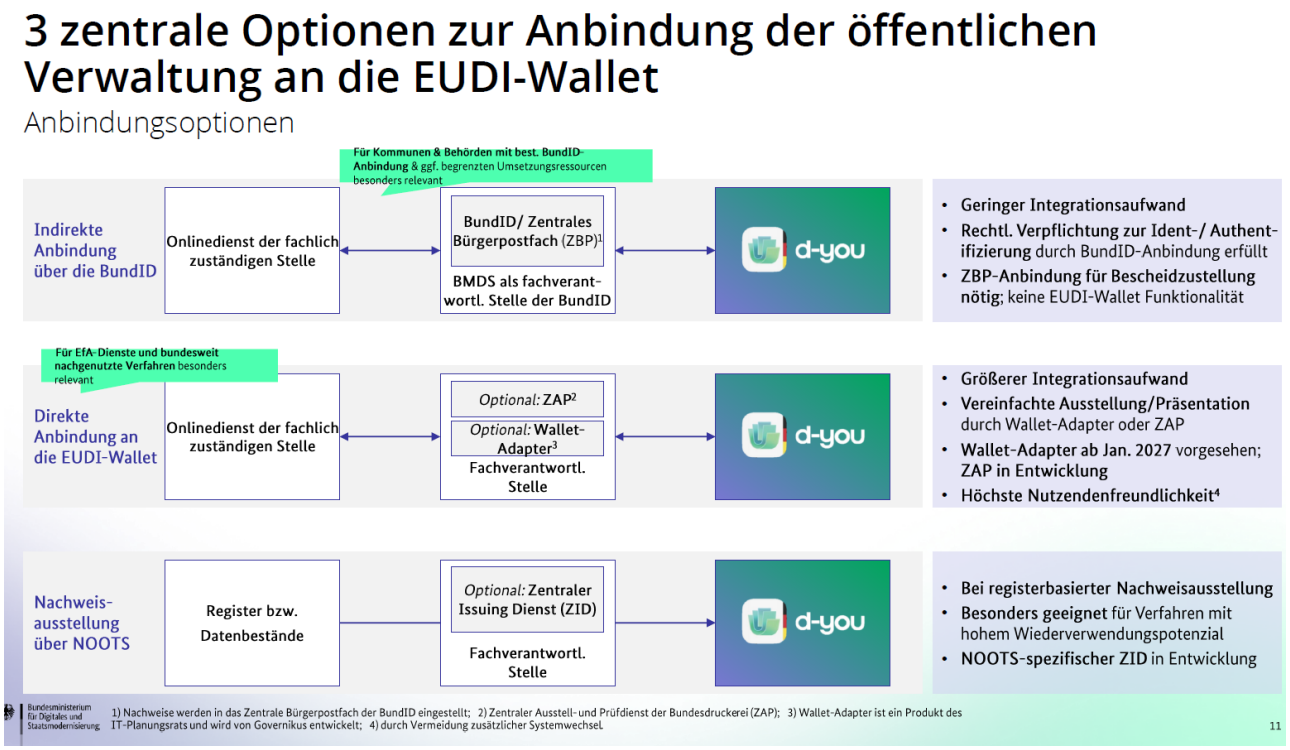


Abbildung 3: Drei Umsetzungswege: BundID/ZBP, direkte Anbindung und ZID/NOOTS (nach BMDS)

Die Abbildung veranschaulicht die drei funktionalen Anbindungswege; enthaltene Produktbeispiele begründen keine Festlegung für den Freistaat Sachsen. Für Fachverfahren und Online-Dienste, bei denen einschlägige Vorgaben eine BundID-Anbindung verlangen, ist diese verbindlich umzusetzen. Daneben soll Amt24 direkt und standardkonform an das EUDI-Wallet-Ökosystem angebunden werden, damit die Wallet-basierte Identifikation in Amt24 neben der BundID als Alternative angeboten werden kann. Die direkte Anbindung schafft eine Plattformfähigkeit; die Aktivierung erfolgt je Online-Dienst nach fachlicher, rechtlicher und technischer Prüfung. Perspektivisch kann die direkte Anbindung auch den Empfang und die Ausstellung weiterer Nachweise unterstützen. Registerdaten werden nicht über eine unkoordinierte parallele Landeslösung abgerufen, sondern grundsätzlich über den vorgesehenen ZID-/NOOTS-Weg eingebunden; ergänzende Landesfunktionen bleiben anhand des bestätigten Bundesumfangs zu prüfen.

BundID, ZBP, EUDI-Wallet Hub DE, Verifier-App, ZID und NOOTS sind konkrete Umsetzungsdienste. Die Zielarchitektur ordnet sie den benötigten Funktionen zu, ohne daraus eine Betreiber- oder Produktentscheidung für den Freistaat Sachsen abzuleiten.

2.1.1 Nachweisformate mdoc und SD-JWT VC

Für Wallet-Nachweise werden insbesondere ISO mdoc und SD-JWT VC als Nachweisformate verwendet. Beide Formate unterstützen kryptografisch geschützte, selektiv offengelegte Attribute und können über die vorgesehenen OpenID-Protokolle ausgestellt und präsentiert werden. Der konkrete Nachweistyp, beziehungsweise sein Rulebook, legt fest, welches Format unterstützt werden soll.

mdoc stammt aus der ISO-18013-Familie und ist besonders für mobile Dokumente sowie Online- und Vor-Ort-Szenarien mit Vor-Ort-Kommunikation etabliert. SD-JWT VC bildet Nachweise im JSON-/JWT-Ökosystem ab und lässt sich gut in webbasierte Dienste und bestehende API-Infrastrukturen integrieren. Die beiden Formate sind nicht als Qualitätsstufen zu verstehen. Interoperabilität entsteht vielmehr, wenn Wallet, Issuer und Verifier dasselbe technische Profil, abgestimmte Schemata und erfolgreich getestete Abläufe verwenden.

2.1.2 Wallet-Landschaft und Interoperabilität

Die für den Freistaat Sachsen relevante Lösungslandschaft umfasst nicht nur Wallet-Apps, sondern auch Referenzimplementierungen, Vermittlungskomponenten, Issuer- und Verifier-Funktionen sowie Integrationsangebote. Die folgenden Beispiele dienen der Markt- und Technologieeinordnung. Sie begründen keine Produktpräferenz und ersetzen keine Eignungs-, Sicherheits- oder Vergabeprüfung.

Im Open-Source-Bereich stehen insbesondere die von der Europäischen Kommission veröffentlichte EUDI-Wallet-Referenzimplementierung und EUDIPLO zur Verfügung. Die Referenzimplementierung stellt quelloffene Bausteine für Wallet-Lösungen bereit. EUDIPLO ist dagegen keine eigene Wallet-App, sondern eine quelloffene Vermittlungskomponente, die Backends über eine einheitliche Schnittstelle mit EUDI-Wallets verbinden soll. Beide Beispiele zeigen, dass der Freistaat Sachsen offene Komponenten nachnutzen kann, ohne die Zielarchitektur an eine einzelne Wallet-App zu binden.

Daneben bieten verschiedene Unternehmen Komponenten und Integrationsleistungen für die Ausstellung, Prüfung oder Anbindung von EUDI-Wallet-Nachweisen an. Exemplarisch zu nennen sind Governikus, Lissi, Procivis und weitere privatwirtschaftliche Anbieter. Die Angebote unterscheiden sich in Funktionsumfang, Betriebsmodell, Offenheit, Zertifizierungsstand und Reifegrad. Für den Freistaat Sachsen sind sie deshalb je nach Leistungsgegenstand als Marktoptionen zu bewerten. Nachweis- und Präsentationsschemata werden unabhängig vom gewählten Wallet-Adapter definiert und über standardisierte Schnittstellen eingebunden. Dadurch bleiben Adapter und Anbieter austauschbar, sofern sie die verbindlichen Protokolle und Schemata unterstützen.

Für Deutschland ist nach dem am 9. September 2026 veröffentlichten Planungsstand zunächst der Start der staatlichen Wallet d-you vorgesehen. Die Marktöffnung für alternative Wallet-Anbieter ist in der bisherigen Ausbaustufenplanung für Januar 2028 angekündigt. Damit ist für das erste Betriebsjahr vor allem d-you als staatliche Referenz relevant. Auch staatliche Wallets anderer Mitgliedstaaten basieren grundsätzlich auf den gemeinsamen europäischen Protokollen. Ob sie mit den jeweils eingesetzten deutschen und sächsischen Komponenten in allen vorgesehenen Anwendungsfällen tatsächlich interoperabel sind, lässt sich erst anhand konkreter Implementierungen und Konformitätstests abschließend bewerten.

Unabhängig vom Anbieter müssen Wallets und angebundene Komponenten die europäischen und nationalen Vorgaben einhalten und grenzüberschreitend interoperabel sein. Die sächsische Architektur sollte deshalb standardbasierte Schnittstellen verwenden, unterschiedliche konforme Wallets testen und einen Anbieter- oder Komponentenwechsel ermöglichen.

2.2 Rollen und Verantwortlichkeiten

Im Folgenden werden die fachlich zuständige Stelle, register- oder datenverantwortliche Stellen und technische Leistungserbringer unterschieden. Die fachlich zuständige Stelle entscheidet, welche Identitätsdaten oder Nachweise benötigt werden, auf welcher Rechtsgrundlage sie verarbeitet werden und welche fachliche Folge ein Prüfergebnis auslöst. Register- und datenverantwortliche Stellen sichern Herkunft und Qualität der verwendeten Daten. Technische Leistungserbringer setzen die festgelegten Anforderungen in Verifier-, Issuer-, Vertrauens- oder Betriebsfunktionen um. Die konkrete Zuordnung richtet sich nach dem jeweiligen Anwendungsfall. Da die technische Unterstützung weder die gesetzliche Zuständigkeit noch die Entscheidung über Rechtsgrundlage, Datenbedarf und fachliche Folgen überträgt, bleibt die Organisation auch dann fachlich verantwortlich, wenn sie sich an einem zentralen Landesdienst orientiert oder technische Leistungen nachnutzt.

Beim Empfang unterstützt ein technischer Verifier die Anforderung, Entgegennahme und kryptografische Prüfung. Beim Ausstellen verantwortet die zuständige Stelle Ausstellungsbefugnis, Inhalt, Datenqualität und Gültigkeit. Ein technischer Issuer, ein Vertrauensdiensteanbieter oder der zentrale Bundesdienst kann einzelne technische Schritte übernehmen. Registerführende Stellen bleiben wiederum für ihre Daten verantwortlich.

Die Sächsische Staatskanzlei kann Anforderungen bündeln, gemeinsame Anschlussmöglichkeiten koordinieren und mit Amt24 oder einem zentralen Landesdienst Orientierung geben. Bundesstellen und weitere Dienstleister stellen übergreifende Wallet-, Registrierungs-, Zertifikats-, NOOTS- oder Vertrauensfunktionen bereit. Betreiber- und Unterstützungsrollen sind vor einem Regelbetrieb gesondert festzulegen.

2.3 Grundsätze für das künftige sächsische Landesangebot

Für das künftige sächsische Landesangebot gelten fünf Gestaltungsgrundsätze:

- Vorhandene Lösungen nachnutzen: Bundesweite und föderal verfügbare Leistungen werden genutzt, wenn sie die sächsischen Anforderungen erfüllen. Nur wo für einen nachgewiesenen Bedarf keine geeignete Lösung von Bund oder anderen Ländern verfügbar ist, wird eine eigene sächsische Entwicklung geprüft.
- Gemeinsame technische Leistungen bedarfsgerecht bereitstellen: Das Land soll Leistungen anbieten, die von vielen Stellen genutzt werden können. Die direkte Amt24-Anbindung ist strategisch vorgesehen. Ob darüber hinaus ein zentral nutzbarer Wallet-Adapter, gemeinsame Verifier- oder Issuer-Funktionen sowie Unterstützung bei Registrierung und Zertifikatsmanagement bereitgestellt werden, ist nach Bedarf, Bundesangebot und Wirtschaftlichkeit gesondert festzulegen. Das Landesangebot soll freiwillig nutzbar sein; jede Organisation kann weiterhin eine eigene standardkonforme Integration umsetzen.
- Fachverfahren und zuständige Stellen bleiben führend: Sie verantworten weiterhin Rechtsgrundlage, Datenqualität, fachliche Ausgestaltung, Prüfung und Entscheidung.
- Dauerhafte Abhängigkeiten vermeiden: Onlinedienste und Fachverfahren werden nicht dauerhaft an einen Anbieter oder eine einzelne technische Lösung gebunden. Anbieter- und Lösungswechsel bleiben möglich.

- Bestehende Zugangswege erhalten: Die Wallet ist ein zusätzlicher Zugang. Andere digitale und nicht digitale Wege werden weiter berücksichtigt, damit die freiwillige Nutzung der Wallet praktisch erhalten bleibt.

2.4 Koordination durch die Sächsische Staatskanzlei

Im Mittelpunkt stehen die strategische Steuerung und Koordination durch die Sächsische Staatskanzlei sowie die direkte Anbindung von Amt24 und die anwendungsfallbezogene Einbindung weiterer Online-Dienste. Ein darüber hinausgehendes Landesangebot wird anhand des nachgewiesenen Bedarfs und bestätigter Bundesleistungen konkretisiert. Es umfasst:

- Handlungsempfehlungen der Sächsischen Staatskanzlei zur Erfüllung der regulatorischen Verpflichtungen zur Identifizierung und Authentifizierung
- Eine technische Vermittlungsfunktion zur direkten, standardbasierten Anbindung von Amt24 und gegebenenfalls weiteren Online-Diensten. Ihr Einsatz und Funktionsumfang richten sich nach den benötigten Funktionen, der Eignung verfügbarer Bundesleistungen, Wirtschaftlichkeit und betrieblicher Unabhängigkeit. Dies kann insbesondere umfassen:
    - Verifier-Funktionen für die technische Prüfung von Identitätsdaten und Nachweisen
    - Issuer-Funktionen für die Ausstellung strukturierter Nachweise
    - Anbindung geeigneter Signatur- und Siegeldienste für die Ausstellung.
- Unterstützung der rollenspezifischen Anmeldung und technischen Anbindung von Relying Parties und Ausstellern.
- Unterstützung der Kommunen bei der Einführung: Leitfäden, standardisierte Prozessmuster und technische Blaupausen sowie Unterstützungsangebote für Einführung und Betrieb. Dabei sollen bestehende Strukturen wie SAKD, Komm24, kommunale Netzwerke und die Digital-Lotsen sowie die Erfahrungen laufender Pilotprojekte, etwa des Proof of Concept in Dresden, einbezogen werden. Die Angebote sind freiwillig nutzbar; sie ersetzen weder die Zuständigkeit der Kommunen noch deren Möglichkeit zu einer eigenen standardkonformen Integration.

Das sächsische Angebot soll verfügbare Dienste des Bundes und föderale Basiskomponenten integrieren oder nachnutzen. Es darf keine vermeidbare Parallelstruktur zu einem zentralen Issuer-, Verifier-, Registrierungs- oder NOOTS-Dienst schaffen.

Eigene Landesfunktionen werden nur für einen nachgewiesenen sächsischen Integrations-, Unterstützungs- oder Betriebsbedarf vorgesehen. Die direkte Amt24-Anbindung bleibt dabei ein eigenständiger strategischer Plattformpfad. Der darüber hinausgehende Leistungsumfang wird anhand der bestätigten Verfügbarkeit, Funktionalität, Nachnutzungsbedingungen und Wirtschaftlichkeit der Bundesdienste entschieden.

2.5 Kernfunktionen

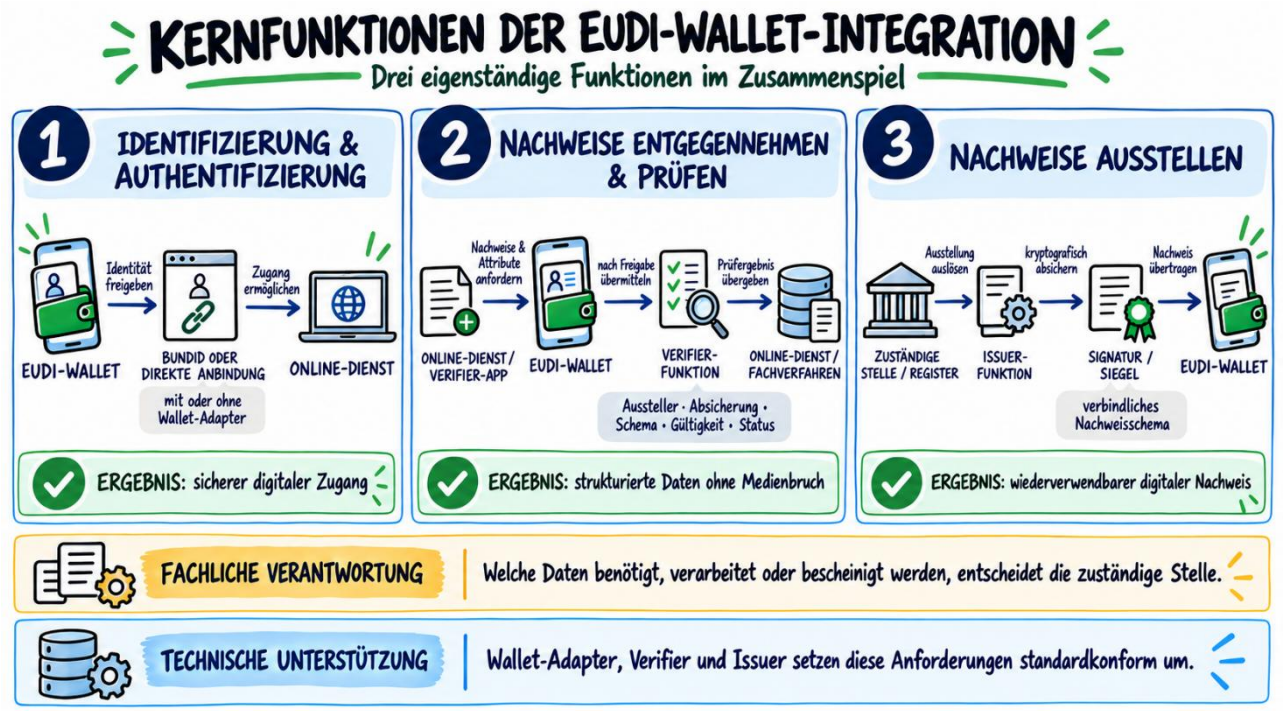


Abbildung 4: Die Kernfunktionen der EUDI-Wallet-Integration

2.5.1 Identifizierung und Authentifizierung

Öffentliche Stellen müssen die EUDI-Wallet akzeptieren, wenn der Zugang zu einem von ihnen erbrachten Online-Dienst eine elektronische Identifizierung und Authentifizierung voraussetzt. Besteht zusätzlich eine verbindliche Vorgabe zur BundID-Anbindung, bleibt diese umzusetzen. In Amt24 soll die Wallet-basierte Identifikation über die direkte Anbindung neben der BundID als Alternative angeboten werden. Die Plattformfähigkeit ersetzt nicht die fachliche, rechtliche und technische Prüfung des jeweiligen Online-Dienstes. Für weitere Dienste ist der geeignete Anbindungsweg anhand des konkreten Anwendungsfalls festzulegen.

2.5.2 Entgegennahme und Prüfung von Nachweisen

Der Empfang strukturierter Nachweise ist deshalb relevant, weil aus der EUDI-Wallet abgefragte und freigegebene Attribute unmittelbar in Online-Dienste einschließlich Formulare und Fachverfahren übernommen werden können. Das kann Medienbrüche und manuelle Erfassung verringern, Rückfragen vermeiden und eine weitgehende Automatisierung ermöglichen. Nachweise können so in vollständig digitalen Angeboten wie auch in Vor-Ort-Situationen angefordert und weiterverwendet werden.

Der Online-Dienst oder die Verifier-App übermittelt der Wallet eine auf den Anwendungsfall abgestimmte Anfrage, in der die benötigten Nachweise und Attribute bezeichnet sind. Die Wallet zeigt der nutzenden Person die angeforderten Daten und den Verwendungszweck an. Nach ihrer Freigabe übermittelt sie nur die erforderlichen Attribute beziehungsweise Nachweise an die Verifier-Funktion. Diese prüft Aussteller, kryptografische Absicherung, Schema, Gültigkeitszeitraum und Status und gibt das strukturierte Prüfergebnis samt freigegebenen Daten an den Online-Dienst oder das Fachverfahren zurück.

Die fachlich zuständige Stelle entscheidet weiterhin, welche Attribute für den konkreten Verwaltungsprozess abgefragt und wie die übermittelten Daten und Prüfergebnisse verarbeitet werden.

Für Amt24, weitere Online-Dienste und Vor-Ort-Anwendungen, etwa im Bürgerbüro oder bei der mobilen Prüfung einer digitalen Berechtigung, werden Datenanforderung, Zuordnung zum Vorgang, Ergebnisübergabe und Fehlerbehandlung je Anwendungsfall konfiguriert. Eine Verifier-App oder andere Bundesleistung wird nur nach bestätigter Verfügbarkeit und Eignung eingeplant.

2.5.3 Ausstellung von Nachweisen

Das Ausstellen strukturierter Nachweise ermöglicht, dass Ergebnisse eines Verwaltungsverfahrens oder bestätigte Registerinformationen unmittelbar digital weiterverwendet werden können. Da empfangende Dienste freigegebene Attribute automatisiert prüfen und in nachgelagerte Prozesse übernehmen können, müssen Nutzende Bescheide oder Bescheinigungen nicht erneut als Datei oder auf Papier vorlegen. Dadurch können durchgängige digitale Verfahren unterstützt werden.

Für die Ausgestaltung der Nachweisausstellung sind EAA, QEAA und Pub-EAA nicht als frei wählbare Ausgangsoptionen gegenüberzustellen. Maßgeblich sind zunächst Rechtsgrundlage, Verwendungszweck und ein bestehendes Rulebook. Dieses bestimmt Nachweistyp, zulässige Aussteller, erforderliche Rechtswirkung, Vertrauensniveau und Prüfanforderungen. Nur wenn kein geeignetes Rulebook besteht, müssen ein neuer Nachweistyp und das zugehörige Rulebook fachlich und rechtlich gestaltet werden. Die Unterschiede zwischen EAA, QEAA und Pub-EAA bleiben für Ausstellerrolle, kryptografische Absicherung und Rechtswirkung relevant und werden im folgenden Abschnitt erläutert.

Die fachlich zuständige Stelle stellt die geprüften Quelldaten für einen festgelegten Nachweistyp bereit und löst die Ausstellung aus. Die Issuer-Funktion übernimmt die erforderlichen Attribute, bildet sie nach dem verbindlichen Nachweisschema ab und versieht den Nachweis entweder selbst oder über einen angebundenen Signatur- beziehungsweise Siegeldienst mit der vorgeschriebenen kryptografischen Absicherung. Anschließend bietet sie den Nachweis über OID4VCI an, sodass die Wallet diesen nach Freigabe durch die nutzende Person übernehmen und speichern kann.

2.5.3.1 Ausstellungswege nach Datenquelle und fachlichem Auslöser

Nachweise aus einem Verwaltungsverfahren entstehen erst durch eine fachliche Entscheidung, beispielsweise mit Bewilligung oder Abschluss eines Vorgangs. Die zuständige Stelle verantwortet Inhalt und Ausstellungsbefugnis, während die technische Ausgabe über das Zentrale Bürgerpostfach, einen nachnutzbaren Issuer-Dienst oder eine direkte Issuer-Anbindung erfolgen kann.

Registerbasierte Nachweise beruhen dagegen auf bereits vorhandenen Daten einer authentischen Quelle. Sie sollen perspektivisch auf Veranlassung der nutzenden Person über den Zentralen Issuing-Dienst aus einem an NOOTS angeschlossenen Register abgerufen, in ein Wallet-Format überführt und ausgestellt werden. Dafür sind Registeranschluss, Abrufberechtigung, Datenqualität und ein geeignetes Nachweisschema erforderlich.

Beide Wege benötigen eine klare Ausstellerrolle, ein verbindliches Nachweisschema, die erforderliche kryptografische Absicherung sowie Regeln für Gültigkeit, Status und Widerruf. Sie unterscheiden sich vor allem darin, ob der Nachweis aus einer neuen Verwaltungsentscheidung oder aus einer bereits vorhandenen Registerinformation entsteht.

Ein weiterer Ausstellungsweg verbindet die Ausstellung mit der Vorlage bereits vorhandener Nachweise (Issuance during Presentation). Dadurch können die sonst getrennten Schritte der Nachweisvorlage, Datenergänzung und Ausstellung in einem durchgängigen Prozess zusammengeführt werden. Der Aussteller fordert dazu über den Verifier beziehungsweise Wallet-Adapter die für den neuen Nachweis erforderlichen

Attribute an. Die Wallet kann geeignete authentische Attribute aus mehreren vorhandenen Nachweisen nach Freigabe durch die nutzende Person bereitstellen. Der Aussteller ergänzt sie bei Bedarf um eigene Verfahrens- oder Registerdaten, prüft die zusammengeführten Angaben und stellt daraus in demselben durchgängigen Prozess einen neuen Nachweis aus. Auf diese Weise lassen sich Attribute aus mehreren Quellen in einem neuen, zweckgebundenen Nachweis bündeln.

2.5.3.2 Rollen- und Falllogik für Akzeptanz und Ausstellung

Für die rechtliche und technische Einordnung ist zunächst zu unterscheiden, ob eine Stelle einen Wallet-Nachweis akzeptiert oder ausstellt. EAA, QEAA und Pub-EAA sind dabei keine frei wählbaren technischen Varianten. Rechtsgrundlage, Verwendungszweck und einschlägiges Rulebook bestimmen Nachweistyp, Ausstellerrolle, Vertrauensniveau, Prüfanforderungen und die erforderliche Infrastruktur.

Akzeptanzstelle: Eine Akzeptanzstelle gestaltet den Nachweistyp nicht selbst und entscheidet nicht zwischen EAA, QEAA und Pub-EAA. Sie legt für ihr Verfahren fest, welche Nachweise und Attribute benötigt werden, und prüft bei der Vorlage, ob der Nachweis den fachrechtlichen Vorgaben, dem einschlägigen Rulebook sowie den technischen und vertrauensbezogenen Prüfanforderungen entspricht. Der Nachweistyp bleibt damit für die Prüfung relevant, ist aber keine Gestaltungsentscheidung der Akzeptanzstelle.

Ausstellung nach bestehendem Rulebook: Will eine öffentliche Stelle einen Nachweis ausstellen, ist zuerst zu klären, ob für diesen Nachweistyp bereits ein anwendbares Rulebook besteht. Die ausstellende Stelle erfüllt diese Vorgaben, woraus folgt, welche technische und vertrauensbezogene Infrastruktur erforderlich ist. Ein geeignetes bestehendes Rulebook ist anzuwenden, bevor ein neuer Nachweistyp gestaltet wird.

Ausstellung mit neuem Rulebook: Besteht kein geeignetes Rulebook, muss die fachlich zuständige Stelle einen neuen Nachweistyp und das zugehörige Rulebook entwickeln oder entwickeln lassen. Vor der technischen Umsetzung sind Rechtsgrundlage, Zweck, Attribute, authentische Quellen, Ausstellungsbefugnis, erforderliche Rechtswirkung und Vertrauensniveau sowie Regeln für Gültigkeit, Status, Widerruf und Akzeptanz festzulegen. Dabei sind die einschlägigen unionsrechtlichen und nationalen Vorgaben einzuhalten. Erst aus diesen Festlegungen folgt, ob der Nachweis als EAA, QEAA oder Pub-EAA auszugestalten ist und welche Komponenten für die Ausstellung benötigt werden.

Eine EAA ist eine elektronische Attributsbescheinigung, die nicht die besonderen Anforderungen einer qualifizierten Bescheinigung oder einer von einer zuständigen öffentlichen Stelle ausgestellten Bescheinigung erfüllen muss; ihre konkrete Vertrauens- und Prüfungslogik ergibt sich aus Rechtsgrundlage und Rulebook. Eine QEAA darf nur von einem qualifizierten Vertrauensdiensteanbieter ausgestellt werden und muss Artikel 45d sowie Anhang V der eIDAS-Verordnung erfüllen. Dazu gehört nach Anhang V Buchstabe g die qualifizierte elektronische Signatur oder das qualifizierte elektronische Siegel des ausstellenden qualifizierten Vertrauensdiensteanbieters.

Eine Pub-EAA ist eine elektronische Attributsbescheinigung, die von einer für eine authentische Quelle zuständigen öffentlichen Stelle oder von einer dafür benannten öffentlichen Stelle in deren Namen ausgestellt wird. Sie muss Artikel 45f und Anhang VII der eIDAS-Verordnung erfüllen; Anhang VII Buchstabe g verlangt die qualifizierte elektronische Signatur oder das qualifizierte elektronische Siegel der ausstellenden Stelle. Der Behördenstatus allein genügt nicht. Zuständigkeit für die authentische Quelle, Benennung beziehungsweise Notifizierung und die Anforderungen an Zuverlässigkeit und Vertrauenswürdigkeit müssen erfüllt sein. Die Rechtswirkungen von QEAA und Pub-EAA ergeben sich insbesondere aus Artikel 45b.

Bei einer QEAA ist der QTSP der Aussteller der qualifizierten Attributsbescheinigung. Die fachlich zuständige Stelle stellt die rechtmäßige Datenquelle, die fachlich geprüften Attribute und den Ausstellungsauftrag sicher. Die genaue Aufgabenteilung bei Identitäts- und Attributprüfung richtet sich nach Artikel 24 der eIDAS-Verordnung, dem Rulebook, den anwendbaren Durchführungsrechtsakten und der konkreten Prozess- und Vertragsgestaltung.

Erfordert das Rulebook einen Signatur-, Siegel- oder qualifizierten Vertrauensdienst, wird dieser über eine definierte Schnittstelle an die Issuer-Funktion angebunden. Ob die sächsische Basiskomponente Elektronische Signatur und Verschlüsselung (ESV) für die im konkreten Nachweistyp benötigte Funktion eingesetzt werden kann, ist fachlich, rechtlich und technisch zu prüfen. Ihr möglicher Einsatz ersetzt weder die Festlegung des berechtigten Ausstellers noch die Einhaltung der Anforderungen an QEAA oder Pub-EAA.

Maßgeblich für die hier behandelten Aspekte sind die Verordnung (EU) Nr. 910/2014 in der durch die Verordnung (EU) 2024/1183 geänderten Fassung, insbesondere Artikel 24, Artikel 45b und Artikel 45d bis 45f sowie die Anhänge V und VII. Technische und verfahrensbezogene Einzelheiten werden unter anderem durch die Durchführungsverordnung (EU) 2025/1569 in ihrer jeweils geltenden Fassung konkretisiert.

2.5.3.3 Vertrauen, Gültigkeit, Status und Widerruf

Aussteller müssen festlegen, wie lange ein Nachweis gilt und unter welchen Voraussetzungen er widerrufen wird. Für QEAA und Pub-EAA ergeben sich die konkreten Vorgaben aus Artikel 45d Absatz 4 und Artikel 45f Absatz 4 der eIDAS-Verordnung sowie aus Artikel 4 der Durchführungsverordnung (EU) 2025/1569 in der jeweils geltenden Fassung. Danach dürfen nur die jeweiligen Anbieter die von ihnen ausgestellten Bescheinigungen widerrufen. Bei einer Gültigkeitsdauer von mehr als 24 Stunden ist ein Widerruf zumindest auf Verlangen der Person, der die Bescheinigung ausgestellt wurde, bei bekannter Beeinträchtigung der Sicherheit oder Vertrauenswürdigkeit sowie in unions- oder nationalrechtlich vorgeschriebenen Fällen erforderlich. Widerrufstechniken müssen die Privatsphäre wahren und Verknüpfbarkeit oder Rückverfolgbarkeit verhindern. Statusinformationen sind so bereitzustellen, dass ihre Integrität und Authentizität gewährleistet sind. Eine widerrufene QEAA oder Pub-EAA verliert ab diesem Zeitpunkt ihre Gültigkeit und darf nicht wieder in den Status „gültig“ zurückkehren.

Technisch verweist der Nachweis auf das vorgesehene Statusverfahren. Abhängig von Format und Rulebook kann dies beispielsweise über eine Token Status List umgesetzt werden. Der Nachweis enthält dabei eine Referenz auf eine vom Aussteller veröffentlichte, kryptografisch geschützte Liste, in der ein Statuswert für diesen Nachweis geführt wird. Ein Verifier ruft die Liste ab und prüft anhand der Referenz, ob der Nachweis gültig oder widerrufen ist. Die Liste bildet nicht den fachlichen Inhalt des Nachweises ab, sondern ermöglicht die Prüfung, ob der betreffende Statuswert beziehungsweise die Kennung noch gültig ist. Gestaltung und Abruf sollen eine unnötige Nachverfolgung einzelner Nutzungen vermeiden.

Die Status- oder Widerrufsinformation ist für die Verlässlichkeit der Nachweisprüfung ein wesentlicher Bestandteil. Ob dafür eine gemeinsam nutzbare Statusinfrastruktur des Landes bereitgestellt wird, ist anhand der Rulebooks, der Rollen der jeweiligen Aussteller, verfügbarer Bundesleistungen, Wirtschaftlichkeit und Betriebsverantwortung gesondert zu entscheiden. Der jeweilige Aussteller legt die Gültigkeitsregeln fest, bewertet fachliche und rechtliche Widerrufsanlässe, veranlasst beziehungsweise vollzieht den Widerruf entsprechend seiner Rolle und sorgt für die unverzügliche Aktualisierung des Status. Bei einer Pub-EAA nimmt diese Verantwortung die ausstellende öffentliche Stelle wahr. Bei einer QEAA ist der QTSP der Aussteller und rechtlich widerrufsbefugt, während die fachlich zuständige Stelle die relevanten Widerrufsanlässe nach dem festgelegten Prozess übermittelt. Ein Verifier prüft bei der Vorlage auch die einschlägige Statusinformation. Der technische Befund wird an den Online-Dienst oder das Fachverfahren übergeben. Die fachliche Entscheidung verbleibt dort.

2.6 Rollen und Verantwortlichkeiten

Für jeden konkreten Anwendungsfall dokumentiert die fachlich zuständige Stelle Rechtsgrundlage, Zweck, benötigte Attribute oder Nachweise und die fachliche Folge des Prüfergebnisses. Register- und datenverantwortliche Stellen bestätigen Herkunft, Qualität und zulässige Nutzung der Daten. Technische Leistungserbringer dokumentieren die übernommenen Verifier-, Issuer-, Vertrauens- oder Betriebsfunktionen

einschließlich Schnittstellen, Sicherheitsanforderungen und Servicegrenzen. Die Rollen sind vor Pilotierung und Regelbetrieb eindeutig zuzuordnen.

Bei Empfang und Ausstellung sind fachliche Verantwortung und technische Ausführung getrennt freizugeben. Eine Organisation kann zugleich Relying Party und Aussteller sein, benötigt dafür jedoch rollenspezifische Registrierung, Zertifikate und Verantwortungszuordnung. Die Nachnutzung eines zentralen Dienstes verlagert weder Ausstellungsbefugnis noch Verantwortung für Datenqualität, Rechtsgrundlage und fachliche Entscheidung.

Die Sächsische Staatskanzlei bündelt übergreifende Anforderungen, koordiniert die direkte Amt24-Anbindung und stimmt Anschlussfragen mit Bund, Ländern und beteiligten Stellen ab. Betreiber-, Support- und Eskalationsrollen sowie die Zuständigkeit für Freigaben sind für jeden gemeinsam genutzten Dienst vor dem Regelbetrieb festzulegen.

2.7 Zugangswege für Bürgerinnen und Bürger

Die Nutzung der EUDI-Wallet bleibt für Bürgerinnen und Bürger freiwillig. Sächsische Online-Dienste müssen daher weiterhin geeignete digitale oder analoge Zugangswege anbieten und dürfen Personen ohne EUDI-Wallet oder ohne geeignetes Endgerät nicht vom Verwaltungsverfahren ausschließen.

Die Nutzerführung berücksichtigt Online-Verfahren auf demselben oder auf einem zweiten Gerät sowie Anwendungen vor Ort. Sie soll barrierefrei und verständlich sein und geregelte Wege für Verlust, Sperrung oder Neueinrichtung einer Wallet vorsehen. Welche Geräte- und Wiederherstellungsfunktionen die staatliche EUDI-Wallet zum Start tatsächlich unterstützt, wird nicht vorweggenommen.

Die fachlich zuständige Stelle legt fest, wie ein unterbrochener Vorgang fortgeführt wird und welcher alternative Zugang zur Verfügung steht. Das zentrale Landesangebot unterstützt die technische Einbindung dieser Wege, ersetzt aber nicht die Verantwortung des jeweiligen Verfahrens.

3. Entscheidungsgrundlagen der EUDI-Wallet-Integration

3.1 EUDI-Wallet-Ökosystem im Freistaat Sachsen

Die Vorbereitung betrifft zunächst bundesweit bereitgestellte Grundlagen. Dazu gehören die geplante Wallet-Unterstützung der BundID, das Onboarding von Relying Parties mit den erforderlichen Zugriffs- und Registrierungszertifikaten, der EUDI-Wallet Hub DE, die Verfügbarkeit einer geeigneten Verifier-App sowie die Registermodernisierung mit NOOTS und dem geplanten zentralen Issuing-Dienst. Die Sandbox bildet dabei die erste Integrationsstufe: Öffentliche Stellen und Unternehmen testen dort ihre Rolle als Relying Party oder Aussteller, den konkreten Anwendungsfall und die technische Anbindung ausschließlich mit Testdaten, bevor sie den produktiven Registrierungsprozess abschließen.

Im Freistaat Sachsen sind insbesondere Amt24, weitere Online-Dienste und Online-Antragsassistenten betroffen. Hinzu kommen die angebundenen Fachverfahren, Register und Datenquellen sowie Landesbehörden, Kommunen und andere öffentliche Stellen, die Identitätsdaten oder Nachweise empfangen beziehungsweise ausstellen wollen.

Die Sächsische Staatskanzlei kann diese Stellen bei der Bestandsaufnahme, der Wahl des Anbindungswegs und der Vorbereitung ihrer Anwendungsfälle unterstützen. Sie bündelt gemeinsame Anforderungen und stellt den Bezug zu verfügbaren Bundesleistungen her. Die jeweilige öffentliche Stelle bleibt für ihren Anwendungsfall, ihre Datenanforderung und die fachliche Verarbeitung verantwortlich.

Die folgenden Abschnitte ordnen die gesetzlichen Akzeptanzanforderungen sowie die fachlichen, technischen und organisatorischen Anschlussvoraussetzungen den drei Einführungsstufen zu. Stufe 1 bereitet die Identifizierung und Authentifizierung vor. Stufe 2 erschließt den Empfang und die Weiterverarbeitung strukturierter Nachweise. Stufe 3 bereitet die Ausstellung geeigneter verfahrens- oder registerbasierter Nachweise vor.

3.2 Stufen der Einführung

3.2.1 Gesetzliche Akzeptanzanforderungen erfüllen

Nach der eIDAS-Verordnung müssen öffentliche Stellen die EUDI-Wallet akzeptieren, wenn der Zugang zu einem Online-Dienst eine elektronische Identifizierung und Authentifizierung voraussetzt. Für die Anbindung an die BundID gelten daneben die jeweils einschlägigen Vorgaben. Ist die BundID für ein Fachverfahren oder einen Online-Dienst verbindlich vorgesehen, muss sie angebunden werden. Parallel soll Amt24 direkt und standardkonform an das EUDI-Wallet-Ökosystem angebunden werden, damit die Wallet-basierte Identifikation neben der BundID als Alternative angeboten werden kann. Für jeden Online-Dienst sind Datenbedarf, Registrierung, Schnittstellen, Prüfergebnisverarbeitung und Freigabe gesondert zu klären.

3.2.2 Empfang von Nachweisen

Über Identifizierung und Authentifizierung hinaus können Akzeptanzstellen in ausgewählten Amt24-Antragsverfahren und weiteren geeigneten Online-Diensten strukturierte Nachweise aus der EUDI-Wallet anfordern und weiterverarbeiten. Für den Freistaat Sachsen liegt es nahe, auf Grundlage der direkten Amt24-

Anbindung und der jeweils verbindlichen BundID-Anbindungen zunächst ausgewählte Empfangsanwendungen anzubinden. Beim Empfang fordert eine öffentliche Stelle ausschließlich die für ihr Verfahren benötigten Nachweise oder Attribute an, prüft sie technisch und verarbeitet das Ergebnis im bestehenden Online-Dienst oder Fachverfahren. Anders als ein Aussteller legt sie weder Inhalt und Schema eines neuen Nachweises noch dessen Gültigkeit, Statusführung und kryptografische Absicherung fest. Deshalb ist die Empfängerrolle in der Regel organisatorisch und rechtlich enger abgegrenzt. Für eine Integration muss die jeweilige Datenanforderung vorab fachlich festgelegt und auf das Nachweisschema abgestimmt werden. Außerdem müssen die freigegebenen Attribute den Formular- und Fachverfahrensfeldern zugeordnet sowie Fehler- und Prüfresultate verarbeitet werden.

Der Empfang kann in einem vollständig digitalen Online-Dienst oder vor Ort über eine geeignete Verifier-App erfolgen. Für durchgängige Verwaltungsprozesse ist die direkte Einbindung der Wallet-Prüfung in lokale Online-Dienste und Backendsysteme grundsätzlich vorzuziehen, weil strukturierte Prüfergebnisse ohne Medienbruch in den jeweiligen Ablauf übernommen werden können. Eine Verifier-App bleibt insbesondere für mobile oder Vor-Ort-Situationen relevant.

Eine wiederverwendbare Funktion im Verifier-Backend erzeugt für den festgelegten Anwendungsfall eine OID4VP-Anfrage und nimmt die Antwort der Wallet entgegen. Anschließend prüft sie den Aussteller, die Signatur oder das Siegel, die Vertrauenskette, das Schema, den Gültigkeitszeitraum und den Status. Die freigegebenen Daten und ein einheitlich aufgebautes Prüfergebnis übergibt sie über eine standardisierte Schnittstelle an den jeweiligen Online-Dienst oder an das angeschlossene Fachverfahren, Kassensystem oder Buchungssystem. Damit unterscheidet sich diese Funktion von einer Verifier-App, die vor allem für mobile oder situative Einzelprüfungen eingesetzt wird. Eine Backend-Anbindung kann insbesondere bei wiederkehrenden Zugangs- und Berechtigungsprüfungen, etwa in Museen, Schwimmbädern oder vergleichbaren Einrichtungen, praktikabler sein. Eine bestätigte, produktiv nutzbare Landes- oder Bundeslösung liegt derzeit nicht vor. Es besteht daher Bedarf, die fachlichen, technischen, datenschutzrechtlichen, sicherheitsbezogenen, betrieblichen und interoperabilitätsbezogenen Anforderungen aufzunehmen und mit anderen Ländern sowie den zuständigen Bundesstellen zu erörtern. Ob eine solche Komponente nachgenutzt, gemeinsam entwickelt oder beschafft wird, bleibt offen; aus diesem Bedarf folgt keine konkrete Aufgabe mit Frist.

3.2.3 Ausstellen von Nachweisen

Die Ausstellung Wallet-fähiger Nachweise schafft Nutzen über das einzelne Ausgangsverfahren hinaus. Denn ein einmal ausgestellter, maschinenprüfbarer Nachweis kann mit Einwilligung der nutzenden Person in weiteren Verwaltungsleistungen wiederverwendet werden, ohne erneut Daten zu erheben oder manuelle Prüfungen vornehmen zu müssen. Ebenso können nachgelagerte Prozesse in der Privatwirtschaft beschleunigt werden, wenn beispielsweise Unternehmen benötigte Nachweise strukturiert und verlässlich prüfen können. Genehmigungs- und Anschlussprozesse können dadurch schneller, medienbruchärmer und für Bürgerinnen, Bürger sowie Unternehmen besser planbar werden.

Die dritte Einführungsstufe richtet sich an öffentliche Stellen, Online-Dienste und Kommunen, die Nachweise in eine EUDI-Wallet ausstellen wollen. Sie folgt auf die Vorbereitung der Akzeptanzstellen und die Erschließung geeigneter Empfangsanwendungen.

Registerbasierte Nachweise sollen perspektivisch über den Zentralen Issuing-Dienst des Bundes aus Registern erzeugt werden, die an NOOTS angeschlossen sind. Die fachlich zuständigen und registerverantwortlichen Stellen wählen geeignete Registerfälle aus, bereiten die Registeranbindung vor und klären Datenqualität sowie Abrufberechtigung. Eine unkoordinierte parallele sächsische Abrufstruktur soll vermieden werden. Ob ergänzende Landesfunktionen für einzelne Nachweistypen erforderlich sind, wird anhand des bestätigten Funktionsumfangs und der Nachnutzungsbedingungen des Bundesdienstes entschieden.

Nachweise, die erst durch ein Verwaltungsverfahren entstehen, können durch die zuständige Stelle oder einen beauftragten Ausstellungsdienst ausgegeben werden. Vorab sind ein vorhandenes oder neu festzulegendes Nachweisschema, die Ausstellungsbefugnis, die benötigten Attribute und der technische Issuer-Weg zu klären.

Das anwendbare Rulebook oder, bei einem neuen Nachweistyp, die fachliche und rechtliche Gestaltung bestimmt, ob eine EAA, QEAA oder Pub-EAA erforderlich ist. Für QEAA und Pub-EAA gelten besondere Anforderungen an qualifizierte Signaturen oder Siegel, Vertrauensketten sowie Status und Widerruf. Ein vorhandener sächsischer Signatur- oder Siegeldienst kann ein Baustein sein, wenn seine fachliche, rechtliche und technische Eignung für den konkreten Nachweistyp bestätigt ist.

3.3 Aufbau einer Strategie und Priorisierung von Anwendungssituationen

Stellen des Landes und der Kommunen sollen für ihren Zuständigkeitsbereich eine eigene Taktik für die Nutzung der EUDI-Wallet entwickeln. Ausgangspunkt ist ein Portfolio möglicher Anwendungssituationen. Dazu gehören Verwaltungsleistungen, Fachverfahren und Online-Dienste ebenso wie Leistungen ohne eigenes Fachverfahren und Anwendungen vor Ort, beispielsweise die Prüfung einer Ermäßigungsberechtigung in einem Museum.

Die Betrachtung beginnt bei einem konkreten Bedarf von Bürgerinnen und Bürgern, Unternehmen oder der Verwaltung. Sie beginnt nicht bei einer technischen Komponente. Dies entspricht dem Ansatz des Architecture and Reference Frameworks für die EUDI-Wallet, das reale Anwendungsfälle und Nutzerabläufe als Ausgangspunkt der fachlichen und technischen Ausgestaltung verwendet.

Der Freistaat Sachsen wird einen gemeinsamen Vorgehensrahmen mit einheitlichen Kriterien und aktuellen Informationen zu Rulebooks, Nachweisschemata und nachnutzbaren Komponenten bereitstellen. Die Auswahl und Priorisierung der Anwendungssituationen bleibt Aufgabe der jeweils verantwortlichen Stelle.

1. Anwendungssituationen erfassen und abgrenzen

Vor der Aufnahme in die Umsetzungsplanung sollten der Nutzen und insbesondere Reichweite, Mehrwert für Bürgerinnen und Bürger, Verbesserungen für die Verwaltung, die Wiederverwendung von Daten und der Wegfall manueller Arbeitsschritte bestimmt. Danach können die entsprechenden Änderungen an Prozessen und Systemen untersucht werden. Dazu gehören die Anbindung betroffener Dienste und Fachverfahren, die technische Prüfung von Identitätsdaten und Nachweisen sowie die Verarbeitung des Prüfergebnisses.

Anschließend ist zu prüfen, welche Komponenten und Dienste des Freistaates Sachsen, des Bundes oder anderer öffentlicher Stellen nachgenutzt werden können. Ihre Eignung richtet sich nach der fachlichen Passung, der Einhaltung der EUDI-Standards, dem Integrationsaufwand, der Betriebsverantwortung, den Betriebskosten und den Risiken. Erst wenn keine geeignete Lösung verfügbar ist, kommen eine Anpassung vorhandener Komponenten oder eine Eigenentwicklung in Betracht. Dabei sind auch Anwendungen ohne Fachverfahren zu berücksichtigen. Das Ergebnis ist ein Portfolio möglicher Anwendungssituationen. Es darf zunächst mehr Fälle enthalten, als kurz oder mittelfristig umgesetzt werden können.

2. Benötigte Wallet-Anforderungen und Rollen zuordnen

Jede Anwendungssituation wird den benötigten Wallet-Funktionen zugeordnet. Zu unterscheiden sind die Identifizierung und Authentifizierung, die Entgegennahme und Prüfung von Nachweisen sowie die Ausstellung von Nachweisen. Eine Anwendungssituation kann mehrere dieser Funktionen verbinden. Aus dieser Zuordnung ergeben sich die beteiligten Rollen und Datenflüsse. Es ist zu klären, welche Stelle Nachweise

entgegennimmt, welche Stelle sie ausstellt, aus welcher authentischen Quelle die Daten stammen und wer das Nachweisschema und das Rulebook verantwortet.

Für jede Anwendungssituation ist zudem zu bestimmen, welches Ergebnis erreicht werden soll und welche Informationen dafür erforderlich sind. Dabei ist zu prüfen, ob eine eindeutige Identifizierung notwendig ist oder ob der Nachweis eines Merkmals, einer Berechtigung oder ein Pseudonym ausreicht. Außerdem sind beispielsweise die benötigten Attribute, ihre Quellen und deren Rechtsgrundlage festzulegen.

Es dürfen nur die für den jeweiligen Zweck erforderlichen Daten angefordert werden. Eine als Relying Party tätige Stelle muss den Verwendungszweck und die benötigten Daten angeben und sich gegenüber der Wallet authentifizieren.

Soll ein Nachweis ausgestellt werden, ist vor der technischen Ausgestaltung zu prüfen, ob bereits ein geeignetes Rulebook und ein nutzbares Nachweisschema bestehen. Maßgeblich sind die fachliche Passung, der aktuelle Stand, die vorgesehenen Attribute und Datenquellen, zulässige Aussteller, Vorgaben für Gültigkeit und Widerruf sowie Anforderungen an Vertrauensdienste, Signaturen oder Siegel.

Ein geeignetes Rulebook und Nachweisschema sind bevorzugt zu übernehmen. Besteht keine geeignete Grundlage, muss zunächst geklärt werden, ob tatsächlich ein neuer Nachweistyp benötigt wird. Danach sind die fachliche Zuständigkeit, die Wiederverwendbarkeit, der verantwortliche Scheme Provider sowie die Erstellung und Pflege des Rulebooks festzulegen.

Die Nutzung der EUDI-Wallet bleibt für Bürgerinnen und Bürger freiwillig. Eine Verpflichtung öffentlicher Stellen zur Bereitstellung oder Akzeptanz der Wallet begründet keine Nutzungspflicht. Alternative Zugangswege zu öffentlichen Leistungen sind daher weiterhin zu berücksichtigen.

3. Erproben, validieren und Strategie weiterentwickeln

Geeignete Anwendungssituationen werden zunächst in einem begrenzten und auswertbaren Rahmen erprobt. Hierbei werden die in Schritt 1 festgelegten Effekte validiert. Dazu können beispielsweise Nutzungsquoten, Bearbeitungszeiten, Fehlerquoten, der Wegfall manueller Arbeitsschritte, Kosten je Vorgang und die Zufriedenheit der Beteiligten gehören. Auf Grundlage dieser Ergebnisse können die Strategie weiterentwickelt, die Anwendungen verbessert und die Akzeptanz der EUDI-Wallet erhöht werden.

3.4 Betrieb und Steuerung

Als mögliches Zielmodell wird ein zentraler Landesbetrieb geprüft. Eine noch festzulegende Betriebsorganisation könnte ausgewählte gemeinsame EUDI-Wallet-Komponenten, sofern nicht vom Bund, zentral bereitstellen und deren technischen Regelbetrieb verantworten. Landes- und Kommunalstellen könnten diese Dienste über definierte Schnittstellen sowie verbindliche Anschluss- und Leistungsbedingungen nutzen. Betreiber, Leistungsumfang, Finanzierung und die Abgrenzung zu Bundesleistungen bleiben gesondert zu entscheiden.

Der zentrale Leistungsumfang kann insbesondere Wallet-Adapter, Verifier- und Issuer-Funktionen, Zertifikatsmanagement sowie Status- und Widerrufsdienste umfassen. Welche Komponenten tatsächlich zentral angeboten werden, ist gesondert festzulegen. Die technische Leistungserbringung kann ganz oder teilweise einem öffentlichen oder privaten IT-Dienstleister übertragen werden. Eine solche Beauftragung ist eine Umsetzungsform des zentralen Landesbetriebs und kein eigenständiges Betriebsmodell. Die zentrale Betriebsverantwortung verbleibt bei der dafür bestimmten Organisation. Vergabe- und Vertragsmodell müssen Steuerungs- und Kontrollrechte, Service Levels, Datenverarbeitung, Haftung, Anbieterwechsel und die Vermeidung dauerhafter Abhängigkeiten absichern.

Die jeweils fachlich zuständige Stelle bleibt für Rechtsgrundlage, Datenbedarf, Ausstellungsbefugnis und fachliche Entscheidung verantwortlich. Der zentrale technische Betrieb verlagert diese gesetzlichen und fachlichen Zuständigkeiten nicht. Fachliche Verantwortung, strategische Steuerung und technische Leistungserbringung sind deshalb auch im zentralen Modell ausdrücklich voneinander abzugrenzen.

Vor der Umsetzung sind insbesondere Betriebsorganisation, Finanzierung, Umfang und Verfügbarkeit der zentralen Leistungen, Anschlussbedingungen für Landes- und Kommunalstellen, Skalierbarkeit, Datenschutz, Informationssicherheit, Zertifikats- und Schlüsselmanagement, Versionierung, Sicherheitsaktualisierungen, Interoperabilität, Störungs- und Notfallmanagement, Service Levels, Haftung, Anbieterwechsel und Exit-Regelungen festzulegen.

Das zentrale Zielmodell legt noch nicht fest, welche Organisation einzelne Komponenten betreibt oder welche Leistungen heute der SID übernimmt. Betreiber, konkreter Leistungsumfang und Finanzierungsverantwortung bleiben als gesonderte Entscheidungen auszuarbeiten.

3.5 Anmeldung und technischer Anschluss im EUDI-Wallet-Ökosystem

Öffentliche Verwaltungen und Unternehmen benötigen für den Zugang zum EUDI-Wallet-Ökosystem einen klar beschriebenen Anwendungsfall und die Rolle als Relying Party oder Aussteller. Sie bereiten die beabsichtigte Datennutzung, die fachliche Zuständigkeit sowie die technische Integration vor und validieren den Anwendungsfall zunächst in der Sandbox mit Testdaten. Der produktive Anschluss erfordert die Registrierung der Organisation und ihres Anwendungsfalls im nationalen EUDI-Wallet-Ökosystem sowie die erforderlichen Zugangs- und Registrierungszertifikate.

Der EUDI-Wallet Hub DE ist als zentrale digitale Unterstützung für Registrierung und Onboarding vorgesehen. Nach dem öffentlich bekannten Planungsstand übernimmt die Common Codes GmbH die Rolle des Scheme Operators für die nationalen Lists of Trusted Entities und damit deren Einrichtung, Pflege, Signatur und Veröffentlichung. Weitergehende Zuständigkeiten und der verfügbare Leistungsumfang sind zum Umsetzungszeitpunkt gesondert zu prüfen.

Die Sächsische Staatskanzlei kann sächsische Stellen beim Einstieg, bei der Zuordnung zu Amt24 und weiteren Online-Diensten sowie bei der technischen Vorbereitung unterstützen. Die Verantwortung für Anwendungsfall, Rechtsgrundlage, angeforderte Daten und fachliche Verarbeitung verbleibt bei der jeweils zuständigen Organisation.

3.6 Roadmap und Abhängigkeiten

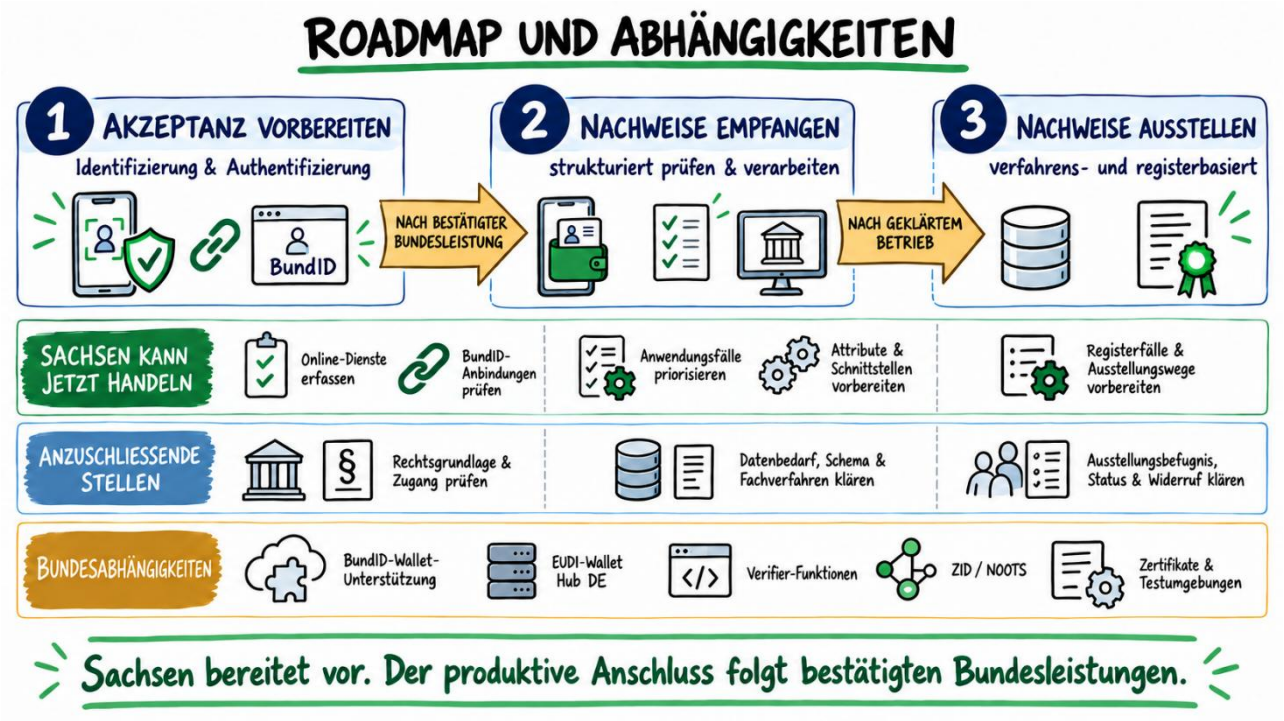


Abbildung 5: Roadmap und Abhängigkeiten (direkte Amt24-Anbindung parallel)

Die Einführung folgt drei fachlichen Stufen, die in parallelen Umsetzungssträngen vorbereitet werden. Für verbindlich vorgegebene Verfahren werden BundID-Anbindungen umgesetzt. Parallel wird die direkte Amt24-Anbindung als Plattformfähigkeit für die Wallet-basierte Identifikation vorbereitet, in einer Testumgebung interoperabel erprobt und anschließend für ausgewählte Online-Dienste pilotiert. Empfang und Ausstellung werden danach anwendungsfallbezogen ergänzt.

Für jede Einführungsstufe sind Verantwortliche, Voraussetzungen, Entscheidungstore, Abnahmekriterien, Abhängigkeiten und ein Ausweichweg zu dokumentieren. Für die direkte Amt24-Anbindung bilden ein abgestimmtes Schnittstellen- und Sicherheitskonzept, ein erfolgreicher Sandbox- und Interoperabilitätstest, die Freigabe eines Pilotumfangs und die Produktivfreigabe nachvollziehbare Entscheidungstore. Bundesleistungen werden erst eingeplant, wenn Funktionsumfang, Test- und Produktivumgebung, Anschlussbedingungen und Finanzierung belastbar bestätigt sind.

Die Sächsische Staatskanzlei koordiniert die übergreifende Planung und die strategische Einordnung. Die für Amt24 zuständigen Betriebs- und Technikverantwortlichen bereiten Plattformintegration, Tests und Pilotierung vor. Die fachlich verantwortlichen Stellen erfassen relevante Online-Dienste, wählen Anwendungsfälle aus, bestimmen Attribute und Nachweise und klären Rechtsgrundlage, Feldzuordnung, Prüfergebnisverarbeitung und fachliche Freigabe. Diese Arbeiten können unabhängig von noch ausstehenden Bundeskomponenten beginnen.

Sobald eine für einen priorisierten Anwendungsfall benötigte Bundesleistung mit bestätigtem Funktionsumfang verfügbar ist und die Bedingungen für Test, Anschluss und Nachnutzung geklärt sind, entscheiden die fachlich verantwortlichen Stellen über den Anschluss. Der direkte Amt24-Pfad wird unabhängig davon entlang seiner eigenen Entscheidungstore fortgeführt. Ergänzende Landesleistungen werden nur vorgesehen, wenn ein konkreter Integrations-, Unterstützungs- oder Betriebsbedarf nachgewiesen ist.

4. Abkürzungsverzeichnis

Abkürzung	Bedeutung
API	Application Programming Interface (Programmierschnittstelle)
BMDS	Bundesministerium für Digitales und Staatsmodernisierung
BundID	Nutzerkonto des Bundes für die Identifizierung und Authentifizierung
EAA	Electronic Attestation of Attributes (elektronischer Attributsnachweis)
eIDAS	electronic Identification, Authentication and Trust Services (EU-Verordnung über elektronische Identifizierung und Vertrauensdienste)
ESV	Basiskomponente Elektronische Signatur und Verschlüsselung (Freistaat Sachsen)
EUDI	European Digital Identity (europäische digitale Identität)
EUDI-Wallet	European Digital Identity Wallet (europäische Brieftasche für die digitale Identität)
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
JSON	JavaScript Object Notation
JWT	JSON Web Token
NOOTS	National Once-Only Technical System
OID4VCI	OpenID for Verifiable Credential Issuance (Standard für die Ausstellung digitaler Nachweise)
OID4VP	OpenID for Verifiable Presentations (Standard für die Vorlage digitaler Nachweise)
PID	Person Identification Data (Personenidentifizierungsdaten)
Pub-EAA	Public Body EAA (elektronischer Attributsnachweis, ausgestellt von oder im Auftrag einer öffentlichen Stelle)
QEAA	Qualified Electronic Attestation of Attributes (qualifizierter elektronischer Attributsnachweis)
QTSP	Qualified Trust Service Provider (qualifizierter Vertrauensdiensteanbieter)
REST	Representational State Transfer (Architekturstil für Schnittstellen)

Abkürzung	Bedeutung
SD-JWT	Selective Disclosure JSON Web Token (Nachweisformat mit selektiver Datenfreigabe)
VC	Verifiable Credential (überprüfbarer digitaler Nachweis)
SID	Staatsbetrieb Sächsische Informatik Dienste
ZBP	Zentrales Bürgerpostfach (der BundID)
ZID	Zentraler Issuing-Dienst (des Bundesverwaltungsamts)

5. Glossar

Begriff	Erklärung
Attribut	einzelnes Merkmal einer Person oder Organisation (zum Beispiel Name, Geburtsdatum oder eine Berechtigung), das Bestandteil eines Nachweises ist und selektiv geteilt werden kann
Authentifizierung	technischer Vorgang, mit dem eine Person die Kontrolle über eine behauptete Identität nachweist, etwa beim Anmelden an einem Online-Dienst
Basiskomponente	zentral bereitgestellte E-Government-Komponente des Bundes oder des Freistaats Sachsen, die von mehreren öffentlichen Stellen nachgenutzt werden kann; eine sächsische Basiskomponente ist beispielsweise die BaK ESV
BundID	zentrales Nutzerkonto des Bundes für die Identifizierung und Authentifizierung gegenüber Online-Diensten einschließlich des Zentralen Bürgerpostfachs (ZBP)
EUDI-Wallet	Europäische digitale Brieftasche nach der eIDAS-2.0-Verordnung: eine App, mit der Bürgerinnen und Bürger Identitätsdaten und Nachweise sicher speichern, verwalten und selektiv teilen können
EUDI-Wallet-Ökosystem	Gesamtheit der Akteure und Infrastrukturen rund um die EUDI-Wallet, darunter Wallet-Anbieter, Issuer, Relying Parties und die Vertrauensinfrastruktur
Fachverfahren	IT-Verfahren einer Behörde zur fachlichen Bearbeitung von Verwaltungsleistungen; je nach Aufgabe verarbeitet es Antrags-, Nachweis- oder Registerdaten und unterstützt fachliche Entscheidungen
Identifizierung	eindeutige Feststellung der Identität einer Person, in der EUDI-Wallet auf Basis der Personenidentifizierungsdaten (PID) auf Vertrauensniveau hoch
Issuer	ausstellende Organisation beziehungsweise technische Funktion für digitale Nachweise. Die Organisation verantwortet Ausstellungsbefugnis und Inhalt; die technische Issuer-Funktion erzeugt den Nachweis, versieht ihn je nach Typ mit Signatur oder Siegel und übermittelt ihn an die EUDI-Wallet
Nachweis	digital signierte oder gesiegelte, maschinell prüfbare Bescheinigung über Attribute einer Person oder Organisation
Onboarding	Prozess der rollenspezifischen Registrierung, Prüfung und technischen Anbindung einer Organisation als Relying Party oder Aussteller im EUDI-Wallet-Ökosystem

Begriff	Erklärung
Online-Dienst	digitaler Verwaltungsdienst, über den Bürgerinnen, Bürger und Unternehmen Anträge stellen und mit der Verwaltung interagieren
Relying Party	vertrauende Partei: Organisation, die Nachweise oder Attribute aus einer EUDI-Wallet anfordert und dafür rollenspezifisch registriert sein muss; eine zusätzliche Ausstellerrolle ist getrennt zu behandeln
Rulebook	nachweisspezifisches Regelwerk im EUDI-Ökosystem, das Datenstruktur, Semantik sowie Ausstellungs- und Prüfregeln eines Nachweistyps festlegt
Verifier	Rolle beziehungsweise technische Komponente, die Nachweise oder einzelne Attribute aus einer EUDI-Wallet anfordert, entgegennimmt und technisch prüft
Verifier-App (Checker-App)	Anwendung zur mobilen oder situativen Prüfung von Wallet-Nachweisen, etwa durch Scannen eines QR-Codes. Funktionsumfang und Weiterverarbeitung richten sich nach Anwendungsfall, Datenschutz und technischer Ausgestaltung.
Vertrauensinfrastruktur	Gesamtheit der Register, Zertifikate und Vertrauenslisten, über die Echtheit und Berechtigung von Wallets, Issuern und Relying Parties kryptografisch geprüft werden
Wallet-Adapter	technische Komponente zur standardbasierten direkten Anbindung von Online-Diensten und Fachverfahren an die EUDI-Wallet, insbesondere für Identifizierung und Authentifizierung sowie für die Ausstellung und Entgegennahme digitaler Nachweise
Zentraler Issuing-Dienst (ZID)	zentraler Ausstellungsdienst des Bundesverwaltungsamts, der registerbasierte Daten abruft, in ein walletfähiges Format transformiert, siegelt und als Nachweis an die EUDI-Wallet übermittelt