

Einführung der EUDI-Wallet in der Versiche-rungswirtschaft

Praxisleitfaden zur Einführung
der EUDI-Wallet in der Versicherungsbranche

bitkom

Inhalt

1 Einleitung 4

Ziel des Leitfadens 4

Zielgruppe 4

Berücksichtigte und nicht berücksichtigte Aspekte der EUDI-Infrastruktur 5

2 EUDI-Wallet in der Versicherungsindustrie 6

eIDAS 2.0 Verordnung als rechtliche Grundlage 6

Pflichten als »vertrauender Beteiligter« (Relying Party) 7

Grundfunktionen der EUDI, die in der Versicherungsindustrie genutzt werden können 8

Einordnung in bestehende Regulatorik in der Versicherungsindustrie (AMLR (GWG), EHDS (gematik)) 9

Kategorie 1: Klare Fälle der Akzeptanzpflicht – Zahlungsdiensterecht (§ 55 ZAG / Art. 85 PSR) 9

Kategorie 2: Gesetzliche und vertragliche Pflichten zur Multi-Faktor-Authentifizierung 9

Kategorie 3: EUDI als probate Alternative – keine Akzeptanzpflicht, aber regulatorischer Anreiz 10

3 Rollenmodell der EUDI und Konsequenz für Versicherer 13

Versicherer als Verifier / Relying Party 13

Technische Konsequenzen 14

Regulatorische Konsequenzen 15

Organisatorische Konsequenzen 15

Versicherer als Issuer 16

Vertrauens- und Governance-Anforderungen 17

Technische Anforderungen 17

Strategische Bedeutung 18

Versicherer als Ökosystempartner 18

Teilnahme an sektorübergreifenden Ökosystemen 18

Kooperation statt isolierter Lösungen 19

Veränderung der Kundeninteraktion 19

4 Typische Anwendungsfälle der EUDI-Wallet in der Versicherungsindustrie (inkl. notwendiger Voraussetzungen) 20

User Experience: Ohne Nutzen keine Akzeptanz 20

Spartenübergreifendes KYC (nutzbar nach AML-Vorgaben) 22

Ausgangslage und Zielbild 22

Ablauf 24

Übergabe der Daten des KFZ-Schein bei Vertragsabschluss 26

Orchestrierung Schadensmeldung in eigener Versicherungs-App mit integrierter EUDI-Wallet Funktion 30

Antrag in der Sparte Leben mit Gesundheitsfragen: Identifizierung mit PID und QES über die EUDI 34

5 Vorgehen für Strategie- und Roadmap-Entwicklung 39

Usecase Design (Pains & Gains, Service Design, Prototyping, Ziel Nutzerversprechen / Machbarkeit) 40

Roadmap Entwicklung und Implementierungsvorgehen 41

6 Zusammenfassung und Schlussbemerkungen 42

Erwartete Weiterentwicklung der EUDI 42

Grundsätzliche Handlungsempfehlungen für die Zukunft 43

Weiterführende Literatur 44

1 Einleitung

Ziel des Leitfadens

Die EUDI-Wallet, dessen staatliche Anwendung in Deutschland nun offiziell unter dem Namen d-you (»digital you«) firmiert, schafft einen neuen europäischen Rahmen für digitale Identitäten, Nachweise und Vertrauensdienste. Für Versicherungsunternehmen betrifft das nicht nur einzelne Identifizierungsstrecken. Je nach Prozess können sie künftig als Relying Party Nachweise prüfen, als Issuer selbst digitale Nachweise bereitstellen oder an branchenübergreifenden Ökosystemen teilnehmen. Damit entstehen sowohl regulatorische Anforderungen als auch Möglichkeiten, bestehende Kunden- und Serviceprozesse einfacher und medienbruchfreier zu gestalten.

Der Leitfaden soll Versicherern eine praxisnahe Orientierung geben, welche Rollen und Funktionen der EUDI-Wallet für die Branche relevant sind, welche regulatorischen Rahmenbedingungen zu berücksichtigen sind und wie sich konkrete Anwendungsfälle strukturieren lassen. Die beschriebenen Use Cases zeigen beispielhaft, wie Wallet-Funktionen in bestehende Prozesse eingebunden werden können. Im Mittelpunkt steht dabei nicht die Wallet als isolierte Technologie, sondern ihr Zusammenspiel mit bestehenden Systemen, Vertrauensdiensten und Fachprozessen.

Die Publikation versteht sich als Arbeits- und Orientierungshilfe. Sie ersetzt keine rechtliche oder technische Einzelfallprüfung, sondern soll eine gemeinsame Grundlage für die strategische Einordnung und die weitere Umsetzung in den Unternehmen schaffen.

Zielgruppe

Der Leitfaden richtet sich an Versicherungsunternehmen und an die Bereiche, die an der Gestaltung und Umsetzung digitaler Identitäts- und Nachweisprozesse beteiligt sind. Dazu zählen insbesondere Digital- und IT-Verantwortliche, Fachbereiche Operations, Vertrieb, Compliance, Datenschutz und Informationssicherheit sowie Produkt- und Prozessverantwortliche. Auch Vermittler, InsurTechs sowie Technologie- und Vertrauensdiensteanbieter können die dargestellten Rollenmodelle und Use Cases als Orientierung für gemeinsame Integrationsprojekte nutzen.

Der Leitfaden soll sowohl für die strategische Einordnung als auch für die konkrete Projektvorbereitung nutzbar sein. Er zeigt, welche Fragestellungen frühzeitig geklärt werden sollten, welche Abhängigkeiten zwischen Regulierung, Technik und Kundenerlebnis bestehen und an welchen Stellen eine unternehmens- oder branchenübergreifende Abstimmung erforderlich werden kann.

Berücksichtigte und nicht berücksichtigte Aspekte der EUDI-Infrastruktur

Betrachtet werden die für die Versicherungswirtschaft besonders relevanten Funktionen und Rollen der EUDI-Wallet. Dazu gehören die Nutzung als Relying Party beziehungsweise Verifier, die mögliche Rolle von Versicherern als Issuer digitaler Nachweise, die Einbindung von Identitäts- und Attributsnachweisen in Versicherungsprozesse sowie Fragen zu Authentifizierung, qualifizierter elektronischer Signatur, technischer Integration und User Experience. Die regulatorische Einordnung konzentriert sich auf diejenigen Vorgaben, die für die dargestellten Prozesse unmittelbar relevant sind.

Nicht Gegenstand des Leitfadens ist eine vollständige technische Beschreibung der EUDI-Infrastruktur oder sämtlicher Durchführungsrechtsakte und Standards. Ebenso ersetzt die Publikation weder eine rechtliche Bewertung des Einzelfalls noch eine konkrete Architektur- oder Produktauswahl. Weitergehende europäische Daten- und Wallet-Infrastrukturen werden nur dort aufgegriffen, wo sie für die strategische Einordnung der beschriebenen Anwendungsfälle erforderlich sind.

2 EUDI-Wallet in der Versicherungsindustrie

eIDAS 2.0 Verordnung als rechtliche Grundlage

Die Einführung der EUDI basiert auf der novellierten Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS 2.0), die nun als Verordnung (EU) 2024/1183 anzuwenden ist. Mit eIDAS 2.0 verfolgt die Europäische Kommission das Ziel, dass bis 2030 mindestens 80 % aller EU-Bürger eine digitale Identitätslösung wie die EUDI-Wallet nutzen. Die EUDI fungiert dabei als eine sichere, nutzergesteuerte App auf dem Smartphone, in der staatlich ausgestellte Personenidentifizierungsdaten, verifizierte digitale Nachweise und qualifizierte elektronische Signaturen gebündelt werden können. Sie soll medienbruchfrei und einheitlich in allen EU-Mitgliedstaaten funktionieren.

Um eine kritische Masse an Nutzern zu erreichen, sieht eIDAS 2.0 ein gestuftes System an Akzeptanzpflichten vor:

Stufe 1 – Öffentliche Hand: Jeder Mitgliedstaat ist gemäß Art. 5a Abs. 1 eIDAS-VO verpflichtet, bis zum 24. Dezember 2026 mindestens eine EUDI-Wallet bereitzustellen. Deutschland hat den Start für den 2. Januar 2027 angekündigt. Öffentliche Stellen müssen die EUDI für den Zugang zu ihren Online-Diensten akzeptieren (Art. 5f Abs. 1 eIDAS-VO).

Stufe 2 – Sehr große Online-Plattformen: Anbieter sehr großer Online-Plattformen (VLOPs) im Sinne des Digital Services Act sind ab Bereitstellung der ersten EUDI-Wallet gemäß Art. 5f Abs. 3 eIDAS-VO verpflichtet, die Wallet bei der Nutzerauthentifizierung für den Onlinezugang zu akzeptieren.

Stufe 3 – Dienstleistungssektor: Ab dem 24. Dezember 2027 wird die Akzeptanzpflicht gemäß Art. 5f Abs. 2 eIDAS-VO auf alle privaten Unternehmen ausgeweitet, die Dienstleistungen erbringen und entweder gesetzlich zur Durchführung einer Online-Identifizierung mit starker Nutzerauthentifizierung verpflichtet sind oder bei denen eine solche vertraglich vorgeschrieben ist. Ausgenommen sind Kleinst- und kleine Unternehmen mit weniger als 50 Beschäftigten und weniger als 10 Mio. Euro Jahresumsatz oder Jahresbilanzsumme. Betroffene Sektoren sind unter anderem Verkehr, Energie, Bankenwesen, Finanzdienstleistungen, soziale Sicherheit, Gesundheit, Trinkwasser, Postdienste, digitale Infrastrukturen, Bildung und Telekommunikation.

Darüber hinaus sieht das im Digitale-Identitäten-Gesetz (DIdG) enthaltene Gesetz über die Europäische Brieftasche für die Digitale Identität (EBDIG) in § 17 vor, dass die EUDI-Wallet als zusätzliche Funktion die Einbindung und Verwendung bestehender Zahlungsmittel des Nutzers umfassen darf – ein Schritt zur universellen App für

Identität und Zahlungsverkehr.1 § 15 Absatz 1 des EBDIG-Entwurfs erweitert die Artikel 5f Absatz 1 bis 3 der eIDAS-VO auf Vorfälle ohne Grenzüberschreitung. § 15 Abs. 2 des EBDIG-Entwurfs regelt, dass die EUDI immer dann zu akzeptieren ist, wenn eine Vorschrift den Nachweis der Identität mittels der eID-Funktion des Personalausweises (§ 18 Personalausweisgesetz) vorsieht. Für die Zukunft könnte auch die Experimentierklausel in § 23 (dort Nr. 11) relevant werden. Per Rechtsverordnung sollen besondere Maßgaben zur Akzeptanz und Verwendung der Europäischen Brieftasche für die Digitale Identität für einzelne Wirtschaftsbereiche, einschließlich der Möglichkeit, Verpflichtungen zur Art und Weise der Akzeptanz von Europäischen Brieftaschen für die Digitale Identität, auf Grundlage einer Abwägung der Folgen unter Berücksichtigung der wirtschaftlichen Auswirkungen, festgelegt werden können.

Pflichten als »vertrauender Beteiligter« (Relying Party)

Soweit ein Unternehmen – ob kraft gesetzlicher Verpflichtung oder freiwillig – die EUDI-Wallet akzeptiert, agiert es als »vertrauender Beteiligter« (Relying Party). Aus der eIDAS-Verordnung und den nationalen Durchführungsgesetzen ergeben sich für vertrauende Beteiligte mehrere zentrale Pflichten:

- **Registrierungspflicht:** Vor der ersten Wallet-Interaktion müssen sich Unternehmen gemäß Art. 5b Abs. 1 eIDAS-VO registrieren (in Deutschland beim Bundesverwaltungsamt). Die angeforderten Daten müssen spezifiziert und begründet werden (Art. 5b Abs. 2 lit. c eIDAS-VO).
- **Abfragebeschränkung:** Es dürfen nur die in der Registrierung benannten Daten abgefragt werden (Art. 5b Abs. 3 eIDAS-VO).
- **Gegenidentifizierung:** Institute müssen sich gegenüber dem Wallet-Nutzer identifizieren (Art. 5b Abs. 8 eIDAS-VO), sodass transparent wird, wer Daten anfordert.
- **Akzeptanz von Pseudonymen:** Nutzergenerierte Pseudonyme dürfen grundsätzlich nicht verweigert werden, es sei denn, gesetzliche Identifizierungspflichten stehen entgegen.
- **Besonderheiten bei Dienstleistern:** Vermittler oder Dienstleister, die im Namen vertrauender Beteiligter handeln, werden ebenfalls als vertrauende Beteiligte eingeordnet und dürfen keine Daten über den Inhalt der Transaktionen speichern (Art. 5b Abs. 10 eIDAS-VO).

[1] Das DidG wurde am 15. Oktober 2026 vom Bundestag beschlossen.

Grundfunktionen der EUDI, die in der Versicherungsindustrie genutzt werden können

Die EUDI bündelt mehrere Funktionen, die in Versicherungsprozessen einzeln oder kombiniert genutzt werden können. Im Kern geht es darum, digitale Identitäten und Nachweise verlässlich bereitzustellen. Für Versicherer sind insbesondere folgende Funktionen relevant:

- Identifizierung und Authentifizierung: Personenidentifizierungsdaten (PID) können genutzt werden, um die Identität einer Person zu prüfen und sie in digitalen Prozessen sicher zu authentifizieren.
- Digitale Nachweise speichern und vorlegen: Neben den PID können weitere elektronische Attributsbescheinigungen in der Wallet hinterlegt und gegenüber einem Versicherer oder einer anderen Stelle vorgelegt werden.
- Selektive Datenfreigabe: Nutzerinnen und Nutzer können die für einen konkreten Vorgang benötigten Attribute freigeben, ohne grundsätzlich den vollständigen Nachweis offenzulegen.
- Prüfung von Herkunft und Gültigkeit: Relying Parties können prüfen, von wem ein Nachweis ausgestellt wurde, ob er gültig ist und ob sich sein Status zwischenzeitlich geändert hat.
- Ausstellung eigener Nachweise: Versicherer können perspektivisch selbst als Issuer auftreten und beispielsweise Versicherungs- oder Vertragsnachweise für die Nutzung bei Dritten bereitstellen.
- Elektronische Signaturen: Die EUDI-Wallet kann in Verbindung mit qualifizierten Vertrauensdiensteanbietern auch für qualifizierte elektronische Signaturen genutzt werden, soweit die jeweilige Ausgestaltung und der konkrete Prozess dies vorsehen.

Die Funktionen greifen über das Rollenmodell von Holder, Issuer und Relying Party ineinander. Der Holder – also die Nutzerin oder der Nutzer der Wallet – erhält digitale Identitätsdaten und Nachweise von einem Issuer, speichert sie in der Wallet und kann sie gegenüber einer Relying Party vorlegen. Der Issuer stellt die jeweiligen Nachweise aus und bestätigt deren Authentizität. Die Relying Party nutzt diese Informationen, um einen bestimmten Sachverhalt zu überprüfen und darauf aufbauend eine Dienstleistung zu erbringen.Welche Rollen davon im Einzelfall relevant sind, hängt daher weniger von der Wallet als solcher als vom jeweiligen Versicherungsprozess und den dafür benötigten Nachweisen ab.

Einordnung in bestehende Regulatorik in der Versicherungsindustrie (AMLR (GWG), EHDS (gematik))

Für Versicherungsunternehmen ist die Frage, ob und in welchem Umfang eine Pflicht zur Akzeptanz der EUDI besteht, differenziert zu betrachten. Anders als bei Kredit- und Zahlungsinstituten, bei denen sich eine Akzeptanzpflicht primär aus dem Zahlungsdiensterecht ergibt, ist die regulatorische Ausgangslage in der Versicherungswirtschaft vielschichtiger.

Je nach regulatorischem Kontext lassen sich drei Kategorien unterscheiden:

Kategorie 1: Klare Fälle der Akzeptanzpflicht – Zahlungsdiensterecht (§ 55 ZAG / Art. 85 PSR)

Soweit Versicherungsunternehmen oder mit ihnen verbundene Zahlungsdienstleister dem Anwendungsbereich des Zahlungsdiensterechts unterliegen, gelten die Pflichten zur starken Kundenauthentifizierung (SKA). Die Zahlungsdiensterichtlinie (PSD2) ist derzeit in § 55 Abs. 1 ZAG umgesetzt und soll künftig in Art. 85 der geplanten Zahlungsdiensteverordnung (PSR) geregelt werden. Sie schreibt eine SKA für den Online-Zugriff auf Konten, die Auslösung elektronischer Zahlungen sowie bei risikobehafteten Aktivitäten vor. Nach Ansicht der Kommission führt dies ab dem 24. Dezember 2027 unmittelbar zu einer Akzeptanzpflicht gemäß Art. 5f Abs. 2 eIDAS-VO.

Relevanz für Versicherer: Dieser Tatbestand betrifft Versicherungsunternehmen in erster Linie dort, wo sie oder mit ihnen verbundene Unternehmen als Zahlungsdienstleister agieren oder Zahlungsauslösungen über eigene digitale Plattformen veranlassen. Für die Mehrzahl der Versicherungsprozesse, die keine Zahlungsdienste im Sinne des ZAG darstellen, besteht keine direkte Akzeptanzpflicht über diesen Weg.

Kategorie 2: Gesetzliche und vertragliche Pflichten zur Multi-Faktor-Authentifizierung

Neben den klaren Fällen des Zahlungsdiensterechts existieren weitere gesetzliche und vertragliche Verpflichtungen zur Multi-Faktor-Authentifizierung (MFA), bei denen zumindest diskutiert wird, ob sie eine Akzeptanzpflicht nach Art. 5f Abs. 2 eIDAS-VO auslösen:

NIS-2-Richtlinie / BSIG: Die im BSIG umgesetzte NIS-2-Richtlinie verpflichtet »besonders wichtige und wichtige Einrichtungen« zur Umsetzung geeigneter Cybersicherheitsmaßnahmen (§ 30 Abs. 1 BSIG). Gemäß § 30 Abs. 2 Nr. 10 BSIG kommt die Multi-Faktor-Authentifizierung als mögliche Maßnahme in Betracht. Versicherungsunternehmen, die als »wichtige Einrichtungen« im Sinne der NIS-2-Richtlinie eingestuft werden, unterliegen dieser Pflicht.

Allerdings wird diskutiert, ob die Anforderungen an eine MFA unter NIS-2 deckungsgleich mit den hohen Anforderungen an die »starke Nutzerauthentifizierung«

im Sinne der eIDAS-VO sind. Die eIDAS-VO spricht in Art. 5f Abs. 2 ausdrücklich von einer Pflicht zur »Online-Identifizierung mit starker Nutzerauthentifizierung«. Nicht jede regulatorisch geforderte MFA erfüllt zwingend diesen Maßstab. Die EUDI-Wallet stellt technisch zwar eine Lösung dar, um MFA-Anforderungen zu erfüllen, ob damit aber auch eine gesetzliche Akzeptanzpflicht einhergeht, ist im Einzelfall zu prüfen.

DORA (Digital Operational Resilience Act): Der DORA-Rahmen, der auch Versicherungsunternehmen erfasst, enthält ebenfalls Anforderungen an die IT-Sicherheit und Authentifizierung. Auch hier stellt sich die Frage, ob die darin geforderten Authentifizierungsmechanismen als »starke Nutzerauthentifizierung« im Sinne von Art. 5f Abs. 2 eIDAS-VO zu qualifizieren sind.

Vertragliche MFA-Pflichten: Auch vertragliche Verpflichtungen zur Nutzung von MFA – etwa in Cybersicherheitsvereinbarungen mit Geschäftspartnern oder regulatorisch induzierten IT-Sicherheitsstandards – könnten potenziell eine Akzeptanzpflicht begründen, sofern sie als »vertraglich vorgeschriebene Online-Identifizierung mit starker Nutzerauthentifizierung« einzuordnen sind.

Bei all den genannten Vorschriften hilft der nationale § 15 Abs. 2 des EBDIG-Entwurfs nicht zur Klärung, da es nicht um Parallelen zur Personalausweisfunktion geht.

Fazit zu Kategorie 2: In dieser Kategorie besteht keine rechtssichere Klarheit darüber, ob die jeweiligen MFA-Anforderungen die Schwelle des Art. 5f Abs. 2 eIDAS-VO erreichen. Versicherungsunternehmen sollten im Rahmen einer individuellen Impact-Analyse prüfen, welche ihrer Kundenschnittstellen mit MFA-Bezug potenziell von einer Akzeptanzpflicht erfasst sind.

Kategorie 3: EUDI als probate Alternative – keine Akzeptanzpflicht, aber regulatorischer Anreiz

In einer dritten Kategorie gibt es Anwendungsfälle, in denen zwar keine Akzeptanzpflicht für die EUDI-Wallet besteht, die Wallet aber als regulatorisch sichere und praktische Alternative zu bisherigen Identifizierungsverfahren dient:

Geldwäscheprävention (AMLR / GWG): Art. 22 Abs. 6 lit. b der EU-Geldwäscheverordnung (AMLR), die ab dem 10. Juli 2027 gilt, verpflichtet »Verpflichtete« dazu, Fernidentitätsprüfungen anhand von eIDAS-konformen elektronischen Identifizierungsmitteln mit einem Sicherheitsniveau »substanziell« oder »hoch« oder anhand einschlägiger qualifizierter Vertrauensdienste durchzuführen. Die Verordnung begründet damit zwar keine eigenständige Pflicht zur ausschließlichen Nutzung der EUDI-Wallet. Diskutieren könnte man aber, ob sich eine Akzeptanzpflicht aus den Art. 22 Abs. 6 der AMLR ergänzenden sog. »RTS« zu den Kundensorgfaltspflichten ergibt. In Art. 4 Ziffer 6 der RTS heißt es, dass elektronische Identifizierungsmittel (...) zulässig sind (englisch: shall be permitted), um die Identität einer Person zu überprüfen, und zwar auch im reinen Face-to-Face-Geschäft. »Shall be permitted« könnte man als Rechtspflicht verstehen, die eine Akzeptanzpflicht im Rahmen der AMLR begründet. Die RTS befanden sich zum Zeitpunkt der Prüfung allerdings im Entwurfsstadium und können sich daher noch ändern. Eine solche Akzeptanzpflicht würde andere zulässige Verfahren nach Art. 22 Abs. 6 AMLR nicht ausschließen.

In jedem Fall ist die d-you mit ihrem Sicherheitsniveau »hoch« ein regulatorisch sicheres Mittel für ein rechtskonformes digitales Onboarding.

Für Versicherungsunternehmen ist dies insbesondere im Kontext der geldwäscherechtlichen Sorgfaltspflichten nach dem GWG relevant. Versicherer in bestimmten Sparten – insbesondere in der Lebensversicherung und bei fondsgebundenen Produkten – unterliegen den geldwäscherechtlichen Identifizierungspflichten. Die EUDI-Wallet kann hier das digitale KYC-Onboarding erheblich vereinfachen und rechtssicher gestalten, ohne dass eine Akzeptanzpflicht im engeren Sinne besteht.

Elektronische Gesundheitskarte und § 291 Abs. 8 SGB V (EHDS / gematik): Im Kontext des Europäischen Gesundheitsdatenraums (EHDS) und der bestehenden Telematikinfrastruktur der gematik eröffnet sich für die Versicherungswirtschaft – insbesondere für Krankenversicherer – ein weiteres relevantes Einsatzfeld. § 291 Abs. 8 SGB V ermöglicht die Nutzung der elektronischen Gesundheitskarte und perspektivisch digitaler Identitätsnachweise für den Zugang zu Gesundheitsdiensten. Die EUDI-Wallet könnte hier als interoperables Medium dienen, um Versichertenstatus, Vertretungsberechtigungen oder Leistungsnachweise digital zu verifizieren. Während eine Akzeptanzpflicht im engeren Sinne derzeit nicht besteht, kann die EUDI ein technisch probates Mittel sein, um den Anforderungen an eine sichere digitale Authentifizierung im Gesundheitsbereich gerecht zu werden und die Anbindung an die europäische Gesundheitsdateninfrastruktur vorzubereiten.

Zusammenfassende Übersicht

Kategorie	Regulatorischer Auslöser	Akzeptanzpflicht	Relevanz für Versicherer
Klare Akzeptanz-pflicht	§ 55 ZAG / Art. 85 PSR (SKA im Zahlungs-verkehr)	Ja, ab 24. Dezember 2027	Begrenzt auf Versicherer mit Zahlungsdienste-Bezug
Akzeptanz-pflicht denkbar	NIS-2 / BSIG (MFA), DORA, vertragliche MFA	Unklar – nicht eindeutig, ob MFA-Anforderungen die Schwelle der »starken Nutzerauthentifizierung« erreichen	Relevant für alle Versicherer mit digitalen Kundenschnittstellen
Probate Alternative	AMLR / GWG (Fern-Identifizierung), § 291 Abs. 8 SGB V (EHDS / gematik), FIDA	Nein, aber regulatorisch sicheres und empfohlenes Mittel	Hohe Relevanz für Lebensversicherer (KYC), Krankenversicherer (EHDS); Open-Finance-Szenarien (soweit relevant)

Unabhängig von der Frage einer formellen Akzeptanzpflicht sprechen sowohl operative als auch strategische Gründe dafür, die Integration der EUDI-Wallet in die Versicherungsprozesse frühzeitig zu planen. Die Wallet bietet die Chance, medienbruchfreie, sichere und europaweit interoperable Identitäts- und Nachweisprozesse zu etablieren – ein Vorteil, der für die Versicherungswirtschaft mit ihren zahlreichen Kundenschnittstellen und regulatorischen Identifizierungspflichten erheblich ist.

3 Rollenmodell der EUDI und Konsequenz für Versicherer

Die EUDI-Wallet etabliert ein europaweit interoperables Vertrauensökosystem für digitale Identitäten, Nachweise und elektronische Vertrauensdienste. Für Versicherungsunternehmen ergeben sich daraus unterschiedliche Rollen mit jeweils eigenen regulatorischen, technischen und organisatorischen Anforderungen.

Dabei ist die EUDI-Wallet nicht isoliert zu betrachten. Sie baut auf der bestehenden eIDAS-Verordnung und den bereits etablierten europäischen Vertrauensdiensten auf. Versicherer nutzen heute schon digitale Identitäts- und Vertrauensmechanismen wie die Online-Ausweisfunktion des deutschen Personalausweises, qualifizierte elektronische Signaturen (QES), elektronische Siegel oder signierte Dokumente. Mit eIDAS 2.0 und der EUDI werden diese bestehenden Mechanismen um interoperable, walletfähige Nachweise und neue Interaktionsmodelle erweitert.

Für Versicherer entstehen daraus drei wesentliche Rollen:

- Versicherer als Verifier beziehungsweise Relying Party,
- Versicherer als Aussteller digitaler Nachweise (Issuer),
- Versicherer als Teilnehmer digitaler Ökosysteme.

Gleichzeitig betrifft die Entwicklung nicht nur einzelne digitale Abschlussstrecken, sondern die gesamte Verarbeitung vertrauenswürdiger digitaler Daten und Dokumente innerhalb der Versicherungsunternehmen.

Für viele Versicherer wird der Einstieg zunächst über die Identifizierung ihrer Versicherten bzw. Neukunden im Kontext ihres »KYC-Prozesses« erfolgen. Die Chance der Versicherer besteht darin,nicht zu warten, bis Versicherungsnehmer weitere digitale Nachweise in den Prozess einbringen, sondern selbst das Ökosystem mitzugestalten und für sich zu nutzen, indem sie selbst digitale Nachweise bereitstellen und sich als aktive Teilnehmer eines europäischen Vertrauensökosystems positionieren.

Versicherer als Verifier / Relying Party

Die kurzfristig naheliegendste Rolle für Versicherungsunternehmen ist die Rolle als Identifizierer im Sinne eines Verifiers bzw. einer Relying Party. Hauptanwendungsfälle werden die Identifizierung und Authentifizierung mit der Wallet sein, so wie dies heute bereits mit dem Personalausweis möglich ist.

Die Annahme beruht darauf, dass die Versicherungsunternehmen die Entwicklung des Ökosystems zunächst passiv begleiten. Diese Position sollte gut bedacht sein, da sich die Frage stellt, wer dem Versicherten welche für die Versicherungsunternehmen relevanten Nachweise digital bereitstellen müsste.

In dieser Rolle fordert der Versicherer bestimmte Daten oder Nachweise aus der Wallet an, prüft deren Echtheit, Gültigkeit und Herkunft und nutzt sie anschließend im Fachprozess.

Typische Anwendungsfälle:

- Identitätsprüfung beim digitalen Vertragsabschluss,
- Übernahme persönlicher Stammdaten,
- Adressvalidierung,
- Führerscheinprüfung bei Kfz-Prozessen,
- Prüfung von Vertretungsberechtigungen,
- KYC-/AML-relevante Identifizierung,
- Re-KYC im Bestand,
- Authentifizierung im Serviceprozess,
- Altersnachweise für bestimmte Produkte oder Leistungen,
- B2B-Onboarding und Verifikation von Unternehmensdaten im Firmenkundengeschäft.

Geldwäscherechtliche Anforderungen betreffen dabei nicht pauschal alle Versicherungsprodukte. Relevanz besteht insbesondere bei Lebensversicherungen sowie bestimmten kapitalbildenden oder anlagebezogenen Versicherungsprodukten. In diesen Bereichen kann die EUDI-Wallet perspektivisch zur Standardisierung regulatorisch erforderlicher Identifizierungsprozesse beitragen.

Für Versicherer ergeben sich daraus mehrere Konsequenzen.

Technische Konsequenzen

Versicherer benötigen Schnittstellen zur Wallet-Infrastruktur sowie Fähigkeiten zur Verarbeitung und Validierung digitaler Nachweise und Vertrauensdienste.

Wichtige technische Bausteine sind insbesondere:

- Unterstützung relevanter EUDI-Protokolle und eIDAS-Standards,
- Verarbeitung von Verifiable Credentials,
- Integration in digitale Abschluss- und Serviceprozesse,
- Anbindung an IAM-, und CRM- und Bestandssysteme,
- Consent-Management und Nachweisprotokollierung,
- Signatur-, Siegel- und Statusvalidierung,
- Nachweisfähigkeit regulatorischer Prozesse.

- Die technische Validierung beschränkt sich dabei nicht auf Wallet-basierte Credentials. Versicherer müssen künftig unterschiedlichste vertrauenswürdige digitale Nachweise verarbeiten können.

  Hierzu zählen unter anderem:

  - Verifiable Credentials aus der EUDI-Wallet,
  - qualifiziert elektronisch signierte Dokumente,
  - elektronisch gesiegelte Dokumente,
  - signierte PDF-Dokumente,
  - Identitätsnachweise aus bestehenden eID-Verfahren,
  - strukturierte Nachweise aus europäischen Vertrauensdiensten.

Damit gewinnen sogenannte Validation Services an Bedeutung. Diese ermöglichen die technische Prüfung elektronischer Signaturen, Siegel, Zertifikate, Vertrauensketten und Wallet-basierter Credentials innerhalb einer gemeinsamen Vertrauensinfrastruktur.

Regulatorische Konsequenzen

Die Nutzung digitaler Nachweise berührt unterschiedliche regulatorische Anforderungen, insbesondere:

- eIDAS 1.0 und eIDAS 2.0,
- AMLR bzw. Geldwäschegesetz (GWG),
- Datenschutzanforderungen nach DSGVO,
- Anforderungen an Einwilligung und Zweckbindung,
- Dokumentations- und Nachweispflichten,
- Anforderungen an sichere Authentifizierung.

Mit eIDAS 2.0 entsteht perspektivisch zudem ein europaweit harmonisierter Rahmen für vertrauenswürdige digitale Identitäten und Nachweise. Versicherer müssen dabei sowohl bestehende Vertrauensdienste als auch zukünftige Wallet-Mechanismen berücksichtigen.

Organisatorische Konsequenzen

Die Einführung walletbasierter Prozesse betrifft typischerweise mehrere Unternehmensbereiche gleichzeitig:

- Vertrieb,
- Betrieb,
- Compliance,

- IT,
- Informationssicherheit,
- Kundenservice,
- Dokumentenmanagement,
- Output-Management.

Die Wallet sollte daher nicht als isoliertes Identitätsprojekt verstanden werden, sondern als Bestandteil einer umfassenderen Strategie für digitale Vertrauensdienste, digitale Nachweise und digitale Kundeninteraktionen.

Versicherer als Issuer

Versicherer können perspektivisch auch selbst digitale Nachweise ausstellen. Diese Rolle ist strategisch relevant, da Versicherungsunternehmen dadurch nicht nur Daten anderer Stellen nutzen, sondern selbst als vertrauenswürdiger Aussteller digitaler Nachweise innerhalb des europäischen Vertrauensökosystems auftreten.

Die Ausstellung digitaler Versicherungsnachweise ermöglicht neue digitale Interaktionen zwischen Versicherern, Kundinnen und Kunden sowie Drittparteien. Versicherungsinformationen können dadurch standardisiert, maschinenlesbar und europaweit interoperabel bereitgestellt werden.

Mögliche Nachweis, die Versicherer ausstellen könnten:

Möglicher Nachweis	Potenzieller Nutzen
Versicherungsdeckungsnachweis	**Nachweis gegenüber Vermietern, Plattformen, Behörden oder Partnern**
Kfz-Versicherungsbestätigung	**Mobilitäts- und Zulassungsprozesse**
Reiseversicherungsnachweis	**Nachweis bei Reisen, Visa, Plattformen**
Krankenversicherungsstatus	**Gesundheits- und Leistungsprozesse**
Berufshaftpflichtnachweis	**Nachweis gegenüber Auftraggebern oder Plattformen**
Schadenfreiheitsnachweis	**Wechsel- und Kfz-Prozesse**
Makler- oder Vertretungsvollmacht	**Vermittler- und Serviceprozesse**
Leistungs- oder Vertragsstatus	**Nachweis gegenüber Dritten**

Die Rolle als Issuer umfasst dabei nicht nur Wallet-basierte Credentials. Versicherer stellen bereits heute unterschiedlichste digitale Dokumente und Nachweise bereit, beispielsweise PDF-Dokumente mit elektronischen Signaturen oder Siegeln. Künftig

wird die Herausforderung darin bestehen, unterschiedliche Ausgabeformate innerhalb einer gemeinsamen Vertrauensarchitektur bereitzustellen.

Für Versicherer entstehen daraus zusätzliche Anforderungen.

Vertrauens- und Governance-Anforderungen

Digitale Nachweise benötigen klare fachliche und technische Regelwerke.

Hierzu gehören insbesondere:

- standardisierte Datenmodelle,
- Governance-Regeln für Ausstellung und Widerruf,
- Haftungs- und Vertrauensmodelle,
- Lebenszyklusmanagement von Nachweisen,
- Interoperabilität mit europäischen Standards,
- Definition zulässiger Nutzungskontexte.
- Hierfür werden sogenannte Rulebooks benötigt, die festlegen, unter welchen Bedingungen Nachweise erstellt, genutzt, geprüft und akzeptiert werden.

Technische Anforderungen

Versicherer benötigen Fähigkeiten zur Ausstellung, Verwaltung und gegebenenfalls zum Widerruf digitaler Nachweise.

Dies umfasst unter anderem:

- Credential Issuance,
- Signatur- und Siegelprozesse,
- Schlüsselmanagement,
- Trust-Registry-Anbindung,
- Revocation- und Statusmechanismen,
- walletfähige Ausgabeformate,
- Integration in Dokumenten- und Output-Management-Systeme.

Das bestehende Output-Management vieler Versicherer muss daher perspektivisch erweitert werden. Dokumente und Nachweise sollten künftig nicht nur analog und als klassische PDF-Dokumente bereitgestellt werden können, sondern gegebenenfalls zusätzlich folgende Eigenschaften aufweisen:

- elektronisch signierbar,
- elektronisch siegelbar,
- strukturiert maschinenlesbar,

- walletfähig,
- interoperabel nutzbar.

Strategische Bedeutung

Die Rolle als Issuer eröffnet Versicherern neue Möglichkeiten zur Positionierung innerhalb digitaler Ökosysteme.

Versicherungsnachweise könnten künftig Bestandteil zahlreicher digitaler Prozesse werden, beispielsweise:

- Mobilitätsplattformen,
- Plattformökonomie,
- Sharing-Modelle,
- digitale Gesundheitsservices,
- grenzüberschreitende Dienstleistungen,
- digitale Behördenprozesse.

Dadurch kann sich die Rolle von Versicherern langfristig verändern — vom reinen Produktanbieter hin zu einem aktiven Vertrauensdienstleister innerhalb digitaler Wertschöpfungsnetzwerke.

Versicherer als Ökosystempartner

Die EUDI-Wallet entfaltet ihr Potenzial nicht nur in einzelnen Abschlussstrecken, sondern in Ökosystemen. Die Wallet ist Teil eines interoperablen Insurance-Ökosystems, in dem Endkunden, Versicherer, Partner, Werkstätten, Makler und Agenten miteinander interagieren.

Beispiele:

- Werkstätten senden verifizierte Schadensdokumente.
- Arbeitgeber übermitteln digitale Gehalts- oder Beschäftigungsnachweise.
- Makler greifen auf verifizierte Kundendaten oder Vollmachten zu.
- Gesundheitsakteure prüfen Versichertenstatus oder Vertretungsberechtigungen.
- Versicherer stellen Nachweise bereit, die Kundinnen und Kunden bei Dritten nutzen.

Teilnahme an sektorübergreifenden Ökosystemen

Die EUDI-Wallet wird nicht ausschließlich im Versicherungsumfeld eingesetzt. Relevante Entwicklungen entstehen parallel unter anderem in den Bereichen:

- Finanzindustrie,
- Gesundheitswesen,

- Mobilität,
- öffentliche Verwaltung,
- Plattformökonomie.

Versicherer sollten daher frühzeitig prüfen, in welchen digitalen Ökosystemen sie künftig eine aktive Rolle einnehmen wollen.

Kooperation statt isolierter Lösungen

- Der Nutzen der Wallet steigt mit der Interoperabilität zwischen Marktteilnehmern. Proprietäre Insellösungen werden langfristig nur begrenzt tragfähig sein.
- Erfolgsentscheidend sind daher:
- gemeinsame Standards,
- interoperable Datenmodelle,
- abgestimmte Governance,
- sektorübergreifende Zusammenarbeit,
- europäische Anschlussfähigkeit.
- Verbände, Standardisierungsgremien und europäische Pilotprojekte spielen hierbei eine wichtige Rolle.

Veränderung der Kundeninteraktion

Mit der EUDI-Wallet verschiebt sich die Kontrolle über Daten stärker auf die Seite der Nutzerinnen und Nutzer. Versicherer erhalten Daten nicht mehr dauerhaft zentral, sondern kontextbezogen und zustimmungsbasiert.

Dies verändert langfristig:

- Datenflüsse,
- Einwilligungsprozesse,
- Kundeninteraktionen,
- digitale Servicearchitekturen,
- Rollenverständnisse im Vertrieb und Service.

Die EUDI-Wallet ist damit nicht nur ein neues Identitätsinstrument, sondern Teil einer umfassenderen europäischen Vertrauensinfrastruktur. Versicherer sollten daher bestehende Prozesse für digitale Identitäten, Signaturen, Nachweise, Dokumente und Vertrauensdienste gemeinsam betrachten und strategisch weiterentwickeln.

4 Typische Anwendungsfälle der EUDI-Wallet in der Versicherungsindustrie (inkl. notwendiger Voraussetzungen)

User Experience: Ohne Nutzen keine Akzeptanz

Die EUDI wird nur erfolgreich, wenn Bürgerinnen und Bürger sie nutzen wollen. Das tun sie, wenn sie einen Vorteil erwarten und die Bedienung einfach ist. Sicherheit und Regelkonformität setzen die Nutzer voraus. Fehlt der Vorteil, bleiben Kunden bei gewohnten Verfahren.

Versicherer gestalten dabei nur einen Teil des Nutzererlebnisses. Die Wallet ist eine generische App, die der Wallet-Anbieter verantwortet. Einwilligungsdialog, PIN-Eingabe und Darstellung der Anfrage werden von ihr vorgegeben. Der Versicherer gestaltet, was vor dem Wechsel in die Wallet geschieht, welche Daten er anfragt und wie der Prozess danach weitergeht.

Rahmenbedingungen

Die erste Hürde liegt vor der Wallet. Für die Ausweisfunktion benötigen Nutzer einen Personalausweis mit aktivierter Online-Ausweisfunktion, die zugehörige PIN und ein NFC-fähiges Smartphone. Viele Bürgerinnen und Bürger erfüllen diese Voraussetzungen derzeit nicht, häufig weil ihnen die PIN fehlt. Zudem ist die EUDI-Wallet in der Bevölkerung noch wenig bekannt. Sollte sich daran nichts ändern, wird die Wallet in den ersten Jahren daher nur ein Teil der Kunden nutzen können und wollen. Die EUDI-Wallet wird in Österreich durch die ID-Austria-App unterstützt. Diese App ermöglicht es Nutzern bereits, digitale Ausweise, Führerscheine und andere Identitätsdokumente sicher zu speichern und zu verwalten, und gehört damit in der Breite der Bevölkerung zu den bevorzugten Anwendungen.

Stellhebel des Versicherers

Den Wechsel zwischen Anwendung und Wallet gestalten. Der Kunde verfolgt ein Ziel: einen Vertrag abschließen, einen Schaden melden. Die Identifizierung ist für ihn nur ein Zwischenschritt. Mit dem Wechsel in die Wallet-App verlässt er die Anwendung. Besonders auf dem Smartphone verliert er dabei den optischen Bezug zum eigentlichen Anwendungsfall, denn die Wallet überdeckt ihn vollständig. Versicherer

sollten den Wechsel vorher ankündigen und den Zweck erklären, den Bearbeitungsstand erhalten und den Rücksprung zuverlässig gestalten. Nach der Rückkehr sollte ein sichtbares Ergebnis stehen, etwa ein vorausgefülltes Formular. Beim Wechsel vom Desktop auf das Smartphone per QR-Code bleibt der Anwendungsfall zwar sichtbar, dafür entsteht ein Bruch zwischen zwei Geräten.

Nur anfragen, was nötig ist. Jede Datenanfrage erscheint im Einwilligungsdialog der Wallet. Je mehr Angaben ein Versicherer anfordert, desto eher zweifelt der Kunde. Datenminimierung schafft damit Vertrauen.

Erkennbar auftreten. Der Kunde muss im Einwilligungsdialog erkennen, wer anfragt. Der registrierte Name sollte der Marke entsprechen, die er kennt, nicht einer ihm unbekannten Konzerngesellschaft. Das erschwert zudem Phishing.

Kunden informieren. Für viele Kunden wird der Versicherer der erste Berührungspunkt mit der Wallet sein. Wirksam ist Information zu einem konkreten eigenen Angebot. Sie gehört dorthin, wo der Kunde gerade handelt: ins Kundenportal, in die Abschlussstrecke, ins Beratungsgespräch. Sinnvoll ist auch der Hinweis auf die Voraussetzungen, insbesondere die Ausweis-PIN. Vermittler können hier eine wichtige Rolle übernehmen.

Fehlerfälle und Alternativen vorsehen. Typische Fehlerfälle sind eine vergessene PIN, ein abgelaufener Ausweis, eine Wallet, die nach dem Handywechsel noch nicht eingerichtet ist, ein fehlender Nachweis oder eine abgelehnte Freigabe. Jeder dieser Fälle braucht einen verständlichen Hinweis und einen Weg zurück in den Prozess. Für Kunden ohne nutzbare Wallet bleiben alternative Identifizierungswege unverzichtbar. Welches Verfahren genutzt wird, sollte die Kundin oder der Kunde selbst entscheiden können.

Alle Kundengruppen und das Handeln für Dritte berücksichtigen. Versicherer dürfen ältere Menschen, Kunden ohne geeignetes Smartphone und Menschen mit Einschränkungen nicht ausschließen. Zudem weist die Wallet nach, wer jemand ist, nicht aber, für wen er handeln darf. Betreuer, Bevollmächtigte, Makler und Vertreter von Firmenkunden benötigen ergänzende Prozesse, solange Vollmachten nicht als digitale Nachweise verfügbar sind.

Ob diese Maßnahmen wirken, lässt sich nur mit Nutzern prüfen und messen, etwa an der Abbruchquote beim Wechsel in die Wallet. Das in Kapitel 5 beschriebene Vorgehen mit Pains & Gains und Prototyping bietet dafür den Rahmen.

Spartenübergreifendes KYC (nutzbar nach AML-Vorgaben)

Rolle des Versicherers	Verifier / Relying Party
Sparte und Prozessphase	Verpflichtet im Leben-, Unfall-mit-Prämienrückgewähr-, Kapitalisierungs- und Darlehensgeschäft sowie für mitwirkende Vermittler; Antrag, Bestand und Leistungsfall
Wallet-Funktion	Nachweis prüfen; qualifizierte elektronische Signatur nur bei Schriftformerfordernis
Zeithorizont	Kurzfristig: EUDI Wallet für Anfang 2027 angekündigt (DIdG), AML-Verordnung ab 10. Juli 2027, Akzeptanzpflicht für private Stellen ab Ende 2027

Ausgangslage und Zielbild

Versicherer identifizieren an vier Stellen des Vertragslebens: beim Antrag den Versicherungsnehmer und den wirtschaftlich Berechtigten, im Bestand turnusmäßig zur Aktualisierung und im Leistungsfall den abweichenden Bezugsberechtigten, spätestens zur Auszahlung. In der Lebensversicherung liegen dazwischen Jahrzehnte. Hinzu kommt, dass der Vertrieb weit überwiegend über Vermittler und Makler läuft, die selbst Verpflichtete sind – die Identifizierung findet in einer Strecke statt, die dem Versicherer nicht gehört. Heute kommen dafür unterschiedliche Verfahren zum Einsatz, etwa videogestützte Identifizierung mittels menschlicher Agenten, die Online-Ausweisfunktion des Personalausweises oder die Identifizierung vor Ort, die in die jeweilige Antragsstrecke eingebunden werden. Jedes dieser Verfahren erfüllt grundsätzlich denselben Zweck, erzeugt jedoch eigene Hürden hinsichtlich Nutzererlebnis, Medienbrüchen, technischer Verfügbarkeit, Prozessaufwand und Kosten. Über den langen Lebenszyklus von Versicherungsverträgen hinweg führt dies regelmäßig zu wiederkehrenden Identifizierungsprozessen und entsprechendem Aufwand für alle Beteiligten.

Die Rechtsgrundlage ändert sich in zwei Stufen. Das Digitale-Identitäten-Gesetz nimmt die Wallet als Identifizierungsmittel in

§ 12 Absatz 1 GwG auf, schreibt die Aufzeichnung des Authentifizierungs- und Validierungsverfahrens fest und lässt die Referenzüberweisung bei der Identifizierung über eine qualifizierte elektronische Signatur entfallen. Ab dem 10. Juli 2027 löst die AML-Verordnung diese Regelungen ab. Artikel 22 Absatz 6 nennt die Wege der Identitätsüberprüfung, darunter elektronische Identifizierungsmittel mit dem Sicherheitsniveau substanziell oder hoch und einschlägige qualifizierte Vertrauensdienste.

Für Versicherer bedeutet das: Die d-you bzw. EUDI-Wallet steht künftig als weiteres zulässiges Identifizierungsmittel neben den bestehenden Verfahren zur Verfügung. Auch videogestützte Verfahren können weiterhin genutzt werden, sofern sie die regulatorischen Anforderungen erfüllen und mit einem entsprechenden qualifizierten Vertrauensdienst kombiniert werden. Für den Use Case eines spartenübergreifenden KYC ist jedoch insbesondere relevant, ob eine einmal bestätigte Identität über Produkte, Sparten, Vertriebskanäle und verschiedene Zeitpunkte hinweg wiederverwendet werden kann. Dies eröffnet die Möglichkeit eines spartenübergreifenden KYC über den gesamten Vertragslebenszyklus hinweg und verschiebt den Fokus von der wiederholten Durchführung einzelner Identifizierungsprozesse hin zur Nutzung vertrauenswürdiger digitaler Identitäten. Im Zielbild wird die Prüfung in die Antragsstrecke integriert, auch in die des Vermittlers, und der Versicherer fordert nur die zweckgebundenen Attribute an. Die bestätigte Identität ist über Sparten hinweg und für die Aktualisierung im Bestand nutzbar; im Leistungsfall weist sich der Bezugsberechtigte mit der eigenen Wallet aus, statt Unterlagen einzureichen. Da die Wallet-Nutzung freiwillig bleibt und die Akzeptanzpflicht nur auf Verlangen greift, läuft ein erheblicher Teil der Fälle weiter über andere zulässige Wege. Der Use Case trägt daher nur mit einer methodenunabhängigen Identifizierungsschicht, die Wallets, nationale eID-Verfahren, eIDAS-konforme Vertrauensdienste sowie, sofern erforderlich, begründete alternative Identifizierungsverfahren über eine einheitliche Schnittstelle integriert. Sie ist sowohl in der Direkt- als auch in der Vermittlerstrecke einsetzbar und gewährleistet

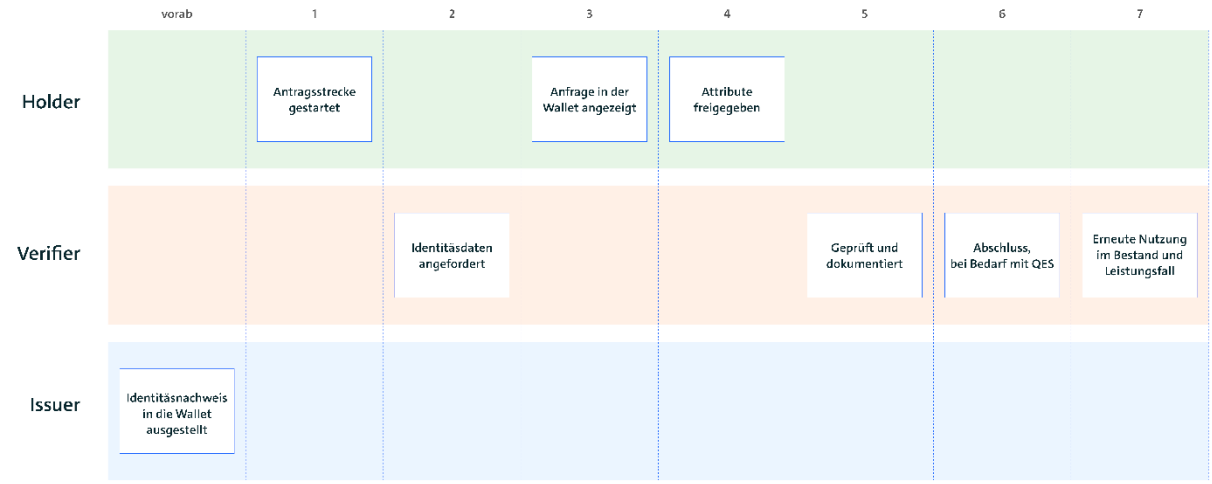
eine konsistente Nachweis- und Beweisführung. Welches Verfahren genutzt wird, kann je nach Kundensituation, Vertriebskanal und regulatorischem Kontext variieren. Für den Versicherer ist jedoch entscheidend, dass die zugrunde liegende Identität und die daraus resultierenden Nachweise verfahrensübergreifend nutzbar sind und konsistent verwaltet werden können.

Holder	Versicherungsnehmer, wirtschaftlich Berechtigter oder Bezugsberechtigter	gibt einzelne Attribute frei
Verifier	Versicherer sowie Vermittler, Makler oder Abschlussplattform	fordert Attribute an und prüft sie; zuvor als Relying Party registriert
Issuer	staatlicher Aussteller der Personenidentifizierungsdaten	stellt den Identitätsnachweis in die Wallet aus
Weitere	Identifizierungs- und Vertrauensdienstleister (evtl. als Intermediaries auftretend)	stellen die zulässigen Verfahren und die Beweisführung bereit, inkl. der Orchestrierung dessen

Ablauf

1. Kundin oder Kunde startet die Antragsstrecke beim Versicherer oder beim Vermittler.
2. Der Versicherer fordert die erforderlichen Identitätsdaten an; angeboten werden die zulässigen Verfahren, darunter die EUDI-Wallet.
3. Die Wallet zeigt transparent an, welche Attribute zu welchem Zweck angefragt werden.
4. Kundin oder Kunde gibt die Attribute per Wallet-Authentifizierung frei.
5. Die Attribute werden übermittelt, kryptografisch geprüft und gegen den erforderlichen Datensatz abgeglichen.
6. Der Antrag wird abgeschlossen, ggf. bei Schriftformerfordernis qualifiziert elektronisch signiert.
7. Die geprüfte Identität steht für weitere Anträge, die Aktualisierung im Bestand und den Leistungsfall zur Verfügung.

Benötigte Nachweise und Attribute



Zu identifizieren sind Versicherungsnehmer, ggf. wirtschaftlich Berechtigte und abweichende Bezugsberechtigte. Einzuholen sind alle Vor- und Nachnamen, Geburtsort und vollständiges Geburtsdatum, Staatsangehörigkeit und ggf. nationale Identifikationsnummer sowie der gewöhnliche Aufenthaltsort und, falls verfügbar, die Steueridentifikationsnummer; die Einzelheiten konkretisieren die technischen Regulierungsstandards. Weitere Attribute werden nicht abgefragt, die selektive Freigabe einzelner Merkmale ist zu nutzen. Der abfragbare Datenumfang wird bereits bei der Registrierung als Relying Party festgelegt, das Attributdesign gehört deshalb an den Anfang des Projekts.

Gespeichert werden nur die aufzuzeichnenden Angaben. Zeitpunkt, Attribute, Quelle, Vertrauensniveau und Ergebnis der Prüfung sind einheitlich über alle Verfahren zu dokumentieren, einschließlich der für das jeweilige Verfahren regulatorisch vorgesehenen Angaben. Soweit alternative Verfahren im Sinne der regulatorischen Vorgaben eingesetzt werden, sind auch die hierfür erforderlichen Begründungen und Nachweise zu dokumentieren. Die Unterlagen sind so aufzubewahren, dass die Identifizierung im Leistungsfall auch Jahre später noch nachvollziehbar und belegbar ist.

Voraussetzungen

Rechtlich: eIDAS 2.0; Digitale-Identitäten-Gesetz mit den Änderungen im Geldwäschegesetz; AML-Verordnung ab dem 10. Juli 2027; versicherungsspezifische Vorgaben zum Bezugsberechtigten; Datenminimierung nach DSGVO.

Technisch: Registrierung als Relying Party mit Angabe der Daten und ihres Zwecks; Anbindung an Antrags-, Bestands- sowie Vermittler- und Maklersysteme über die etablierten Branchenschnittstellen; langfristige, revisionssichere Beweisspeicherung; eine gemeinsame Schnittstelle für alle zulässigen Verfahren.

Organisatorisch: Anpassung von Antrags-, Bestands- und Leistungsprozessen; Einbindung des Geldwäschebeauftragten; Schulung von Vertrieb und Innendienst; Abstimmung mit Vermittlern; Dienstleistersteuerung im Auslagerungsmanagement.

Extern: Verfügbarkeit der nationalen Wallet und der Personenidentifizierungsdaten; Verbreitung in der Zielgruppe, auch bei älteren Bestandskunden; Mitwirkung von Vermittlern und Maklerpools; Konkretisierungen durch die Aufsicht.

Nutzen

Kundennutzen	Nutzen Versicherer
Vereinfachte Identifizierung im Antrag	schnellere Antragsstrecke, geringere Abbruchquote, keine Kosten für Einzelauthentifizierungen
kein Nachreichen von Unterlagen im Leistungsfall	schnellere Leistungsbearbeitung
transparente Datenfreigabe	einheitliche Nachweisbarkeit gegenüber der Aufsicht
gleiches Erlebnis über Sparten und Kanäle	eine Integration statt mehrerer Einzelverfahren

Herausforderungen

- Vermittlervertrieb: Die Identifizierung findet häufig beim Vermittler statt, der selbst Verpflichteter ist. Sie muss in dessen Strecke funktionieren und das Ergebnis prüffest beim Versicherer ankommen.
- Verbreitung: Kundinnen und Kunden ohne Wallet oder Smartphone sowie Personen mit Nicht-EU-Dokumenten müssen gleichwertig identifiziert werden können.
- Abgrenzung: Der Use Case deckt die Identifizierung ab, nicht die Risikobewertung, Sanktions- und PEP-Abgleich oder das laufende Monitoring.

Übergabe der Daten des KFZ-Schein bei Vertragsabschluss

Rolle des Versicherers	Issuer
Sparte und Prozessphase	Kfz | Bestand, mit Bezug zu Schaden
Wallet-Funktion	Nachweis ausstellen, Speicherung
Zeithorizont	mittelfristig

Ausgangslage und Zielbild

Die Grüne Karte (Internationale Versicherungskarte für den Kraftverkehr) belegt, dass für ein Fahrzeug Kfz-Haftpflichtschutz besteht. Sie wird heute als Papier oder PDF verschickt und vom Kunden selbst ausgedruckt. Im Alltag hat der Kunde sie oft nicht dabei. Wer sie prüft, kann weder die Echtheit sicher feststellen noch erkennen, ob der Vertrag noch gültig ist. Gefälschte Nachweise sind ein bekanntes Problem.

Zielbild: Der Versicherer stellt den Nachweis als elektronische Attributsbescheinigung aus. Der Kunde speichert diesen in seiner EUDI-Wallet und zeigt ihn bei einer Verkehrs- oder Grenzkontrolle oder nach einem Unfall vor. Der Prüfer erkennt sofort, ob der Nachweis echt ist, von einem vertrauenswürdigen Versicherer stammt und noch gilt. Ändert sich der Vertrag, widerruft der Versicherer den alten Nachweis und stellt einen neuen aus.

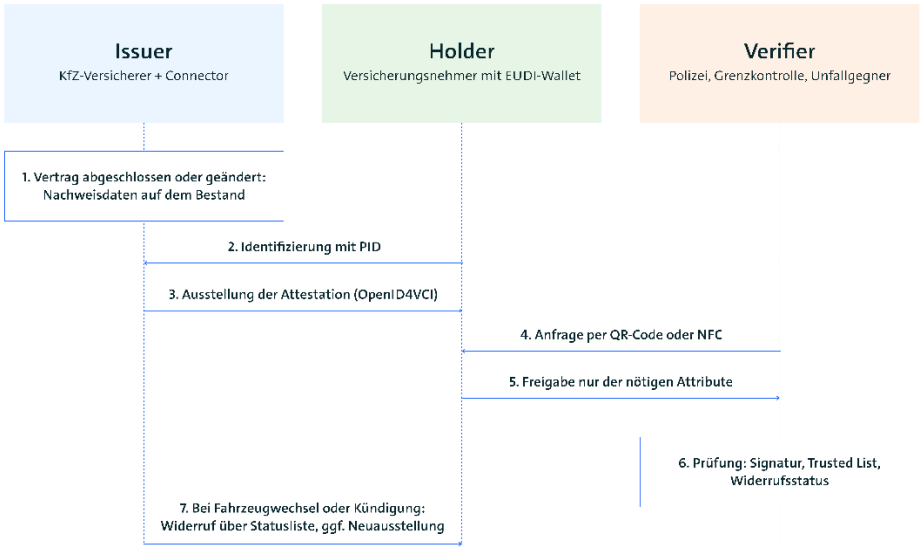
Übertragbarkeit: Das Muster lässt sich auf weitere Versicherungsnachweise übertragen, zum Beispiel auf die Auslandsreisekrankenversicherung oder Berufshaftpflicht.

Holder	Versicherungsnehmer bzw. Halter	hält den Nachweis in der EUDI-Wallet und gibt bei Bedarf nur die nötigen Attribute frei
Verifier	Polizei und Grenzkontroll-behörden (In- und Ausland), Unfallgegner bzw. dessen Versicherer	fordert den Nachweis an und prüft Echtheit, Herkunft und Gültigkeit
Issuer	Kfz-Versicherer	stellt den Nachweis aus, aktualisiert und widerruft ihn
Weitere	Connector; Büro Grüne Karte	Connector: bindet das Bestandssystem des Versicherers an die Ausstellungsschnittstelle zur EUDI an. Büro Grüne Karte: Abstimmung des Nachweisformats im Grüne-Karte-System

Ablauf

1. Der Kunde schließt einen Kfz-Vertrag ab oder ändert ihn (Fahrzeugwechsel, Verlängerung). Das Bestandssystem stellt die Nachweisdaten bereit.
2. Der Kunde identifiziert sich im Kundenportal oder in der App des Versicherers mit den Personenidentifizierungsdaten (PID) aus seiner EUDI-Wallet.
3. Der Versicherer stellt die Attestation »Kfz-Versicherungsnachweis« über OpenID4VCI aus. Die Wallet speichert sie.
4. Bei einer Kontrolle oder nach einem Unfall fordert der Verifier den Nachweis per QR-Code oder NFC an.
5. Der Kunde sieht, welche Attribute angefragt werden, und gibt nur diese frei.
6. Der Verifier prüft die Signatur, den Vertrauensstatus des Versicherers (Trusted List) und den Widerrufsstatus.
7. Bei Fahrzeugwechsel, Kündigung oder Vertragsende widerruft der Versicherer den Nachweis über eine Statusliste und stellt bei Bedarf einen neuen aus.

Prozessdiagramm



Nachweise und Attribute

Für die Ausstellung: PID des Versicherungsnehmers (Name, Vorname, Geburtsdatum), um den Nachweis an die richtige Person zu binden.

Im Kfz-Versicherungsnachweis: amtliches Kennzeichen, Fahrzeugart, optional Fahrzeug-Identifizierungsnummer, Name des Versicherungsnehmers, Versicherer mit Länder- und Versichererkode, Nummer der Versicherungskarte, Gültigkeitszeitraum, Geltungsbereich (Länder) sowie Kontakt für die Schadenmeldung.

Selektive Offenlegung: Für eine Kontrolle reichen meist Kennzeichen, Versicherer und Gültigkeit. Name und weitere Angaben werden nur freigegeben, wenn der Anlass es verlangt, etwa bei einem Unfall.

Voraussetzungen

Rechtlich: eIDAS-Verordnung (VO (EU) 2024/1183) und Durchführungsrechtsakte; Anerkennung eines elektronischen Nachweises im Pflichtversicherungsrecht und im Grüne-Karte-System; DSGVO, insbesondere Datenminimierung

Technisch: Ausstellung über OpenID4VCI, Vorlage über OpenID4VP bzw. ISO/IEC 18013-5; Formate SD-JWT VC oder mdoc; Statusliste für Widerruf; Anbindung Bestandssystem über Connector; Registrierung als Issuer

Organisatorisch: Ausstellung und Widerruf im Bestandsprozess verankern; Zuständigkeit für Schlüssel und Zertifikate klären; Schulung Kundenservice

Extern: Rulebook und Attestation-Schema für Kfz-Versicherungsnachweise (Branche, Büro Grüne Karte); Prüf-Apps bei Polizei und Behörden; Verbreitung der EUDI

Nutzen

Kundennutzen	Nutzen Versicherer
Nachweis immer auf dem Smartphone, kein Ausdruck nötig	Weniger Druck, Versand und Serviceanfragen
Schnelle Klärung bei Kontrolle oder Unfall	Schutz vor gefälschten Nachweisen durch prüfbare Signatur
Kontrolle darüber, welche Daten geteilt werden	Digitaler Kontaktpunkt im Bestand und Baustein für weitere Nachweise

Herausforderungen

- Akzeptanz beim Verifier: Ohne Prüf-Apps bei Polizei und Behörden bleibt der Nachweis eine reine Anzeige.
- Fehlendes Schema: Für Versicherungsnachweise gibt es noch kein abgestimmtes Rulebook. Das braucht eine branchenweite und internationale Abstimmung.
- Fahrzeug statt Person: Der Nachweis gehört zum Fahrzeug, die Wallet zur Person. Für weitere Fahrer (Familie, Flotte) braucht es eine Lösung.
- Übergangsphase: Papier bzw. PDF und EUDI-Attestation laufen eine Zeit lang parallel, bis die EUDI-Wallet verbreitet ist.
- Aktualität: Widerruf muss schnell und zuverlässig greifen, etwa bei Kündigung oder Fahrzeugwechsel

Orchestrierung Schadensmeldung in eigener Versicherungs-App mit integrierter EUDI-Wallet Funktion

Rolle des Versicherers	Verifier / Relying Party
Sparte und Prozessphase	Kranken | Bestand
Wallet-Funktion	Nachweis prüfen (PID)
Zeithorizont	kurzfristig, sobald die EUDI-Wallet in Deutschland verfügbar ist

Ausgangslage und Zielbild

Im Kundenportal eines Krankenversicherers liegen besonders schützenswerte Daten: Arztrechnungen, Leistungsabrechnungen, Diagnosen und Tarifdaten. Das sind Gesundheitsdaten nach Art. 9 DSGVO. Der Versicherer muss deshalb sicherstellen, dass wirklich nur die berechtigte Person Zugang erhält.

Ausgangslage: Heute geschieht das meist über zwei Briefe: Einer enthält die Zugangsdaten oder einen Registrierungscode, der zweite einen Aktivierungscode. Das kostet Druck und Porto, dauert mehrere Tage und führt zu Abbrüchen, wenn ein Brief verloren geht oder der Code abgelaufen ist. Auch die Wiederherstellung eines gesperrten Zugangs läuft oft erneut per Post.

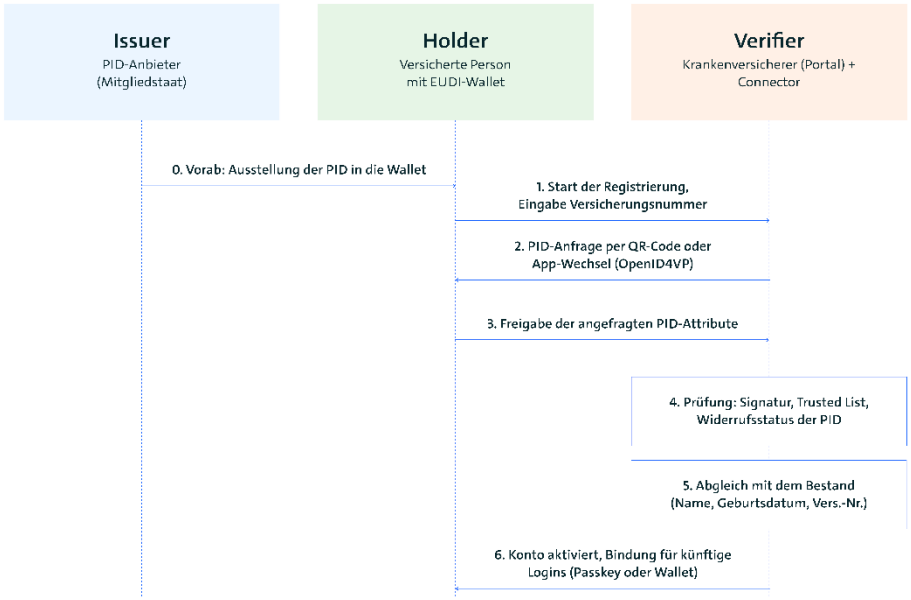
Zielbild: Der Kunde legitimiert sich bei der Registrierung mit den PID aus seiner EUDI-Wallet. Der Versicherer prüft die PID, gleicht sie mit dem Bestand ab und schaltet den Zugang sofort frei. Die PID haben das Vertrauensniveau »hoch« und sind damit mindestens so belastbar wie das Briefverfahren. Dieselbe Prüfung dient zur Wiederherstellung des Zugangs und für eine erneute Bestätigung vor besonders sensiblen Aktionen, etwa der Änderung der Bankverbindung.

Holder	Versicherungsnehmer, wirtschaftlich Berechtigter oder Bezugsberechtigter	gibt einzelne Attribute frei
Verifier	Versicherer sowie Vermittler, Makler oder Abschlussplattform	fordert Attribute an und prüft sie; zuvor als Relying Party registriert
Issuer	staatlicher Aussteller der Personenidentifizierungsdaten	stellt den Identitätsnachweis in die Wallet aus
Weitere	Identifizierungs- und Vertrauensdienstleister (evtl. als Intermediaries auftretend)	stellen die zulässigen Verfahren und die Beweisführung bereit, inkl. der Orchestrierung dessen

Ablauf

1. Der Kunde startet im Portal oder in der App die Registrierung und gibt seine Versicherungsnummer ein.
2. Das Portal fordert die PID an: am Desktop per QR-Code, am Smartphone per Wechsel in die Wallet (OpenID4VP).
3. Die Wallet zeigt, dass der Krankenversicherer anfragt und welche Attribute er verlangt. Der Kunde bestätigt die Freigabe.
4. Der Versicherer prüft die Signatur der PID, den Vertrauensstatus des Ausstellers (Trusted List) und den Widerrufsstatus.
5. Der Versicherer gleicht Name, Geburtsdatum und Versicherungsnummer mit dem Bestand ab. Bei eindeutigem Treffer wird der Zugang freigeschaltet, sonst greift das Briefverfahren.
6. Der Kunde legt für künftige Logins einen Passkey an oder meldet sich weiter mit der Wallet an.
7. Bei Gerätewechsel, gesperrtem Zugang oder sensiblen Änderungen wiederholt der Kunde die PID-Prüfung statt auf neue Briefe zu warten.

Prozessdiagramm



Benötigte Nachweise und Attribute

Aus der PID: Familienname, Vorname, Geburtsdatum; optional Geburtsname und Anschrift, soweit in der PID enthalten und für den Abgleich nötig.

Vom Kunden: Versicherungsnummer, die der Kunde selbst eingibt. Sie verbindet die geprüfte Identität mit dem Vertrag.

Datenminimierung: Der Versicherer fragt nur die Attribute an, die er für den Abgleich braucht und für die er registriert ist. Gesundheitsdaten fließen in diesem Schritt nicht.

Voraussetzungen

Rechtlich: eIDAS-Verordnung (VO (EU) 2024/1183) und Durchführungsrechtsakte, insbesondere zur Registrierung von Relying Parties; DSGVO, besonders Art. 9 und Art. 32; DORA für die IKT-Sicherheit; Prüfung, ob die Akzeptanzpflicht für private Relying Parties mit starker Authentifizierung greift

Technisch: Prüfkomponente für OpenID4VP (same-device und cross-device) mit Formaten SD-JWT VC bzw. mdoc; Anbindung an Portal und Identitätsmanagement über Connector; Registrierung als Relying Party mit Zugangszertifikat

Organisatorisch: Regeln für den Bestandsabgleich und Fälle ohne eindeutigen Treffer; Briefverfahren als Rückfallweg; Zuständigkeit Datenschutz und Informationssicherheit; Schulung Kundenservice

Extern: Verfügbarkeit der deutschen EUDI-Wallet und der PID; Verbreitung bei den Versicherten; Registrierungsstelle für Relying Parties

Nutzen

Kundennutzen	Nutzen Versicherer
Sofortiger Zugang statt mehrerer Tage Warten auf zwei Briefe	Wegfall von Druck und Porto für zwei Briefe je Registrierung
Keine Codes aufbewahren, einfache Wiederherstellung des Zugangs	Weniger Abbrüche und Serviceanfragen zu Codes und Sperren
Hoher Schutz der eigenen Gesundheitsdaten	Identifizierung auf Vertrauensniveau »hoch«, gut dokumentierbar gegenüber Datenschutz und Aufsicht

Herausforderungen

- Langzeitbeweiswert: Lebensversicherungen laufen oft Jahrzehnte. Zertifikate und Algorithmen veralten, deshalb braucht es eine Nachsignierung oder einen qualifizierten Bewahrungsdienst.
- Zwei Personen: Sind Versicherungsnehmer und versicherte Person verschieden, müssen sich beide identifizieren, und die versicherte Person muss die Gesundheitsangaben selbst signieren.
- Vermittlergestützter Antrag: Erfasst der Vermittler die Antworten, muss der Antragsteller sie vor der Signatur vollständig sehen und bestätigen können.
- Verständlichkeit: Der Kunde muss im Moment der Signatur sehen, was er unterschreibt. Beim Antrag am PC heißt das: Die Antworten müssen auf dem Smartphone noch einmal lesbar angezeigt werden. Lange Fragebögen auf dem kleinen Bildschirm sind dabei eine Hürde.
- Phishing im Cross-Device-Flow: Beim reinen QR-Code kann ein Angreifer dem Kunden einen fremden Code unterschieben und dessen Freigabe für die eigene Sitzung nutzen. Die Digital Credentials API mit Näheprüfung per Bluetooth senkt dieses Risiko. Links per SMS oder E-Mail sind besonders anfällig.
- Rechtliche Einordnung: Die Anerkennung der PID im Geldwäscherecht und die QES-Funktion der deutschen Wallet müssen geklärt sein.

Antrag in der Sparte Leben mit Gesundheitsfragen: Identifizierung mit PID und QES über die EUDI

Rolle des Versicherers	Verifier / Relying Party
Sparte und Prozessphase	Leben (z. B. Risikoleben, Berufsunfähigkeit) | Antrag
Wallet-Funktion	Nachweis prüfen (PID), Signatur (QES)
Zeithorizont	kurzfristig für die PID-Identifizierung, mittelfristig für die QES über die Wallet

Ausgangslage und Zielbild

Ausgangslage: Bei Online-Anträgen in der Lebensversicherung wird der Antragsteller heute über verschiedene Fernidentifizierungsverfahren identifiziert, etwa per Video-Ident oder mit der Online-Ausweisfunktion des Personalausweises. Die Gesundheitsfragen werden online beantwortet oder vom Vermittler erfasst und mit einer einfachen elektronischen Unterschrift oder per Klick bestätigt.

Die Angaben zu den Gesundheitsfragen sind über die gesamte Vertragslaufzeit wichtig. Im Leistungsfall prüft der Versicherer, ob die vorvertragliche Anzeigepflicht nach § 19 VVG erfüllt wurde. Ob ein Rücktritt oder eine Anfechtung möglich ist, hängt dann von dem Nachweis ab, dass genau diese Angaben vom Antragsteller stammen. Mit einem Klick oder einer einfachen Signatur ist dieser Nachweis schwach, besonders wenn ein Vermittler die Angaben eingetragen hat.

Zielbild: Der Antragsteller identifiziert sich mit den PID aus seiner EUDI-Wallet, als eine von mehreren Identifizierungsoptionen, zwischen denen er frei wählen kann. Seine Antworten auf die Gesundheitsfragen unterschreibt er mit einer qualifizierten elektronischen Signatur (QES), die die EUDI bereitstellt. Die QES ist der handschriftlichen Unterschrift gleichgestellt. Der Versicherer archiviert das signierte Dokument so, dass die Signatur auch nach Jahrzehnten noch prüfbar ist.

Variante PC und Smartphone: Der Kunde füllt den Antrag am PC aus und bestätigt PID und Signatur auf dem Smartphone, auf dem die Wallet liegt (Cross-Device-Flow). Die Verbindung entsteht über einen QR-Code auf dem Bildschirm oder über die Digital Credentials API des Browsers. Nach der Freigabe läuft der Antrag am PC weiter. Ein Link per SMS oder E-Mail ist nur als Rückfallweg gedacht.

Beteiligte

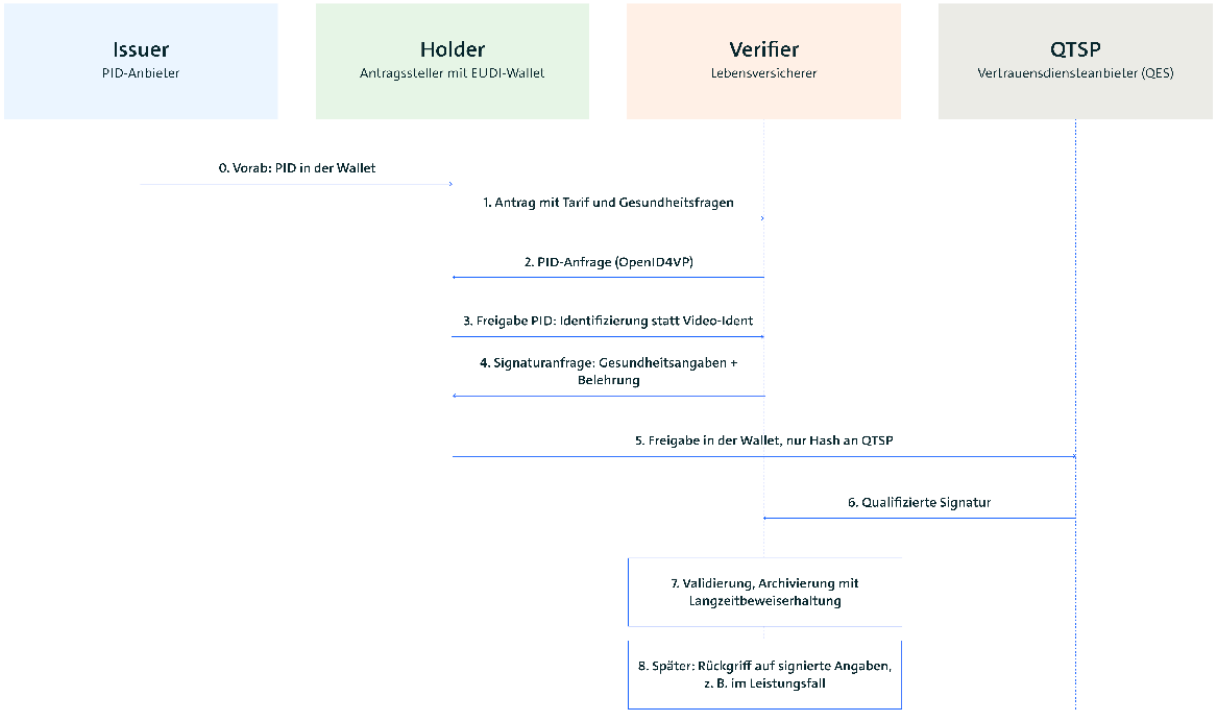
Holder	Antragsteller bzw. zu versichernde Person	hält PID und Signaturfunktion in der EUDI-Wallet, gibt die PID frei und signiert die Gesundheitsangaben
Verifier	Lebensversicherer	fordert die PID an und prüft sie, fordert die Signatur an und validiert sie
Issuer	PID-Anbieter des Mitgliedstaats	stellt die PID aus (in Deutschland abgeleitet vom Personalausweis)
Weitere	Qualifizierter Vertrauensdiensteanbieter (QTSP); Connector; ggf. Vermittler	QTSP: stellt das qualifizierte Zertifikat und die Signaturerstellung bereit. Connector: bindet PID-Prüfung und Signaturanfrage an die Antragsstrecke an. Vermittler: begleitet den Antrag, signiert aber nicht für den Kunden

Ablauf

1. Der Antragsteller wählt online oder mit einem Vermittler Tarif und Versicherungssumme und beantwortet die Gesundheitsfragen.
2. Die Antragsstrecke fordert die PID an (OpenID4VP): am Smartphone per Wechsel in die Wallet, am PC per QR-Code oder Digital Credentials API. Der Antragsteller gibt sie in der Wallet frei. Der Versicherer prüft Signatur, Aussteller und Widerrufsstatus und dokumentiert die Identifizierung. Ein weiteres Identifizierungsverfahren ist dann nicht erforderlich.
3. Der Versicherer erzeugt aus den Gesundheitsangaben ein Dokument (z. B. PDF/A). Es enthält Fragen, Antworten, die gesonderte Belehrung über die Folgen einer Anzeigepflichtverletzung (§ 19 Abs. 5 VVG) und bei Bedarf die Einwilligung zur Schweigepflichtentbindung.

4. Die Wallet zeigt das Dokument und fordert die Signatur an, beim Antrag am PC ebenfalls auf dem Smartphone. Der Antragsteller sieht seine Antworten dort noch einmal, prüft den Inhalt und bestätigt mit PIN oder Biometrie. Danach läuft der Antrag am PC weiter.
5. Der QTSP erzeugt die qualifizierte Signatur. Er erhält dafür nur den Hashwert des Dokuments, nicht die Gesundheitsdaten.
6. Der Versicherer validiert die Signatur und archiviert das Dokument mit Validierungsnachweis und Maßnahmen zur Langzeitbeweiserhaltung. Danach folgen Risikoprüfung und Policierung.
7. Im Leistungsfall oder bei Zweifeln an den Angaben greift der Versicherer auf das signierte Dokument zurück und kann Echtheit und Urheberschaft belegen.

Prozessdiagramm



Benötigte Nachweise und Attribute

Aus der PID: Familienname, Vorname, Geburtsdatum, Geburtsort, Staatsangehörigkeit und Anschrift. Das deckt die Angaben ab, die für eine Identifizierung nach Geldwäschegesetz erhoben werden, soweit der Tarif darunterfällt.

Für die Signatur: Qualifiziertes Zertifikat des Antragstellers, ausgestellt vom QTSP auf Basis der PID.

Im signierten Dokument: Gesundheitsfragen und Antworten, Belehrung nach § 19 Abs. 5 VVG, Zeitpunkt, bei Bedarf Einwilligung zur Schweigepflichtentbindung (§ 213 VVG). Diese Inhalte bleiben beim Versicherer und gehen nicht in die Wallet als Attestation.

Voraussetzungen

Rechtlich: eIDAS-Verordnung (VO (EU) 2024/1183): PID, QES über die Wallet, Gleichstellung der QES mit der handschriftlichen Unterschrift, Bewahrungsdienste; Geldwäschegesetz, Anerkennung der PID als Identifizierungsmittel; VVG §§ 19 und 213; DSGVO Art. 9; Aufbewahrungsfristen über die Vertragslaufzeit

Technisch: Prüfkomponente für OpenID4VP, same-device und cross-device (QR-Code bzw. Digital Credentials API); Signaturanfrage an die Wallet bzw. den QTSP (z. B. CSC-Schnittstelle); Signaturformat PAdES; Validierungsdienst; Archiv mit Langzeitbeweiserhaltung (z. B. nach BSI TR-ESOR); Registrierung als Relying Party

Organisatorisch: Regeln für den Bestandsabgleich und Fälle ohne eindeutigen Treffer; Briefverfahren als Rückfallweg; Zuständigkeit Datenschutz und Informationssicherheit; Schulung Kundenservice

Extern: eIDAS-Verordnung (VO (EU) 2024/1183): PID, QES über die Wallet, Gleichstellung der QES mit der handschriftlichen Unterschrift, Bewahrungsdienste; Geldwäschegesetz, Anerkennung der PID als Identifizierungsmittel; VVG §§ 19 und 213; DSGVO Art. 9; Aufbewahrungsfristen über die Vertragslaufzeit

Prüfkomponente für OpenID4VP, same-device und cross-device (QR-Code bzw. Digital Credentials API); Signaturanfrage an die Wallet bzw. den QTSP (z. B. CSC-Schnittstelle); Signaturformat PAdES; Validierungsdienst; Archiv mit Langzeitbeweiserhaltung (z. B. nach BSI TR-ESOR); Registrierung als Relying Party

Antragsstrecke anpassen; Rolle des Vermittlers klar trennen; Ablauf, wenn Versicherungsnehmer und versicherte Person verschieden sind; weitere Identifizierungsverfahren (z. B. Video-Ident, Online-Ausweisfunktion) als Optionen nach Wahl des Kunden; Schulung Vertrieb und Antragsprüfung

Verfügbarkeit von PID und QES in der deutschen EUDI-Wallet; Vertrag mit einem QTSP; aufsichtliche Klarheit zur PID im Geldwäscherecht

Nutzen

Kundennutzen	Nutzen Versicherer
Abschluss jederzeit und in wenigen Minuten	Geringeres Abbruchsrisiko in der Antragsstrecke und vergleichsweise geringe Kosten
Klarheit, welche Angaben genau abgegeben und unterschrieben wurden	Beweissichere Gesundheitsangaben für eine spätere Prüfung, Rücktritt oder Anfechtung
Schutz vor falsch übertragenen Angaben durch Dritte	Medienbruchfreier Antrag ohne Papier und Nachforderung von Unterschriften

Herausforderungen

- Langzeitbeweiswert: Lebensversicherungen laufen oft Jahrzehnte. Zertifikate und Algorithmen veralten, deshalb braucht es eine Nachsignierung oder einen qualifizierten Bewahrungsdienst.
- Zwei Personen: Sind Versicherungsnehmer und versicherte Person verschieden, müssen sich beide identifizieren, und die versicherte Person muss die Gesundheitsangaben selbst signieren.
- Vermittlergestützter Antrag: Erfasst der Vermittler die Antworten, muss der Antragsteller sie vor der Signatur vollständig sehen und bestätigen können.
- Verständlichkeit: Der Kunde muss im Moment der Signatur sehen, was er unterschreibt. Beim Antrag am PC heißt das: Die Antworten müssen auf dem Smartphone noch einmal lesbar angezeigt werden. Lange Fragebögen auf dem kleinen Bildschirm sind dabei eine Hürde.
- Phishing im Cross-Device-Flow: Beim reinen QR-Code kann ein Angreifer dem Kunden einen fremden Code unterschieben und dessen Freigabe für die eigene Sitzung nutzen. Die Digital Credentials API mit Näheprüfung per Bluetooth senkt dieses Risiko. Links per SMS oder E-Mail sind besonders anfällig.
- Rechtliche Einordnung: Die Anerkennung der PID im Geldwäscherecht und die QES-Funktion der deutschen Wallet müssen geklärt sein. Unabhängig davon stehen den Kundinnen und Kunden weitere zulässige Verfahren wie die Online-Ausweisfunktion oder Video-Ident zur Wahl.

5 Vorgehen für Strategie- und Roadmap-Entwicklung

Dieser Leitfaden hat aufgezeigt, wie die Etablierung des eIDAS-Ökosystems und die Einführung der EUDI-Wallet-Technologie die Digitalisierung bei Kunden, Mitarbeitern und Partnern einer Versicherung beeinflussen werden. Mit dem branchenübergreifenden Ansatz werden Prozesse gestaltet, die den Datenaustausch über die Versicherungsindustrie hinaus ermöglichen. Das hierbei entstehende Ökosystem von Datenausstellern (Issuern), Datenempfängern (Relying Parties bzw. eines Verifiers) aber auch Anbietern von eigenen Wallet-Lösungen (Wallet-Provider) wird schrittweise skalieren und die Versicherungswirtschaft wird hiervon profitieren, aber auch selber einen wichtigen Impuls einbringen.

Gleichzeitig dienen der Einsatz der Technologie und die Nutzung des Ökosystems keinem Selbstzweck und sind auch nur wirksam durch die Integration mit weiteren IT-Lösungen, die gemeinsam die Prozessoptimierung ermöglichen. Die Entwicklung von konkreten Anwendungsfällen für den Einsatz der EUDI startet auf Basis der Digitalstrategie einer Versicherung. Die hier festgelegten Prioritäten und die sich daraus ableitende Roadmap für die Anpassung bzw. Neugestaltung von digitalen Kunden-, Mitarbeiter- und Partnerprozessen können genutzt werden, um den sinnvollen Einsatz der EUDI-Technologie bzw. des eIDAS-2.0-Vertrauensraums zu verproben.

Damit integrieren sich das Wissen und die Expertise zum eIDAS-2.0-Ökosystemansatz, der EUDI-Wallet und den Funktionen, die sich aus deren Nutzung ergeben, in laufende und zukünftige Projekte zur Umsetzung der Digitalstrategie. Es bedarf also einer Analyse, welche konkreten Digitalisierungsinitiativen durch die EUDI auch im Wettbewerb / Vergleich zu anderen Ansätzen (z. B. FIDA, zentralem Datenaustausch) besser umgesetzt werden können.

Damit wird es zur wichtigen Aufgabe einer Versicherung, das Wissen und die Kompetenz zum eIDAS-2.0-Ökosystem, den dort verankerten Designprinzipien und die Expertise zu den technischen Möglichkeiten im Unternehmen so aufzubauen und in der Struktur zu verankern, dass diese als Querfunktion in laufende und zukünftige Digitalisierungsprojekte integriert werden können. Der Aufbau eines zentralen »Kompetenzträgers« / einer zentralen »Kompetenzträgerin« bzw. eines »Kompetenzteams« mit entsprechenden Aufgaben und Verantwortlichkeiten ist daher notwendig. Eine solche Funktion kann dann ähnlich einem CISO oder einem Geldwäschebeauftragten den Vorstand bei der Umsetzung seiner Digitalstrategie unterstützen.

Dabei kommt die spartenübergreifende Nutzung der EU-weiten Standards und IT-Sicherheitsvorgaben gerade Versicherungen zugute, die unterschiedlichen Vorgaben aus den Bereichen AMLR bzw. GWG oder auch für die Gesundheitssparte der gematik bzw. des EHDS umsetzen müssen. Es wird mit der eIDAS-2.0-Verordnung nun möglich, diese Vorgaben durch übergreifend nutzbare Komponenten, wie die EUDI-Wallet

umzusetzen und damit brancheübergreifend einheitlich zu etablieren. Umso mehr braucht es bei der strategischen Einordnung dieser Themen einen übergreifenden Ansatz und Blick, um zukünftig Spartenlösungen zu vermeiden.

Um eine echte eIDAS-2.0-Perspektive einzunehmen, werden zukünftig unterschiedliche Perspektiven gekoppelt, eben in Kombination von Kunden, Mitarbeitern und Partnern, aber auch im Hinblick auf Personen und Unternehmen, die in diesen Rollen agieren. Mit der Einführung der EU-Business-Wallet bis 2029 wird es möglich sein, diese unterschiedlichen funktionalen Anforderungen aus diesen Perspektiven einzubinden und somit auch alle Instrumente aus dem eIDAS-2.0-Ökosystem in konkreten Geschäftsprozessen zu nutzen.

Bei der weiteren Betrachtung der EUDI-Einführung sind somit Personen, Unternehmen und auch IoT-Geräte und deren technische Wallet-Lösungen von Anfang an einzubeziehen.

Usecase Design (Pains & Gains, Service Design, Prototyping, Ziel Nutzerversprechen / Machbarkeit)

Die Entwicklung neuer digitaler Services und damit die Identifizierung und Umsetzung konkreter Use Cases sollte sich in einem Versicherungsunternehmen an einem Lean-Product-Management-Ansatz orientieren. Vorteil eines solchen Verfahrens ist die frühzeitige Verprobung von Annahmen bzw. des Nutzens bei den späteren Anwendern und auch der technischen Machbarkeit.

Aufbauend auf einer Digitalstrategie und bereits identifizierten Bereichen mit Optimierungsbedarf braucht jede neue Service-Idee zunächst eine Analyse der vorhandenen Probleme, die gelöst werden sollen, bzw. von Wünschen, die Anwender mit einer Prozessoptimierung verbinden. Eine solche Pain- und Gain-Analyse findet häufig mit Experten aus dem eigenen Versicherungsunternehmen statt. Die sich hieraus ergebenden Annahmen müssen daher mit Anwendern bzw. anhand deren Prozesserlebens verprobt werden, bevor sie als Grundlagen für die Use Case-Entwicklung angesehen werden.

Solche verprobten Annahmen helfen dabei, den eigentlichen digitalen Service mit der EUDI-Wallet zu designen, die Integration mit bestehenden Systemen zu beschreiben und Mock-ups für die spätere Umsetzung zu erstellen. Auch diese Ergebnisse lassen sich mit Anwendern verproben. Sie geben frühzeitig Rückmeldung über den zu erwartenden Nutzen, aber auch die Usability. Gerade das Zusammenspiel mit einer Applikation, wie der EUDI, die als generische App keine versicherungsspezifischen Funktionen anbieten wird, braucht beim Design versicherungsrelevanter Prozesse (wie z. B. in Kapitel 4 beschrieben) ein gutes Feedback von den Nutzern bezüglich Handling und Integration in deren Lebensrealität.

Diese Prototyping-Phase bildet die Grundlage für die spätere technische Gestaltung des konkreten Anwendungsfalls. Die Ergebnisse der Prototyping-Phase werden gemeinsam mit der IT-Kompetenz im Versicherungsunternehmen zu einer technischen Gesamtarchitektur weiterentwickelt.Wird die Entwicklung des neuen Services nicht

über einen solchen Lean-Ansatz mit der frühzeitigen Verprobung der entsprechenden Annahmen durchgeführt, besteht bei der Implementierung des Use Cases die große Gefahr, dass später grundlegende Funktionen noch einmal verändert werden müssen, um Nutzerakzeptanz bzw. auch das Nutzerversprechen zu erreichen. Dies kann zu erheblichen Nachteilen, wie Zeitverzögerungen bzw. Folgekosten führen.

Roadmap Entwicklung und Implementierungsvorgehen

Auf Basis verprobter Annahmen aus der Use-Case-Design-Phase, aber auch der in Kapitel 2 aufgezeigten Annahmeverpflichtungen einer Versicherung, lassen sich eine Roadmap und Implementierungsstrategie für die EUDI-Wallet entwickeln.

Heute stehen Versicherungen für die Integration der EUDI-Technologie zahlreiche technische Komponenten am Markt zur Verfügung, die sie für die Implementierung ausschreiben und später nutzen können. Diese Partnerauswahl inkl. eventuell. notwendiger Implementierungsberatung unterstützt das Projektmanagement beim Aufsetzen der konkreten Implementierungsprojekte.

In den unterschiedlichen Rollen im eIDAS-Ökosystem der EUDI-Wallet ergeben sich als Relying Party (datenannehmende Stelle) und Issuer (datenabgebende Stelle) unterschiedliche Implementierungsvoraussetzungen. Gerade als Issuer werden Anforderungen an die Datenbereitstellung (z. B. als qualifizierte bzw. nicht qualifizierte Attribute) gestellt, die durch entsprechend zertifizierte Vertrauensdiensteanbieter gelöst werden.

Echte Mehrwerte bestehen aber für Versicherungen in ihrem Rollenwechsel als Issuer und Relying Party (siehe die in Kapitel 4 aufgezeigten Use Cases).

Ab 2028 wird es Versicherungen auch ermöglicht, selbst Wallet-Provider zu werden und damit ihren Kunden eine eigene EUDI-Wallet bzw. eine in ihre Bestands-App integrierte EUDI-Technologie anzubieten. Damit lassen sich Anwendungsfälle für den Nutzer noch einfacher gestalten, da somit ein Wechsel in die staatliche EUDI-Wallet-App (d-you) nicht mehr zwingend notwendig sein wird.

Roadmap und Implementierungsvorgehen benötigen einen schrittweisen Aufbau von technischem Know-how bzw. Expertise zur Integration in die Bestandssysteme. Der Aufbau dieses Know-how ist heute schon durch die Teilnahme an Initiativen, wie die der Sandbox der Common Codes GmbH (in ihrer Rolle als Bereitsteller für die staatliche EUDI-Infrastruktur), möglich.

6 Zusammenfassung und Schlussbemerkungen

Erwartete Weiterentwicklung der EUDI

Die Einführung der EUDI wird nicht in einem Schritt erfolgen. In einer ersten Phase werden walletbasierte Verfahren neben bestehenden Identifizierungs-, Signatur- und Nachweisprozessen stehen. Für Versicherer bedeutet das, dass neue Wallet-Prozesse zunächst in bestehende Kunden- und Bestandsprozesse integriert werden müssen, ohne etablierte Alternativen unmittelbar abzulösen. Besonders relevant wird daher die Fähigkeit, unterschiedliche Identitäts- und Nachweisverfahren über gemeinsame Schnittstellen zu orchestrieren.

Mit wachsender Verfügbarkeit von Wallets und digitalen Nachweisen dürfte sich der Schwerpunkt schrittweise verschieben. Versicherer werden nicht nur Nachweise von Kundinnen und Kunden entgegennehmen, sondern zunehmend prüfen, welche eigenen Nachweise sich standardisiert und maschinenlesbar ausstellen lassen. Dadurch kann sich die Rolle vom reinen Verifier, beziehungsweise Relying Party, hin zum Issuer und aktiven Teilnehmer eines europäischen Vertrauensökosystems erweitern.

Parallel dazu wird die technische Standardisierung weiter voranschreiten. Für die Unternehmen bleibt entscheidend, neue Wallet-Funktionen nicht als isolierte Lösung aufzubauen, sondern mit IAM, CRM, Bestands-, Portal- und Vermittlersystemen sowie bestehenden Vertrauensdiensten zu verbinden. Die in Kapitel 4 beschriebenen Use Cases zeigen, dass der konkrete Nutzen vor allem dort entsteht, wo Nachweise und Identitäten in bestehende Prozesse integriert werden.

Perspektivisch wird zudem das Zusammenspiel mit weiteren europäischen Identitäts- und Dateninfrastrukturen an Bedeutung gewinnen. Dazu können unter anderem Unternehmens- beziehungsweise Business-Wallets und weitere sektorübergreifende Nachweise gehören. Die konkrete Ausgestaltung und der Zeitpunkt einzelner Entwicklungen sind teilweise noch offen. Für Versicherer spricht dies dafür, technische und organisatorische Grundlagen so aufzubauen, dass neue Nachweisarten und Rollen schrittweise ergänzt werden können.

Grundsätzliche Handlungsempfehlungen für die Zukunft

Aus den beschriebenen Rollen, Use Cases und Rahmenbedingungen lassen sich für Versicherungsunternehmen einige grundsätzliche Schritte ableiten:

- Verantwortlichkeiten bündeln: Die EUDI-Wallet betrifft Fachbereiche, IT, Compliance, Datenschutz und Informationssicherheit. Versicherer sollten früh festlegen, wer die fachliche und technische Koordination übernimmt und wie Entscheidungen über Rollen, Daten und Schnittstellen getroffen werden.
- Betroffene Prozesse systematisch erfassen: Zunächst sollte geprüft werden, in welchen Kunden-, Vermittler- und Partnerprozessen Identifizierung, Authentisierung, Nachweise oder Signaturen heute relevant sind. Daraus lässt sich ableiten, wo regulatorischer Handlungsbedarf, Effizienzpotenziale oder neue Issuer-Rollen entstehen.
- Relying-Party- und Issuer-Rolle gemeinsam denken: Der kurzfristige Einstieg wird häufig über die Prüfung von PID und anderen Nachweisen erfolgen. Gleichzeitig sollte früh bewertet werden, welche eigenen Versicherungsnachweise sich für eine digitale Ausstellung eignen.
- Architektur modular vorbereiten: Wallet-Anbindungen sollten möglichst nicht als Einzellösungen pro Sparte entstehen. Sinnvoll ist eine wiederverwendbare Integrationsschicht für Identitätsprüfung, Nachweisvalidierung, Signaturen und Statusprüfung, die an bestehende IAM-, CRM-, Bestands- und Vermittlersysteme angebunden werden kann.
- Use Cases früh mit Nutzern verproben: Technische Machbarkeit allein reicht nicht. Gerade Wechsel zwischen App, Browser und Wallet, Datenfreigaben sowie Fehler- und Rückfallprozesse sollten früh prototypisch getestet werden.
- Übergangsphase mitdenken: Wallet-basierte Verfahren werden bestehende Verfahren ergänzen. Versicherer sollten daher alternative Identifizierungs- und Nachweiswege weiter vorsehen und definieren, wie Ergebnisse verschiedener Verfahren einheitlich dokumentiert und verarbeitet werden.
- Standards und Ökosysteme begleiten: Viele Nutzenpotenziale entstehen erst, wenn Nachweise, Rollen und Prüfprozesse branchenübergreifend abgestimmt sind. Für Versicherer ist es daher sinnvoll, die Entwicklung relevanter Standards, Rulebooks und sektorübergreifender Anwendungsfälle zu verfolgen und sich dort einzubringen, wo gemeinsame Branchenlösungen erforderlich sind.

Weiterführende Literatur

Durchführungsrechtsakte der Europäischen Kommission zur Umsetzung der EUDI-Wallet und des europäischen Rahmens für eine digitale Identität.

Europäische Kommission: European Digital Identity Wallet Architecture and Reference Framework (ARF), jeweils aktuelle Fassung.

OpenID Foundation: OpenID for Verifiable Credential Issuance (OpenID4VCI) und OpenID for Verifiable Presentations (OpenID4VP), jeweils aktuelle Fassung.

Verordnung (EU) 2024/1183 des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EU) Nr. 910/2014 hinsichtlich der Schaffung des europäischen Rahmens für eine digitale Identität (eIDAS 2.0).

Verordnung (EU) 2024/1624 des Europäischen Parlaments und des Rates zur Verhinderung der Nutzung des Finanzsystems für Zwecke der Geldwäsche oder der Terrorismusfinanzierung (AMLR).

Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates über die digitale operationale Resilienz im Finanzsektor (DORA).

Verordnung (EU) 2025/327 des Europäischen Parlaments und des Rates über den europäischen Raum für Gesundheitsdaten (EHDS).

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 700 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner/in
Lukas Spohr | Referent Digitale Transformation
T +49 30 27576-340 | l.spohr@bitkom.org

Verantwortliches Bitkom-Gremium
AK Digital Insurance & InsurTech
AK Digitale Identitäten

Autorinnen und Autoren
Allianz SE
Dominik Deimel | Wallet Experts GmbH
Luke Fraser Dunnet | Nect GmbH
Karl Grandl | Miss Moneypenny Technologies GmbH
Bernd Lohmeyer | Materna Information & Communications SE
Nils Merdian | R+V Versicherung AG
Per Meyerdierks | GSK Stockmann
Robert Musick | Swisscom AG

Copyright
Bitkom 2026

Diese Publikation stellt eine allgemeine unverbindliche Information dar. Die Inhalte spiegeln die Auffassung im Bitkom zum Zeitpunkt der Veröffentlichung wider. Obwohl die Informationen mit größtmöglicher Sorgfalt erstellt wurden, besteht kein Anspruch auf sachliche Richtigkeit, Vollständigkeit und/oder Aktualität, insbesondere kann diese Publikation nicht den besonderen Umständen des Einzelfalles Rechnung tragen. Eine Verwendung liegt daher in der eigenen Verantwortung des Lesers. Jegliche Haftung wird ausgeschlossen. Alle Rechte, auch der auszugsweisen Vervielfältigung, liegen beim Bitkom oder den jeweiligen Rechteinhabern.