

# EUDI-Wallet: Handlungsfelder und Einbindungsmöglichkeiten für Issuer-Banken

Oliver Maskus, Gral Glec, Mario Lang

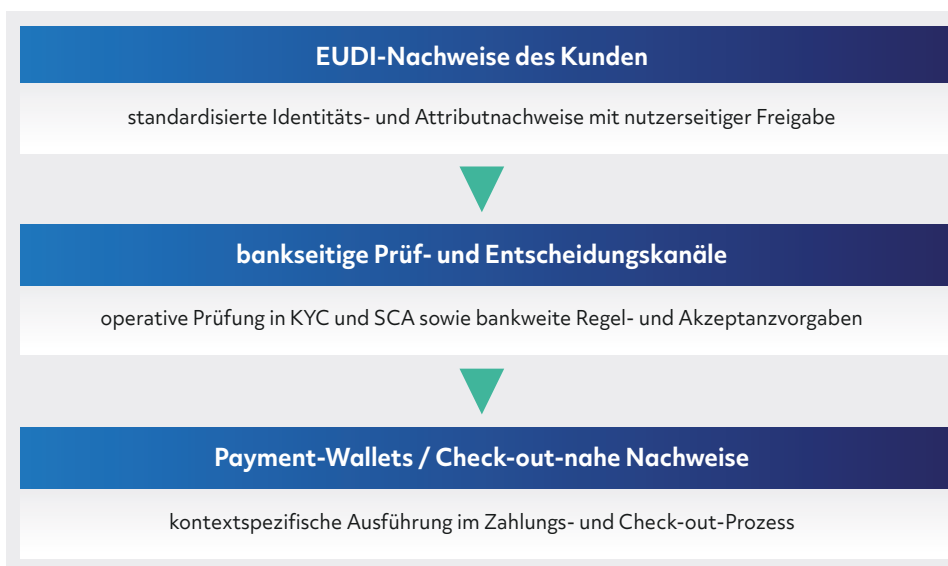
## Einleitung

Die EUDI-Wallet ist kein weiteres Wallet-Produkt, sondern der europische eIDAS-2.0-Rahmen fr digitale Identitt und digitale Nachweise. Fr Issuer-Banken liegt ihr Mehrwert in Prozessen, in denen heute Identitts- oder Berechtigungsprfungen aufwendig, manuell oder mehrfach durchgefhrt werden – insbesondere bei der Kontoerffnung, bei KYC-Aktualisierungen und bei der Zahlungsfreigabe im Onlinehandel. In diesen Anwendungsfllen ermglicht die EUDI-Wallet erstmals die Nutzung standardisierter, EU-weit interoperabler Nachweise, die vom Kunden kontrolliert freigegeben und von Banken prfbar verarbeitet werden knnen.<sup>1</sup> Gerade im volumenstarken KYC-Umfeld zeigt sich, dass EUDI-Wallet-Nachweise bereits bei sechsstelligen Fallzahlen Einsparpotenziale im Millionenbereich erschlieen knnen.

Der zentrale Aufwand fr Banken entsteht damit nicht durch eine zustzliche Kundenschnittstelle, sondern durch die bankweite Ausgestaltung von Integration, Governance und Betrieb dieser Nachweise. Dazu zhlt insbesondere die technische Anbindung an das EUDI-kosystem ber eine bankseitige Integrationsschicht, die Wallet-Nachweise entgegennimmt, validiert und in bankinterne Prf- und Entscheidungsprozesse berfhrt.<sup>2 3 4</sup>

### Nach der Lektüre sind drei Entscheidungen zu treffen:

1. Welche Rolle die Bank im EUDI-Ökosystem einnimmt und welche Use-Cases priorisiert werden.<sup>2 3</sup>
2. Welches bankweite Regelwerk für Attribute und Nachweise gilt (Zweckbindung, Aktualität, Widerruf, Ausnahmen, Auditierbarkeit).
3. Wie die Wallet-Landschaft geschnitten wird: Die EUDI-Wallet als standardisierter Nachweisrahmen, eine bankseitige Entscheidungs- und Nachweislogik und Payment-Wallets als Check-out-Schicht.



**Abbildung 1:** Drei-Ebenen-Logik – Einordnung der EUDI-Nachweise in bankseitige Prüf- und Entscheidungsprozesse

## Einordnung und Timeline

Mit dem europäischen Rechtsrahmen (eIDAS 2.0) ist die Richtung gesetzt. Digitale Identität und digitale Nachweise werden EU-weit standardisiert und angeboten. Für Banken folgt daraus keine Verpflichtung zur Bereitstellung einer eigenen EUDI-Wallet. eIDAS 2.0 adressiert öffentliche Stellen ebenso wie private Akteure wie Banken, Händler und Plattformen und etabliert einen sektor-übergreifenden Identitäts- und Nachweisstandard.<sup>1</sup>

Im EUDI-Ökosystem wird zwischen der Prüfung und der Ausstellung digitaler Nachweise unterschieden. Für Banken ist insbesondere die Rolle als prüfende Stelle von Bedeutung. In eigenen Prozessen wie Kontoeröffnung, KYC-Aktualisierung oder Authentifizierung im Onlinehandel fragt die Bank Nachweise an und entscheidet über deren Akzeptanz. In der Terminologie des EUDI-Rahmens tritt sie damit als Wallet-Relying-Party auf. Davon abzugrenzen ist die ausstellende Rolle. Attribut-Aussteller sind Stellen, die prüfbare Merkmale (Attribute), wie zum Beispiel das Alter, aus einem qualifizierten Nachweis bereitstellen. Dies sind insbesondere staatliche Stellen sowie privatwirtschaftliche Organisationen mit entsprechender Legitimation. Ob und in welchem Umfang Banken als Attribut Aussteller auftreten, ist regulatorisch festgelegt und an die Eintragung in nationale Register gebunden. Diese Register bestimmen, welche Wallet-Relying-Parties zugelassen sind und unter welchen Bedingungen Nachweise abgefragt werden dürfen.<sup>2 3</sup>

Die Umsetzung wird durch Implementing Acts und technische Spezifikationen konkretisiert. Ein zentraler Baustein ist die Registrierung von Wallet-Relying-Parties in nationalen Registern. Diese erfolgt über standardisierte Schnittstellen. Sicherheitsanforderungen werden so ausgestaltet, dass sie Grundlage formaler Zertifizierungsverfahren sind. Die EU-Agentur ENISA unterstützt die Zertifizierung der EUDI-Wallets und die Vorbereitung eines europäischen Cybersecurity-Zertifizierungsschemas.<sup>4</sup>

Deutschland plant die Einführung einer staatlichen Wallet für Anfang 2027.<sup>5</sup> Auf EU-Ebene soll bis 2026 mindestens eine Wallet-Version je Mitgliedstaat verfügbar sein.<sup>6</sup> Für Banken ergibt sich daraus ein zentrales Vorbereitungsfenster in den Jahren 2025 und 2026. Ein zusätzlicher Adoptionstreiber liegt außerhalb des Bankings. Dazu zählen insbesondere die aktuell in der Politik diskutierten Alters- und Zugangsnachweise.<sup>7</sup>

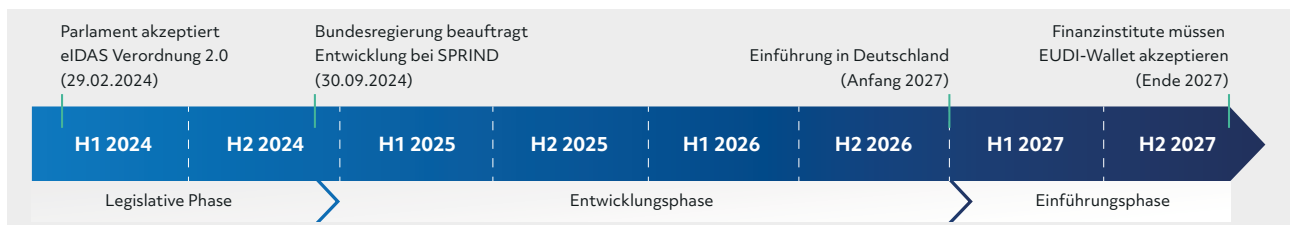


Abbildung 2: Timeline zur Einführung der EUDI-Wallet

## Warum Abwarten trügerisch ist

„Abwarten, bis alles final ist“ wirkt in großen Instituten zunächst plausibel. In der Praxis entstehen die teuersten Schleifen nicht durch offene Detailfragen, sondern durch späte Anpassungen an Governance, Budget und Betrieb.<sup>4</sup> Typische Fehlannahmen sind, dass alle relevanten Entscheidungen erst nach finaler Spezifikationsreife getroffen werden könnten.

### Gründe, warum Abwarten den Aufwand erhöht:

- Zeitdruck in der Umsetzungsphase: Rechtsrahmen und Umsetzungsregeln geben die Einführung vor.<sup>1</sup> Werden zentrale Entscheidungen verschoben, fallen sie unter erhöhtem Zeit- und Koordinationsdruck in der Umsetzung. Zudem findet die Umsetzung nicht isoliert zu anderen Projekten der Banken statt und muss im Gesamtkontext der Budgetplanung berücksichtigt werden.
- Ungeklärte Rollen im EUDI Ökosystem: Die EUDI-Wallet ist ein Rollen-ökosystem aus Ausstellern von Nachweisen und Wallet-Relying-Parties.<sup>2</sup> Bankrollen ergeben sich nicht automatisch aus bestehenden Prozessen, sondern müssen bewusst festgelegt werden, um Zuständigkeiten eindeutig zuzuordnen.
- Register als früh wirksame Vorgaben: Register und Registrierung sind staatliche Vorgaben.<sup>3</sup> Sie bestimmen, wie eine Bank als Wallet-Relying-Party identifiziert wird und unter welchen Bedingungen EUDI-Wallet-Nachweise abgefragt werden können.
- Zertifizierung und Sicherheitsanforderungen als strukturelle Rahmenbedingungen: Zertifizierungs- und Sicherheitsanforderungen wirken von Beginn an als verbindliche Rahmenbedingungen. Sie beeinflussen frühzeitig Budget, Governance- und Betriebsentscheidungen. Werden sie erst später berücksichtigt, sind Anpassungen an Nachweisführung und Kontrollen kostspielig.<sup>4</sup>
- Koexistenz und Übergänge im Betrieb: EUDI wird in bestehende Verfahren integriert. Fehlende Übergänge zwischen bestehenden Verfahren führen dabei früh zu strukturellem Mehraufwand.

### Beispiel für einen frühen Einstieg:

Kontoeröffnung und KYC-Prüfung sind naheliegende Startpunkte. Identitäts- und Nachweisprozesse sind dort streng reguliert und operativ aufwendig. Welche wirtschaftlichen Effekte sich aus dem Einsatz der EUDI-Wallet ergeben können, zeigt exemplarisch der Use-Case KYC.

# Use-Case 1: KYC und Kontoeröffnung

## Ausgangslage: KYC-Prüfung und Nachweislogik

Kontoeröffnung und KYC-Prüfung bündeln Identitäts- und Nachweislogik, zum Beispiel bei der Identifizierung eines Neukunden oder der Aktualisierung eines Ausweisdokuments. Diese Prozesse sind bankseitig durch definierte Prüf- und Dokumentationsanforderungen abgesichert. Das gilt für Neukunden ebenso wie für Aktualisierungen im Bestand.

In der heutigen Praxis wird der Nachweis häufig über manuelle Verfahren beschafft, beispielsweise durch Video-Ident. Dort werden Informationen, wie Name, Geburtsdatum oder Wohnsitz erhoben, bewertet, dokumentiert und bei Bedarf nachbearbeitet. Hierdurch entstehen erhebliche Kosten und operativer Aufwand für Banken. Diese manuellen Verfahren sind fehleranfällig und zugleich steigt das Risiko durch Identitätsmanipulationen, etwa durch Deep Fakes. Die EUDI-Wallet adressiert diese Bruchstelle, indem Identitätsdaten und Attributsmerkmale als standardisierte, prüfbare Nachweise bereitgestellt werden.<sup>2</sup> Dadurch verändert sich die Nachweisbeschaffung grundlegend.

## Trennlinie: Nachweis und Entscheidung

Zentral ist ein bankseitiges Attribut-Regelwerk, da Nachweise über die EUDI-Wallet standardisiert bereitgestellt und einheitlich bewertet werden müssen. Es definiert, welche Attribute in welchen Prozessen akzeptiert werden. Zudem legt es fest, welche Anforderungen an Aktualität und Gültigkeit gelten und wann zusätzliche Kontrollen erforderlich sind.

Für die Bank verschiebt sich damit die Verantwortung von der operativen Erhebung hin zur Steuerung von Prüflogik, Ausnahmen und Nachweisführung. Die fachliche Entscheidung über die Akzeptanz eines Nachweises verbleibt bankseitig, während die technische Bereitstellung der Attribute über die Wallet erfolgt. Kontrollen erforderlich sind.

## Umsetzung und Betriebsvoraussetzungen

KYC-Prozesse auf Basis der EUDI-Wallet sind nur dann skalierbar, wenn Prüfungsergebnisse revisionssicher nachvollziehbar bleiben. Dafür sind definierte Nachweise und Dokumentationen erforderlich. Diese müssen vor einer Nutzung über mehrere Prozesse hinweg festgelegt sein.<sup>4</sup> Dazu zählen Zielprozesse für Neukunden und Bestandsaktualisierung, ein versioniertes Attribut-Regelwerk, ein Logging-Konzept zur revisionssicheren Nachvollziehbarkeit, definierte Ausnahmewege sowie eine eindeutig prüfbare Checkliste.

Der operative Aufwand verlagert sich dabei von manuellen, fallbasierten Prüfungen hin zu standardisierten und überwiegend maschinellen Prüfprozessen. Dies reduziert nicht nur die Bearbeitungszeit je Kontoeröffnung. Es wirkt sich auch unmittelbar auf die operativen Kosten aus. Abbildung 3 stellt diesen Effekt anhand eines Vergleichs heutiger Verfahren mit einer Umsetzung auf Basis der EUDI-Wallet dar.

KPI	Heute	mit EUDI-Wallet	Effekt
<b>manueller Aufwand pro Fall (Bank)</b>	15 bis 25 Minuten	3 bis 8 Minuten	-55 % bis -80 %
<b>Durchlaufzeit</b>	1 bis 3 Tage	15 bis 60 Minuten	-70 % bis -90 %
<b>Fehler- / Rückfragenquote</b>	20 % bis 30 %	2 % bis 8 %	-70 % bis -90 %
<b>OPEX pro Kontoeröffnung</b>	18 € bis 35 €	7 € bis 15 €	-40 % bis -60 %

Abbildung 3: Kontoeröffnung mit KYC-Prüfung im Vergleich

### Einordnung des Potenzials (Szenario):

Abbildung 3 weist für die Kontoeröffnung mit KYC-Prüfung eine Reduktion der operativen Kosten von 18-35 € auf 7-15 € je Vorgang aus.<sup>8</sup> Daraus ergibt sich eine Einsparung von rund 10-20 € pro Kontoeröffnung. Bereits bei 100.000 KYC-Vorgängen entspricht dies einem Einsparpotenzial von etwa 1-2 Mio. €. Mit steigenden Volumina wächst dieser Effekt linear und erreicht bei großen Retail-Instituten schnell einen zweistelligen Millionenbetrag. Der wirtschaftliche Hebel der EUDI-Wallet liegt damit nicht im einzelnen KYC-Vorgang, sondern in der Skalierung standardisierter Nachweis- und Entscheidungslogiken über hohe Fallzahlen hinweg.

## Use-Case 2 – Zahlungsfreigabe (SCA/3DS)

### Ausgangslage: SCA im Online-Payment aus Bankensicht

Im Onlinehandel ist die starke Kundenauthentifizierung (SCA) als regulatorischer Standard zur Betrugsprävention etabliert und wird in der Praxis überwiegend über EMV® 3D Secure (3DS) umgesetzt. Abhängig vom Risikoprofil einer Transaktion entscheidet die Issuer-Bank, ob eine Zahlung ohne aktive Kundeneingabe erfolgen kann oder ob eine zusätzliche Freigabe erforderlich ist.

Diese Freigaben werden heute häufig über bankeigene Authentifizierungskanäle realisiert, etwa durch App-to-App-Freigaben oder push-basierte TAN-Verfahren. Für Issuer-Banken entsteht daraus ein Spannungsfeld: Zusätzliche Authentifizierungsschritte erhöhen die Sicherheit, führen jedoch zu zusätzlicher Reibung im Check-out und wirken sich negativ auf Abschlussquoten aus, während reibungsarme Prozesse mit erhöhtem Betrugsrisiko einhergehen.<sup>9</sup>

Die EUDI-Wallet adressiert dieses Spannungsfeld durch eine standardisierte, EU-weit interoperable Freigabe, die Identität, Gerät und transaktionsbezogene Zustimmung bindet und europaweit bankenübergreifend einsetzbar macht.

### Einbindung der EUDI-Wallet: Ergänzung statt Ersatz für 3DS

Die EUDI-Wallet ersetzt bestehende SCA-Verfahren nicht, sondern erweitert den technischen Rahmen für die Nutzung standardisierter, interoperabler Authentifizierungsergebnisse.<sup>10</sup> Aus dem eIDAS-2.0-Rechtsrahmen folgt für Issuer-Banken keine Verpflichtung, die EUDI-Wallet als eigenen Freigabe- oder Authentifizierungskanal zu betreiben oder in bestehende Bank-Apps zu integrieren.<sup>1</sup> Davon zu unterscheiden ist die Akzeptanz von Authentifizierungsergebnissen aus der EUDI-Wallet. Diese ist erforderlich, wenn der Kunde bei einer zusätzlichen starken Kundenauthentifizierung verlangt, dass die EUDI-Wallet genutzt werden soll. An dieser Stelle darf die Issuer-Bank deren Einsatz nicht pauschal ausschließen und ist gehalten, entsprechende Wallet-basierte Ergebnisse zu akzeptieren (s. Abbildung 4).

Die konkrete technische Einbindung liegt somit im Gestaltungsspielraum der Bank. Dies kann etwa innerhalb bestehender 3DS-Flows erfolgen oder über eine angebundene, vom bankeigenen Kanal entkoppelte Wallet-Interaktion. Maßgeblich ist die Fähigkeit der Bank, die Ergebnisse der Wallet-basierten Authentifizierung SCA-konform zu verarbeiten, revisionsicher zu dokumentieren und im Streitfall nachvollziehbar nachzuweisen. Payment-Wallets im Check-out (z. B. Apple Pay, Google Pay, Wero) sind hiervon abzugrenzen und werden in diesem Use-Case nicht betrachtet.

### Vorgehen: Pilotierung in 3DS-Flows

Ein Pilot in ausgewählten 3DS-Flows bietet einen geeigneten Einstieg, um Integrationsfähigkeit, Betriebsstabilität und Nachweisführung der EUDI-Wallet unter realen Bedingungen zu erproben, bevor sie in den bankseitigen Regelbetrieb überführt wird. Besonders geeignet sind Flows, in denen Issuer Banken bereits heute aktiv über Auslösung und Ausgestaltung der Authentifizierung entscheiden. Der Nutzen einer Pilotierung liegt in der frühzeitigen Absicherung der bankseitigen Betriebs- und Nachweisfähigkeit vor einer Skalierung.

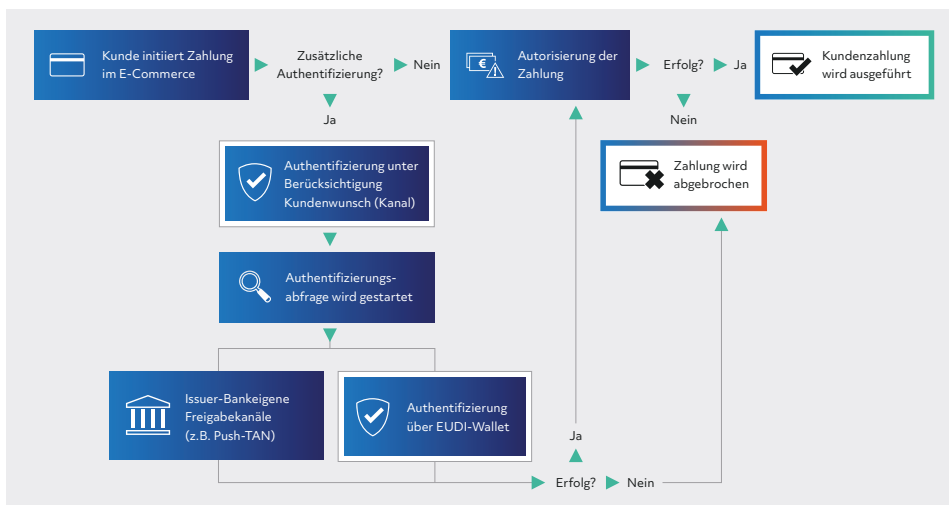


Abbildung 4: Swim-Lane – EUDI-Wallet im 3DS-Flow

## Use-Case 3 – Check-out-nahe Nachweise

### Ausgangslage: Prüfpflichten im Check-out

Alters- und Berechtigungsnachweise sind im Check-out heute häufig uneinheitlich umgesetzt. Dazu zählen das Ausfüllen von Formularen, der Upload von Ausweisdokumenten oder externe Prüfungen, die ein Kunde durchlaufen muss. Diese Verfahren führen zu zusätzlichen Interaktionsschritten und erhöhen die Abbruchwahrscheinlichkeit im Check-out.<sup>9</sup>

Mit der EUDI-Wallet steht ein EU-weit harmonisierter Mechanismus zur Verfügung, um qualifizierte Nachweise standardisiert und zustimmungsbasiert bereitzustellen. Für Issuer-Banken ist in diesem Kontext entscheidend, dass Rollen und Verantwortlichkeiten eindeutig zugeordnet sind. Insbesondere muss nachvollziehbar bleiben, wer berechtigt ist, einen Nachweis abzufragen, wer ihn prüft und wer die Verantwortung trägt, falls ein Prüfergebnis später bestritten wird.<sup>1</sup>

### Trennlinie: Nachweis und Zahlungsausführung

Im Check-out rückt neben dem Prinzip der Datenminimierung (Minimal Disclosure) die zeitliche Entkopplung von Nachweisprüfung und Zahlungsfreigabe in den Vordergrund. Bestimmte Attribute des Kunden können bereits im Check-out durch den Händler oder den angebundenen Zahlungsdienstleister geprüft werden, bevor eine Zahlungsfreigabe ausgelöst wird. Minimal Disclosure basiert technisch auf Selective Disclosure, also der gezielten Offenlegung einzelner Attribute aus einem qualifizierten Nachweis. Die EUDI-Wallet ist darauf ausgelegt, solche Attribute standardisiert, zustimmungsbasiert und prüfbar bereitzustellen. Die Zahlungsausführung und deren Authentifizierung erfolgen davon unabhängig in den etablierten Authentifizierungsflüssen.<sup>2</sup>

### Rollen im Check-out-Ablauf

Im Check-out wirken Händler, PSP und Wallet-Relying-Parties zusammen, da Kundennachweise kontextabhängig von unterschiedlichen berechtigten Stellen geprüft werden können. Die Nachweisprüfung übernimmt eine eigenständige Gate-Funktion im Check-out-Ablauf (s. Abbildung 5) und entscheidet über dessen Fortsetzung.<sup>7</sup> Für Kunden ist dieser Ansatz dann von Bedeutung, wenn die Nachweisprüfung gegenüber bestehenden Verfahren keine zusätzlichen Interaktionsschritte erfordert. Händler profitieren in diesen Fällen von stabileren Check-out-Abläufen und besseren Abschlussquoten.<sup>11</sup>

Für Issuer-Banken ergibt sich daraus in der Regel keine unmittelbare operative Rolle im Check-out. Ihre Aufgabe liegt in der bankweiten Festlegung von Akzeptanz- und Kontrollanforderungen für banknahe Nachweisketten, insbesondere in Bezug auf Zweckbindung, Gültigkeit, Widerruf und Nachvollziehbarkeit, ohne im Check-out selbst operativ zu wirken. Die bankseitige Zahlungs- und 3DS-Governance bleibt davon in ihrer Struktur unberührt.

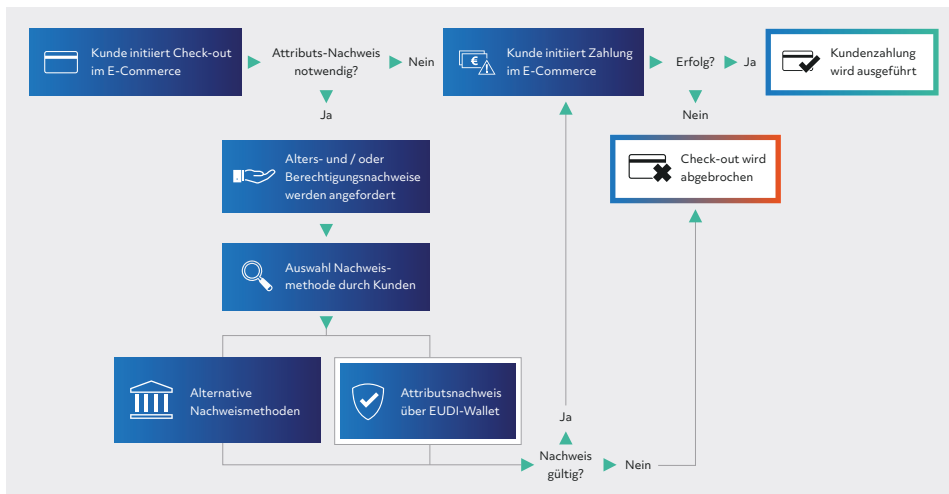


Abbildung 5: Swim Lane – Check-out-nahe Nachweise (Händler/PSP)

## Ableitung: Muster und Konsequenzen

### Wiederkehrende Muster über alle Use-Cases

Über alle Use-Cases hinweg zeigt sich: Integrationspunkte, revisions sichere Nachweisführung und bankweiter Betrieb sind die entscheidenden Stellhebel.<sup>4</sup> Erst durch diese Zusammenführung werden Identität, Nachweise und Zustimmung zu einer operativ wirksamen, skalierbaren Fähigkeit.

Die drei Use-Cases verdeutlichen dieses Muster aus unterschiedlichen Perspektiven:

1. Im KYC liegt der Engpass nicht im Nachweis selbst, sondern in Bewertung, Aktualität und Dokumentation.
2. In der SCA entscheidet nicht die zusätzliche Benutzerinteraktion, sondern Gerätebindung, Wiederherstellung und eine transaktionsbezogene Zustimmung, die im Disput belegbar bleibt.

3. Im Check-out rückt neben Minimal Disclosure eine durchgängige Nachweis-Prozesskette mit eindeutigen Zuständigkeiten in den Vordergrund.

**Zusammengeführt zeigen diese Beobachtungen:** Der Einsatz der EUDI-Wallet wird für Banken dort wirksam, wo bankseitige Entscheidungs-, Ausnahme- und Nachweislogiken einheitlich definiert und über mehrere Prozesse hinweg konsistent angewendet werden.

### Operating Model und notwendige Umsetzungsentscheidung

Voraussetzung für eine konsistente Nutzung der EUDI-Wallet über mehrere Prozesse hinweg ist ein eindeutiges bankweites Operating Model. Die Bank muss festlegen, nach welchen Regeln EUDI-Wallet-Nachweise akzeptiert, bewertet und dokumentiert werden und wie diese Entscheidungen in die bestehenden Prüf- und Kontrollmechanismen eingebettet sind.<sup>2 3</sup>

Zentrale Elemente dieses Operating Models sind ein bankweites Attribut-Regelwerk, klare Vorgaben zu Zweckbindung, Gültigkeit und Widerruf sowie eine revisions sichere Dokumentation der Prüfergebnisse.<sup>4</sup>

Ein tragfähiger Ansatz zur EUDI-Nachweisfähigkeit besteht darin, dass Banken die nationale EUDI-Wallet als Quelle standardisierter Nachweise nutzen und diese in ihre bankweiten Prüf- und Entscheidungsprozesse integrieren. Check-out- und Zahlungsflüsse bleiben davon getrennt und werden weiterhin über bestehende Händler- und PSP-Infrastrukturen abgewickelt. Dadurch können Banken Prüf- und Entscheidungslogiken vereinheitlichen, prozessspezifische Sonderlösungen abbauen und operative Komplexität über KYC-Prozesse, Zahlungsfreigaben und Check-out-nahe Nachweise hinweg reduzieren.<sup>1 2</sup>

Aus dem Operating Model ergibt sich damit die Notwendigkeit, Nachweis- und Entscheidungsfähigkeit unabhängig von konkreten Interaktions-, Check-out- oder Authentifizierungskanälen auszugestalten. Während Auslösung und Nutzerinteraktion je nach Prozess variieren können, müssen Akzeptanz-, Prüf- und Dokumentationslogik bankweit konsistent bleiben.<sup>4</sup>

## Technischer Anschluss an das EUDI-Ökosystem

Unabhängig von der fachlichen Rollenentscheidung stellt sich für Issuer-Banken frühzeitig die Frage, wie der technische Anschluss an das EUDI-Ökosystem konkret ausgestaltet wird. Der regulatorische Rahmen definiert Rollen, Schnittstellen und Sicherheitsanforderungen, nicht jedoch die technische Bankenarchitektur.<sup>2 3</sup> In der Praxis erfolgt die Anbindung daher nicht direkt aus einzelnen Fachprozessen, sondern über eine zentrale Anbindung der Bank an das EUDI-Ökosystem (im Folgenden: EUDI-Connector) als vermittelnde Schicht zwischen Wallet-Ökosystem und bankinternen Prüf- und Entscheidungsprozessen.

Der EUDI-Connector ist keine regulatorische Vorgabe, sondern eine bewusste Architekturentscheidung der Bank. Er bündelt die Anbindung der Bank in ihrer Rolle als Wallet-Relying-Party an die EUDI-Wallets und stellt die standardisierte Entgegennahme und technische Validierung Wallet-basierter Nachweise sicher.<sup>2</sup> Fachliche Prüf-, Akzeptanz- und Dokumentationsentscheidungen werden dadurch von der konkreten Ausprägung einzelner Wallet-Implementierungen entkoppelt und in bankseitigen Entscheidungs- und Kontrolllogiken verankert.

Für Issuer-Banken ergeben sich dabei grundsätzlich zwei Umsetzungsoptionen: die Nutzung eines extern bereitgestellten EUDI-Connectors als Produkt oder Plattformleistung oder der Aufbau eines bankinternen Connectors als Bestandteil der eigenen Zielarchitektur. Beide Ansätze sind fachlich gleichwertig, unterscheiden sich jedoch deutlich hinsichtlich Integrationsaufwand, Betriebsverantwortung und langfristiger Skalierungsfähigkeit.

Unabhängig vom gewählten Modell ist entscheidend, dass der EUDI-Connector als bankweite Fähigkeit verstanden wird. Eine isolierte Umsetzung pro Use-Case oder Fachbereich führt zu mehrfachen Integrationen und inkonsistenter Nachweisverarbeitung. Da EUDI-Wallet-Nachweise perspektivisch in mehreren Prozessen genutzt werden, bildet der Connector einen zentralen Baustein für eine konsistente und skalierbare Nutzung der EUDI-Wallet über KYC-Prozesse, Zahlungsfreigaben und Check-out-nahe Anwendungsfälle hinweg.<sup>4 12</sup>

## Koexistenz von Wallets und Kanälen als bankweite Integration

Vor diesem Hintergrund ist entscheidend, wie die EUDI-Wallet als bankweite Nachweisfähigkeit je Anwendungsfall wirkt und klar von Payment- und Authentifizierungskanälen abgegrenzt wird (s. Abbildung 6).<sup>2 12</sup>

Die dargestellte Drei-Ebenen-Logik (s. Abbildung 1) erfordert einheitliche Prüf- und Entscheidungsregeln, auch wenn Authentifizierung, Freigabe und Zahlung über unterschiedliche Kanäle erfolgen. Voraussetzung hierfür ist eine bankweit konsistente Anbindung der EUDI-Wallet an die internen Prüf- und Entscheidungsprozesse, unabhängig vom auslösenden Kanal.<sup>6</sup>

Die Wallet-Landschaft organisiert sich dabei in drei Ebenen: bankeigene Kanäle für Authentifizierung und Freigaben, Payment-Wallets im Check-out und die EUDI-Wallet für Identifikation und Nachweise. Der EUDI-Connector bildet die verbindende Integrationsschicht, über die Wallet-basierte Nachweise kanalunabhängig verarbeitet werden.<sup>2 12</sup>

Fall	EUDI relevant?	Begründung	Wer entscheidet?
Kontoeröffnung mit KYC-Prüfung	✓	Identitäts- und Attributsnachweise, nicht Payment-SCA	Bank
KYC-Abfrage (Aktualisierung der Bestandsdaten)	✓	Identitäts- und Attributsnachweise, nicht Payment-SCA	Bank
Online-Banking (Überweisung)	✓ / ✗	Optionale, bankseitige Authentifizierung; keine eIDAS-Pflicht	Bank
E-Commerce ohne SCA	✗	Keine SCA angefordert	Bank
E-Commerce mit 3DS-Challenge	✓	EUDI als Authentifizierung innerhalb 3DS nutzbar	Bank; Kunde nur als Ausführer der Challenge
Provisionierung einer digitalen Karte	✓ / ✗	Optionale, bankseitige Authentifizierung; keine eIDAS-Pflicht	Bank
Point of Sale	✗	kein 3DS	Gerät / Wallet
Kundennachweise im Check-out (händlerinitiiert)	✓	Check-out-nahe Nachweisprüfung, getrennt von Freigabe	Händler (Relying Party)

Abbildung 6: Einordnung der EUDI-Wallet-Relevanz nach Anwendungsfall

# Vorgehenslogik für Issuer-Banken und Ausblick

## Vorgehenslogik: erst Rahmen, dann Use-Case-Priorisierung

Auf dieser Basis empfiehlt sich für Issuer-Banken folgendes Vorgehen:

1. Rollenbild und Zielbild definieren: Wallet-Relying-Party-Rolle, Attribut-Rolle, Scope je Use-Case<sup>2 3</sup>
2. Regelwerk festlegen: Bankweites Attribut-Regelwerk, Aktualität, Widerruf, definierte Ausnahmen, Logging- und Nachweiskonzept<sup>4</sup>
3. Pilotieren entlang vorhandener Protokolle: Nutzung vorhandener 3DS-Flows zur Validierung von Integrations- und Nachweisfähigkeit<sup>10</sup>
4. Skalieren als Fähigkeit: Wiederverwendbare Bausteine für weitere Nachweise und Prozessstrecken<sup>2</sup>

Dieses Vorgehen stellt sicher, dass EUDI-Wallet-Fähigkeiten nicht punktuell eingeführt, sondern von Beginn an als skalierbarer Bestandteil der bankweiten Prozess- und Systemlandschaft etabliert werden.

## Ausblick: Basisschicht heute, Automatisierung später

Weitergehende Automatisierung im Sinne von Agentic Commerce ist ein späterer Ausbauschnitt. Sie setzt voraus, dass Nachweise und Zustimmung standardisiert, maschinenlesbar und prüfbar vorliegen. Sind diese Grundlagen etabliert, eröffnen sich für Banken perspektivisch weitergehende Automatisierungsmöglichkeiten.

# Literaturverzeichnis

## 1. EUR-Lex: Regulation (EU) 2024/1183

Rechtsrahmen zur Etablierung des European Digital Identity Frameworks

## 2. Europäische Kommission: The European Digital Identity Wallet – Architecture and Reference Framework (ARF)

Referenzrahmen für interoperable Wallet-Lösungen

## 3. EUR-Lex: Regulation (EU) 2025/848

Registrierung von Wallet-Relying-Parties und nationale Register im Rahmen des European Digital Identity Frameworks

## 4. ENISA: EU Digital Identity Wallet: A leap towards secure and trusted electronic identification through certification (Press Release, 24.09.2024)

Zertifizierungsunterstützung und Vorbereitung eines europäischen Zertifizierungsschemas

## 5. Bund (BMDS): EUDI-Wallet

Nationales Projekt und Einordnung; Planung zur Einführung in Deutschland

## 6. Europäische Kommission: EU Digital Identity Wallet Home

Zielbild zur Verfügbarkeit mindestens einer Wallet-Version je Mitgliedstaat bis 2026

## 7. Europäische Kommission: Blaupause für eine Altersüberprüfungslösung zum Schutz von Minderjährigen im Internet

Datenschutzschonende Altersverifikation und Minimal-Disclosure-Ansatz

## 8. Paperfly: eIDAS 2.0 & EUDI-Wallet – Vorbereitung für Banken

Fachbeitrag zur operativen Vorbereitung von Banken auf eIDAS-2.0, Wallet-Integration und Pilotierung in bankrelevanten Prozessen

## 9. Baymard Institute: Cart & Checkout Usability Research

Empirische Analysen zu Check-out-Reibung, Nutzerverhalten und Abbruchquoten im Onlinehandel

## 10. EMVCo: EMV® 3-D Secure White Paper – Use of the EUDI Wallet in EMV® 3-D Secure Payment Authentication, Version 1.0, June 2025, EMVCo, LLC.

## 11. PlainSignal: Check-out Conversion Rate

Definition, Messlogik und Bedeutung der Abschlussquote im Check-out-Kontext

## 12. Mobey Forum: Mapping the Business Case: Banks and the European Digital Identity Wallet

Strategische Analyse zu Rollen, Operating Models und Integrationsansätzen europäischer Banken

## PPI AG

Die PPI AG ist spezialisiert auf Softwareprodukte, Consulting sowie Services im Bereich Zahlungsverkehr (ZV) und Marktführer für EBICS- und FinTS-Lösungen. Mit der TRAVIC-Suite-Produktfamilie bietet PPI die komplette ZV-Verarbeitungskette für Banken aus einer Hand – von der Kunde-Bank-Schnittstelle über die ZV-Kernverarbeitung bis zur Interbankenkommunikation. Entsprechend den Kundenanforderungen stellt PPI die Payment-Lösungen on-Premises oder als Service mit Betrieb in der Cloud zur Verfügung.

Das Beratungsangebot von PPI umfasst sowohl die strategische und bankfachliche Beratung als auch das IT-Consulting mit ZV-Bezug. Dabei berät PPI die Kunden unter anderem in den Themen Cross-Border- und High-Value-Payments, SEPA, Instant Payments, Request to Pay, Cards sowie Next Generation Payments. Als stabil wachsende Aktiengesellschaft in Familienbesitz verfügt PPI über mehr als 40 Jahre Erfahrung in der Finanzbranche und beschäftigt heute rund 900 Mitarbeiter, davon über 250 im Bereich Zahlungsverkehr. Neben ihrem Hauptsitz in Hamburg hat PPI fünf weitere Standorte in Deutschland sowie drei internationale Niederlassungen in der Schweiz, Frankreich und Italien.

## Ansprechpartner



Oliver Maskus  
Senior Manager  
+49 160 8046448  
Oliver.Maskus@ppi.de



Gural Gülec  
Consultant  
+49 175 6350233  
Gural.Guelec@ppi.de



Mario Lang  
Partner  
+49 151 16471842  
Mario.Lang@ppi.de

PPI AG  
Moorfuhrweg 13  
22301 Hamburg  
www.ppi-group.eu