

Elektronische Gesundheitskarte und Telematikinfrastruktur

Grobkonzept Digitale Leistungserbringer- identitäten (eID-LE) und Signaturen

Version:	1.0.0_CC2
Revision:	1682916
Stand:	05.08.2026
Status:	zur Abstimmung freigegeben
Klassifizierung:	öffentlich_Entwurf
Referenzierung:	gemKPT_eID-LE

Dokumentinformationen

Gender-Hinweis

Aus Gründen der besseren Lesbarkeit wird in diesem Dokument überwiegend die männliche Form verwendet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

Änderungen zur Vorversion

Es handelt sich um eine Erstveröffentlichung.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0_CC	01.02.2026		Initiale Version	gematik
1.0.0_RC	31.03.2026		Kommentierung der Gesellschafter	gematik
1.0.0_CC2	05.08.2026		Konsolidierung strategischer Eckpunkte	gematik

Inhaltsverzeichnis

1 Einleitung.....	5
1.1 Einordnung des Dokuments.....	5
1.2 Ausgangssituation.....	6
1.3 Motivation.....	6
1.4 Übergreifende Anforderungen.....	7
2 Management Summary.....	9
2.1 Ausgangssituation.....	9
2.2 Lösung.....	9
3 Konzeptionelle Umsetzung eID-LE.....	12
3.1 Rechtliche Anforderungen.....	12
3.2 Fachliche Anforderungen.....	13
3.2.1 Strukturbedingte Schmerzpunkte.....	13
3.2.2 Schmerzpunkte nach Anwendungsumgebungen.....	14
3.2.3 Anforderungen.....	14
3.3 Umsetzung eID-LE mittels Wallet-Adapter.....	15
3.3.1 Systemüberblick.....	16
3.3.1.1 Akteure und Rollen.....	16
3.3.1.2 Komponenten und Dienste.....	17
3.3.2 Nutzung der digitalen Identität.....	18
3.3.2.1 Vorbedingungen:.....	18
3.3.2.2 Interaktionsübersicht.....	18
3.3.2.3 Praktische Aspekte in der Nutzung der digitalen Identität.....	19
3.3.3 Nutzung der digitalen Identität im Kontext der LEI.....	19
3.3.3.1 Systemüberblick.....	19
3.3.3.2 Interaktionsübersicht:.....	21
3.3.4 Nutzung der kartengebundenen Identität (HBA).....	21
3.3.4.1 Systemüberblick.....	21
3.3.4.2 Interaktionsübersicht.....	22
4 Konzeptionelle Umsetzung (Fern-)Signatur.....	23
4.1 Rechtliche Grundlagen.....	23
4.2 Fachliche Anforderungen.....	23
4.2.1 Strukturbedingte Schmerzpunkte.....	23
4.2.2 Schmerzpunkte nach Anwenderumgebung.....	23
4.2.3 Anforderungen.....	24
4.3 Umsetzung (Fern-)Signaturdienst.....	25
4.3.1 Systemüberblick.....	25
4.3.2 Interaktionsübersicht:.....	26
5 Planung benötigter Produkte und Dienste.....	28

82	5.1 eID-LE: Wallet-Adapter mit VC-Provisionierung.....	28
83	5.2 (Fern-)Signaturdienst.....	29
84	6 Weiterführende Klärung und thematische Abgrenzung.....	31
85	6.1 Weiterführende Klärungsbedarfe.....	31
86	6.1.1 Rolle der Attributsbestätigenden Stellen und des Wallet Adapters.....	31
87	6.1.2 Machbarkeit der Komfort-Fernsignatur.....	31
88	6.1.3 BYOD.....	32
89	6.1.4 Signaturfunktion des HBA.....	32
90	6.1.5 Verschlüsselungsfunktion des HBA.....	32
91	6.2 Thematische Abgrenzung.....	32
92	6.2.1 Digitale Institutionsidentitäten (SMC-B).....	32
93	6.2.2 Protokollierung.....	33
94	7 Anhang A - FAQ: Weiterführende Aspekte der eID-LE.....	35
95	8 Anhang B - Verzeichnisse.....	39
96		
97		

1 Einleitung

1.1 Einordnung des Dokuments

Das vorliegende Grobkonzept „*Digitale Leistungserbringeridentitäten (eID-LE) und Signaturen*“ schafft eine Grundlage für die in § 340 Abs. 6 SGB V geforderte Einführung von digitalen Identitäten für Leistungserbringer.

Hierzu werden strategische Fragestellungen rund um die Weiterentwicklung der Leistungserbringeridentitäten und Signaturerstellung unter Berücksichtigung der bald verfügbaren Europäischen digitalen Identitäts-Wallet (EUDI-Wallet) beantwortet. Kern der im Konzept dargestellten Lösung ist die Bereitstellung der digitalen Leistungserbringeridentität eID-LE als dezentrale EUDI-Wallet basierte Identität, welche ergänzend zum Heilberufsauseis (HBA) eingeführt wird („HBA auf dem Smartphone“). Der zweite Teil des Konzepts diskutiert die Umsetzung eines (Fern-)Signaturdienstes, da die Modernisierung der Signaturen und deren Entkopplung von physischer Hardware zwangsweise mit den digitalen Identitäten verknüpft ist. Dies gilt als wesentlicher Schritt, um den Einboxkonnektor als Signaturerstellungsanwendung bis 2030 ablösen zu können. Im Fokus stehen insbesondere die Architektur sowie die Beschreibung und Bewertung der notwendigen Komponenten und Dienste. Das Grobkonzept benennt darüber hinaus Punkte rund um die Integration der EUDI-Wallet, die sich in Klärung befinden oder mit den Gesellschaftern der gematik und weiteren relevanten Stakeholdern entschieden und ausgestalten werden sollen.

Das Dokument gliedert sich in sechs Kapitel, die gemeinsam einen strukturierten Überblick über die konzeptionelle Ausgestaltung der eID-LE und begleitender Verfahren bieten:

- **Kapitel 1** führt in den Gesamtkontext ein und beschreibt Zielsetzung sowie Rahmenbedingungen.
- **Kapitel 2** fasst die Kernaussagen des Konzeptes als Management Summary zusammen.
- **Kapitel 3** behandelt die konzeptionelle Umsetzung der eID-LE, einschließlich der rechtlichen Grundlagen und der fachlichen Anforderungen.
- **Kapitel 4** widmet sich der konzeptionellen Ausgestaltung der (Fern-)Signatur und stellt Rechtsgrundlagen und fachliche Anforderungen dar.
- **Kapitel 5** beschreibt die Planung der für die eID-LE und den neuen (Fern-)Signaturdienst benötigten Dienste, einschließlich Zeit- und Migrationsplanung zur schrittweisen Einführung.
- **Kapitel 6** adressiert weiterführende Klärungsbedarfe, die für die weitere Ausgestaltung und Abstimmung mit relevanten Stakeholdern von Bedeutung sind. Darüber hinaus werden thematische Abgrenzungen des Konzepts vorgenommen.
- **Anhang A** geht in Form von FAQ auf weiterführende Aspekte der eID-LE ein.

1.2 Ausgangssituation

Aktuell werden Identitäten in der Telematikinfrastruktur (TI) auf Basis von Chipkarten-Technologie betrieben. Die Zugriffe von Organisationen auf Dienste der TI erfolgen auf Basis von Institutionsidentitäten, die dezentral in Form der SM(C)-B bereitgestellt werden. Die Institutionsidentität kann prinzipiell von jedem durch die Organisation ermächtigten Mitarbeiter genutzt werden.

Personenbezogene Identitäten werden derzeit über den elektronischen HBA abgebildet. Bei Nutzung des HBA zur Authentisierung ermöglicht der IDP-Dienst der TI eine Umsetzung der Zertifikats-basierten Identität des HBA auf eine Token-basierte Identität (OpenID Connect Identity-Token). Ein personenbezogener Zugriff mit dem HBA auf Dienste der TI erfolgt in der Regel nicht. Jedoch ist ein personenbezogener Zugriff mit der personenbezogenen elektronischen Leistungserbringeridentität auf dem HBA für weitere, außerhalb der TI liegende Dienste im Gesundheitswesen notwendig, wie z.B. das Zentrale Vorsorgeregister, BTM-Portal, Organspende-Register (in Kombination mit SM(C)-B), Mitgliederportale von Kammern und Vereinigungen und diverse weitere.

Für den personenbezogenen Zugriff muss der Leistungserbringer den HBA pro Session mittels Eingabe einer PIN freischalten, wodurch er authentifiziert wird und ihm personenbezogene Merkmale attestiert werden, u.a.: Vorname, Nachname, ID der Berufsgruppe (Profession OID), Telematik-ID und potenziell weitere.

Zur Verwendung des HBA in der TI werden weitere Komponenten wie das eHealth-Kartenterminal (eHealth-KT) und ein Einbox-Konnektor oder High-Speed Konnektor (HSK) respektive Vertrag mit einem TI-Gateway Anbieter benötigt. Darüber hinaus können die kartengebundenen persönlichen Merkmale nicht flexibel oder ohne zeitlichen Verzug geändert werden, sondern bedürfen der erneuten Personalisierung, Herausgabe und Aktivierung eines neuen HBA. Gleiches gilt für eine Erweiterung der Merkmale wie bspw. Zusatzqualifikationen, die zukünftig aufgrund von neuen Aufgaben und Befugnissen für bestimmte Berufsgruppen relevant werden können.

Der HBA übernimmt neben der Funktion zur Authentisierung auch das Signieren von medizinischen Dokumenten mittels qualifizierter elektronischer Signatur (QES) für bspw. E-Rezepte und elektronische Arbeitsunfähigkeitsbescheinigungen (eAU). Im Standardablauf der QES wird der HBA – analog zum Vorgehen einer Authentisierung – in ein eHealth-KT gesteckt und die Signatur durch Eingabe einer PIN über den Konnektor bzw. HSK als Signaturerstellungskomponente ausgelöst. Mit der Komfortsignatur muss die PIN lediglich einmal eingegeben werden. Bleibt der HBA gesteckt, können anschließend weitere Signaturen innerhalb eines definierten Zeitfensters ohne erneute Eingabe erfolgen. Die Stapelsignatur ermöglicht das Signieren mehrerer Dokumente auf einmal mit nur einer PIN-Eingabe.

In der ortsunabhängigen Patientenversorgung ist eine Authentisierungs- oder Signaturlösung für Leistungserbringer bzw. Gesundheitsberufler aufgrund der fehlenden Verfügbarkeit der erforderlichen Spezialhardware zurzeit nicht möglich.

1.3 Motivation

Die derzeitige, kartengebundene Ausgestaltung des HBA weist hinsichtlich Nutzbarkeit, Flexibilität und Wirtschaftlichkeit Limitationen auf, die sich sowohl in den Administrationsprozessen als auch den bestehenden Fachprozessen niederschlagen und ortsunabhängige Versorgungsszenarien verhindern. Entsprechend liegen Mehrwerte und Motivation der Bereitstellung von digitalen Identitäten für Leistungserbringer nicht nur in einer vorteilhafteren, digitalen Umsetzung der HBA-Funktionen (vor allem Authentisierung, QES) und damit assoziierter Prozesse, sondern auch im Ermöglichen bisher nicht abbildbarer Anwendungsfälle, vor allem in mobilen Versorgungsszenarien.

Die digitalen Identitäten gemäß § 340 Abs. 6 SGB V sollen als Ergänzung zur kartengebundenen Identität des HBA bis 1. Januar 2029 bereitgestellt werden. Die Gesetzesgrundlage berücksichtigt hier bereits, dass die aktuellen hardware- und kartenbasierten Authentisierungs- und Signaturprozesse je nach Arbeitsumfeld des Leistungserbringers mit unterschiedlichen Anforderungen und Problemen verknüpft sind und von einer digitalen Identität sinnvoll komplementiert werden. Beispielsweise kann im Praxisalltag die im Lesegerät eingesteckte Karte bereits eine auskömmliche Lösung für das digitale Signieren unter Anwendung der Komfortsignatur sein, während im Klinikumfeld seltener, dafür ortsflexibel digital signiert werden muss, was mit einer fest installierten Kartenlese-Infrastruktur schwierig zu realisieren ist.

Eine digitale Lösung muss entlang der gesetzlichen Intention daher als Alternative zum HBA verstanden werden dessen Mehrwerte sich für verschiedene Zielgruppen, Anwendungsumgebungen, und Zielerwartungen unterschiedlich äußern. Im Vordergrund steht die Motivation mobile Versorgungsszenarien außerhalb der Leistungserbringerinstitution (LEI) zu ermöglichen. Gleichmaßen wird auch die Versorgung innerhalb der Institution mobiler. Mit der Einführung von digitalen Identitäten werden zudem bestehende Hürden in der Administration und Handhabung abgebaut, um Abläufe zeiteffizient und ohne mehrfache Medienbrüche zu durchlaufen. Auch senkt sich der Aufwand rund um den Beschaffungsprozess des HBA bei Verlust oder Neubeschaffung. Ebenso kann der Einsatz von Spezialhardware vermieden werden. Es kann vermehrt auf die Nutzung bestehender Standard-Hardware, wie z.B. Smartphones, gesetzt werden, was die Flexibilität der Institutionen erhöht.

1.4 Übergreifende Anforderungen

Sowohl die nationalen Paradigmen der TI 2.0 als auch die normativen Anforderungen der Europäischen Union (EU) stellen übergreifende Anforderungen an die Konzeption der digitalen Identitäten für Leistungserbringer.

Strategischer Rahmen der TI 2.0

Bisher werden Lösungen zur Nutzung der elektronischen Identität für Leistungserbringer (HBA) nur in den vom SGB V regulierten Bereichen aktiv unterstützt. Realisiert wird dies durch die TI-Föderation und deren Regelwerk sowie durch den Zugang zur TI über Spezialhardware wie eHealth-KT, Konnektoren oder TI-Gateway Zugänge. Dementgegen steht der Wunsch nach einer flächendeckenden Digitalisierung im Gesundheitswesen sowie mehr Innovationskraft, was nur über einen niederschweligen Zugang zu den grundlegenden Digitalisierungsbausteinen, wie die Identifizierung von Nutzern auf Basis von digitalen Identitäten, an Kraft gewinnen kann.

Die TI 2.0 stellt in diesem Zuge das Leitbild der digitalen Transformation im Gesundheitswesen dar. Sie sieht vor, den Zugang zu digitalen Diensten deutlich zu vereinfachen, indem sie von einer hardwarebasierten Infrastruktur (z.B. Inbox-Konnektoren, Kartenlesegeräte, SMC-B, Chipkarten) mit geschlossenem Netz zu einer

internetbasierten, flexiblen und an gängigen Industriestandards orientierten Umgebung weiterentwickelt wird. Dabei steht besonders die Einführung digitaler Identitäten im Mittelpunkt. Sie ergänzen die bisherigen physischen Karten und ermöglichen es Leistungserbringern und Patienten, sich mobil, ortsunabhängig und sicher auszuweisen – etwa über das Smartphone. Dadurch wird die Nutzung der TI-Dienste flexibler und unabhängiger von stationärer Hardware.

EU-übergreifende Anforderungen

Die EU verfolgt mit der EHDS (VERORDNUNG (EU) 2025/327 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 11. Februar 2025 über den europäischen Gesundheitsdatenraum sowie zur Änderung der Richtlinie 2011/24/EU und der Verordnung (EU) 2024/2847)- und eIDAS(VERORDNUNG (EU) 2024/1183 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 11. April 2024 zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung des europäischen Rahmens für eine digitale Identität)-Verordnung (VO) die Vision einer integrierten, sicheren und interoperablen digitalen Infrastruktur in Europa, in der Identitäten, Daten und Dienste einheitlich funktionieren, Vertrauen schaffen und den digitalen Binnenmarkt stärken.

Der EHDS bildet dabei den EU-weiten Raum für Gesundheitsdaten ab und stellt mit spezifischen Identifikations-, Authentifizierungs-, und Protokollierungsanforderungen normative Anforderungen, z.B. an Electronic Health Records-Systeme (u.a. Artikel 9 EHDS-VO). Die eIDAS-VO setzt den Rahmen für eine harmonisierte europäische digitale Identität, damit Menschen und Unternehmen sich EU-weit sicher digital ausweisen und digitale Dienste nutzen können. Kernpunkt ist die verpflichtende Einführung der europäischen digitalen Identitäts-Wallet (EUDI-Wallet), die grenzüberschreitend anerkannt, interoperabel und vertrauenswürdig funktioniert.

2 Management Summary

2.1 Ausgangssituation

Der HBA ist die kartengebundene Identität der Leistungserbringenden und ist in der Mitte der Versorgung angekommen. Mittels HBA wird täglich zum Teil millionenfach signiert, um u.a. mittels E-Rezept und eAU die deutsche Gesundheitsversorgung zu digitalisieren und zu optimieren. Die Nutzung als Sichtausweis oder als Authentisierungsmittel, beispielsweise bei der Anmeldung am Organspende-Register, spielt dabei eine vergleichsweise untergeordnete Rolle.

Das derzeitige Konzept zur Einbindung und Nutzung des HBA ist aus wesentlichen Gründen zwingend zu modernisieren:

- Mit der steigenden Zahl an ortsungebundenen Versorgungsprozessen steigt auch der Bedarf an Signaturmöglichkeiten außerhalb der Betriebsstätte.
- Die aktuelle TI sieht den Konnektor als Signaturerstellungsanwendung sowie das eHealth-Kartenterminal als Kartenlesegerät vor und blockiert demnach die Entwicklung einer TI 2.0 ohne Konnektor und ohne Spezialhardware.

Mit der EUDI-Wallet steht ab 2027 ein digitales Identifikations- und Authentisierungsmittel zur Verfügung, das eine niedrighschwellige Nutzung auf persönlichen mobilen Endgeräten ermöglicht. Hierzu zählen insbesondere Smartphones sowie geeignete Tablets mit Internetanbindung und sicheren Speicherelementen zur Verwaltung und zum Schutz digitaler Identitäten.

2.2 Lösung

Das vorliegende Konzept adressiert die zentralen strategischen Fragestellungen zur Weiterentwicklung der Leistungserbringeridentitäten im Kontext der Einführung der EUDI-Wallet. Hieraus lassen sich die folgenden Ziele und Kernaussagen ableiten:

1. Das EUDI-Wallet wird als Träger der digitalen Identität der Leistungserbringenden (eID-LE) gem. § 340 Abs. 6 SGB V etabliert.

Mit der eID-LE wird Leistungserbringern künftig eine digitale Leistungserbringeridentität bereitgestellt, die in einer EUDI-Wallet eingerichtet und über diese genutzt werden kann. Dafür muss prinzipiell ein persönliches mobiles Endgerät genutzt werden, welches mit der EUDI-Wallet App eine Gerätebindung eingeht und dem Nutzer somit eindeutig zugeordnet werden kann. Die EUDI Wallet richtet sich dabei an natürliche Personen und kann grundsätzlich entweder auf einem beruflichen oder privaten Endgerät genutzt werden. Der HBA ist keine Voraussetzung für den Erhalt einer eID-LE, sodass diese für Leistungserbringer eine Alternative oder einen Zusatz zum HBA darstellt.

Entsprechend der gesetzlichen Vorgaben verbleibt der HBA als Authentisierungsmittel für Leistungserbringer, die keine Wallet nutzen möchten,

können, oder dürfen. Ziel ist es, die eID-LE nach einer erfolgreichen technischen Erprobungsphase langfristig als Alternative zu etablieren.

Die gematik und ihre Gesellschafter prüfen die Ausgestaltung der technischen Herausgabe der eID-LE (Issuing) sowie dafür notwendige Komponenten und Prozesse. Auf wie vielen mobilen Endgeräten die Nutzung der eID-LE möglich sein wird, befindet sich in Klärung.

2. Alle Signaturen in der TI werden ausschließlich über einen (Fern-)Signaturdienst erzeugt.

Im Rahmen einer Vergabe wird ein zentraler (Fern-)Signaturdienst auf Basis vorhandener technischer Grundlagen geschaffen, der den aktuellen Funktionsumfang, insbesondere die Komfortfunktion, der TI erhält. Ein beauftragter Dienst sichert einen festen und planbaren Kostenrahmen, uniforme Schnittstellen, geringere Implementierungsaufwände und kürzere sowie einfachere Nutzerflows. Zur Authentisierung am (Fern-)Signaturdienst werden die EUDI-Wallet mit der eID-LE und der HBA angebunden. Zum Auslösen einer Organisationssignatur werden bestehende sowie auch zukünftige digitale Lösungen einer Identität für Leistungserbringerinstitutionen angebunden.

Die Vergabe des Signaturdienstes ergibt sich aus umfangreichen und spezifischen- und damit marktunüblichen – Sicherheitsanforderungen zur Umsetzung der Komfortsignaturfunktion. *Aufgrund der zentralen Bedeutung dieses Dienstes prüfen die gematik und ihre Gesellschafter notwendige Maßnahmen zur Gewährleistung einer höchstmöglichen Betriebsstabilität, beispielsweise die Etablierung einer Second-Source.*

3. Der HBA bleibt weiterhin als Smartcard erhalten. Vereinfachungen sind möglich.

Der HBA (und die SMC-B) werden als Authentisierungsmittel, auch gegenüber dem neuen Signaturdienst, weiterhin zur Verfügung stehen. Dies stellt die Versorgung insbesondere für Leistungserbringende ohne EUDI-Wallet sicher. Die Authentisierung mit Hilfe des HBA, insbesondere am (Fern-)Signaturdienst, wird zukünftig alternativ mittels Standard-Kartenterminals anstatt der Kombination aus eHealth-Kartenterminal und Inbox- oder Highspeed-Konnektor nutzbar. Die gematik wird zur Ansteuerung des HBAs kein eigenständiges Softwareprodukt bereitstellen. *Die gematik behält sich jedoch weitere technische und organisatorische Festlegungen vor.*

Der HBA bleibt vorerst in seinem vollen Funktionsumfang erhalten. Der HBA benötigt allerdings perspektivisch keine Signaturzertifikate mehr und würde somit auch nicht mehr der Zertifizierungspflicht als QSCD (Qualified Signature Creation Device) unterliegen. Die personenbezogene Ver- und Entschlüsselung mittels separater Zertifikate (HBA.ENC) wird für die eID-LE nicht fortgeführt. Auch eine etwaige Anforderlichkeit zum Kartentausch aufgrund eines veralteten QES-Zertifikats oder Signatur-Algorithmus kann so entfallen. *Ob eine funktionale Verschlankung des HBA perspektivisch erfolgen kann, bleibt eine zu treffende Entscheidung der gematik und ihrer Gesellschafter.*

4. Für die mobile Versorgung wird die digitale, Wallet-gestützte eID-LE positioniert.

Die EUDI-Wallet ist ein elementarer Baustein, um die mobile Versorgung zu ermöglichen. Einerseits werden in der vorgeschlagenen Architektur mobile Versorgungsszenarien zwar auch mit Standard-Kartenterminal, HBA, Primärsystem oder einer Authenticator App auf dem Laptop ermöglicht, andererseits ist die Nutzung der EUDI-Wallet per se deutlich leichtgewichtiger und wird daher als nutzerfreundlicher erachtet. Konsequenterweise ist langfristig auch die native Unterstützung der EUDI-Wallet in der TI ein Ziel der gematik.

Im Ergebnis vereinfacht die eID-LE bestehende Prozesse, unterstützt die ortsungebundene Patientenversorgung und ermöglicht die Abkündigung von Spezialhardware zur konsequenten Einführung der TI 2.0.

Für die Umsetzung der vorgeschlagenen Lösungsoption wird ein „Wallet-Adapter“ mit den Funktionen der eID-LE-Prüfung, Protokollumsetzung und potenziell der eID-LE-Provisionierung (siehe Kapitel 3.3- Umsetzung eID-LE mittels Wallet-Adapter) sowie ein (Fern-)Signaturdienst (siehe Kapitel 4.3- Umsetzung (Fern-)Signaturdienst) benötigt.

Der Wallet-Adapter wird als neuer zentraler TI-Dienst konzipiert und soll im Rahmen einer Neuvergabe umgesetzt werden. Die Einführung des Wallet-Adapters erfolgt dabei im Zuge der Ablösung und Modernisierung des bestehenden IdP-Dienstes schrittweise, um eine kontrollierte Migration sowie einen stabilen Übergang in das Zielbild der TI 2.0 zu gewährleisten. Die vorgesehene funktionale Entkopplung der zu übernehmenden Bestandsfunktionen ermöglicht zugleich den sukzessiven Rückbau künftig nicht mehr benötigter Funktionalitäten.

3 Konzeptionelle Umsetzung eID-LE

3.1 Rechtliche Anforderungen

Sowohl nationale Vorgaben als auch die verbindlichen rechtlichen Anforderungen der EU setzen übergreifende Rahmenbedingungen für die Gestaltung digitaler Identitäten von Leistungserbringern.

Tabelle 1: *Rechtliche Vorgaben an die digitale Identität (Authentisierung)*

Gesetz / Verordnung	Thema	Anforderungen
SGB V § 340 Absatz 6	Bereitstellung digitaler Identitäten	Spätestens ab dem 1. Januar 2029 haben die Stellen nach Absatz 1 Satz 1 Nummer 1 sowie den Absätzen 2 und 4 ergänzend zu den Heilberufs- und Berufsausweisen auf Verlangen des Leistungserbringers eine digitale Identität für das Gesundheitswesen zur Verfügung zu stellen, die nicht an eine Chipkarte gebunden ist.
eIDAS-Verordnung Artikel 5f.	Verpflichtende Einbindung der EUDI- Wallet für öffentliche Stellen und private vertrauende Beteiligte mit starker Nutzerauthentifizierung.	(1) Verlangen Mitgliedstaaten für den Zugang zu einem von einer öffentlichen Stelle erbrachten Online- Dienst eine elektronische Identifizierung und Authentifizierung, so akzeptieren sie auch europäische Brieftaschen für die Digitale Identität, die gemäß dieser Verordnung bereitgestellt werden. (2) Sind private vertrauende Beteiligte, die Dienste erbringen [...], nach Unionsrecht oder nationalem Recht verpflichtet, eine Online- Identifizierung mit starker Nutzerauthentifizierung vorzunehmen [...], so akzeptieren diese privaten vertrauenden Beteiligten [...] auch europäische Brieftaschen für die Digitale Identität, die gemäß dieser Verordnung bereitgestellt werden.

3.2 Fachliche Anforderungen

Die derzeitige, kartengebundene Ausgestaltung des HBA weist hinsichtlich Nutzbarkeit, Flexibilität und Wirtschaftlichkeit Limitationen auf. Diese beeinflussen sowohl administrative Abläufe als auch bestehende Fachprozesse und verhindern vor allem mobile Anwendungsfälle. In diesem Abschnitt werden zunächst die Schmerzpunkte vorgestellt und in welchen Anwendungsumgebungen (Krankenhaus, Praxis, mobile Szenarien) diese vorrangig sichtbar werden. Anschließend werden die daraus resultierenden, zentralen fachlichen Anforderungen an die Authentisierung mittels digitaler Identitäten zusammengefasst.

3.2.1 Strukturbedingte Schmerzpunkte

Komplexität und Kosten durch Spezialhardware:

Die aktuelle, kartengebundene HBA-Lösung führt zu einer starken Abhängigkeit von spezialisierter Hardware wie physischen Karten und stationären Kartenlesegeräten. Diese Abhängigkeit verursacht hohe Beschaffungs-, Vorhalte- und Investitionskosten und erhöht zugleich die organisatorische Komplexität bei Bereitstellung, Betrieb und Support. Zugleich schränkt sie Einrichtungen in ihrer Flexibilität ein, da Prozesse nur mit separat angeschaffter und verwalteter Spezialtechnik funktionsfähig sind.

Fehlende Umsetzbarkeit mobiler Versorgungsszenarien:

Darüber hinaus ist die heutige Architektur des HBA räumlich stark gebunden: die Authentisierung kann nur im Umfeld physischer Praxis- oder Klinikinfrastrukturen genutzt werden, da der Zugriff das Stecken des HBA erfordert. Dadurch lassen sich mobile oder ortsunabhängige Versorgungsszenarien technisch nicht abbilden. Authentisierungsvorgänge sind somit häufig an einen bestimmten Ort und ein bestimmtes Gerät gebunden, was innerhalb der Organisation zu Verzögerungen und unflexiblen Abläufen führt. Es fallen nicht nur Wege innerhalb, sondern auch außerhalb bzw. zur Institution an.

Mangelhafte Prozesseffizienz und Handhabung:

Anwender erleben das Zusammenspiel aus Karte und Kartenlesegerät vor allem im ortsungebundenen Versorgungskontext als umständlich, fehleranfällig und wenig effizient. Die Medienbrüche zwischen Arbeitsplätzen und Endgeräten erzeugen Reibungsverluste, und die physische Gebundenheit an Terminals führt insbesondere in größeren Einrichtungen wie Krankenhäusern zu unnötigen Wegzeiten. Prozesse, die zwingend den physischen Einsatz des HBA erfordern, werden dadurch langsamer, komplizierter und störanfälliger.

Hoher Administrationsaufwands des HBA:

Ein weiteres strukturelles Problem ergibt sich aus dem hohen administrativen Aufwand, der bei Verlust, Defekt oder Erneuerung des physischen HBA entsteht. Die notwendigen Schritte – Registrierung, Aktivierung und Freischaltung – sind mehrstufig, teils zeitaufwendig und wirken sich unmittelbar auf die Arbeitsfähigkeit der betroffenen Personen aus. Da zentrale Fachprozesse ohne funktionierenden HBA oder ohne intaktes Lesegerät nicht fortgeführt werden können, führen Ausfälle der physischen Komponenten schnell zu längeren Unterbrechungen der beruflichen Tätigkeit. Die starre Bindung an eine physische Smartcard erschwert zudem den kurzfristigen Ersatz oder flexible Übergangslösungen.

3.2.2 Schmerzpunkte nach Anwendungsumgebungen

Die Schmerzpunkte der aktuellen Prozesse sind je nach Anwendungsumgebung, Zielanwendung und Zielgruppe unterschiedlich stark ausgeprägt. Mit Blick auf die Notwendigkeit bzw. den Bedarf an digitalen Identitäten und den daran geknüpften Anforderungen sind, stark abstrahiert, drei Anwendungsumgebungen zu unterscheiden:

Große stationäre Einrichtungen(Krankenhäuser, große MVZs, Pflegeeinrichtungen) sind von den zuvor genannten Schmerzpunkten **stark betroffen**. Dies liegt vor allem an der hohen Fluktuation des Personals und Komplexität des Behandlungsteams sowie dem Behandlungsumfeld, was durch wechselnde Arbeitsplätze, (Unter-)Abteilungen und räumliche Distanz charakterisiert ist. Es existieren unterschiedliche IDs für verschiedene Systeme, davon sind manche Sammelidentitäten, andere sind personalisiert. Zudem bestehen verschiedene Sicherheitsniveaus, aus der Verwendung von Kombinationen einfacher Nutzernamen / Passwörter oder Zweifaktor-Authentisierung.

Kleine niedergelassene Einrichtungen(Arztpraxen, Zahnarztpraxen, Apotheken, Psychotherapiepraxen) sind aufgrund kleiner Behandlungsteams und weniger Arbeitsplatzwechsel von den Schmerzpunkten **vergleichsweise gering betroffen**, sofern die bestehende Infrastruktur fehler- und störungsfrei läuft. Schmerzpunkte liegen, wenn auch nicht ausschließlich, als administrativer und wirtschaftlicher Faktor vor.

Mobile Szenarien(Hausbesuch, Rettungseinsatz, Telemedizin, häusliche Pflege, ...) sind aufgrund der Abhängigkeit von Spezialhardware **derzeitig überhaupt nicht möglich**.

3.2.3 Anforderungen

Tabelle 2 fasst Anforderungen an die digitale Identität zur Authentisierung zusammen. Diese werden bei der Lösungsdefinition beachtet, jedoch im Nachgang nicht einzeln adressiert.

Tabelle 2: Fachliche Anforderungen an die digitale Identität (Authentisierung)

No.	Fachliche Anforderung
Auth-1	Mobile Nutzbarkeit innerhalb der Institution (Arbeitsplatzwechsel)
Auth-2	Mobile Nutzbarkeit außerhalb der Institution (remote)
Auth-3	Keine Spezialhardware erforderlich
Auth-4	Wahl des Authentisierungsmittels innerhalb einer Institution (persönliches mobiles Endgerät oder physische Smartcard)
Auth-5	Abbildung (mehrerer) TI und TI-fremder Attribute in der Identität
Auth-6	Identität derselben Person muss bei Institutions- oder Standortwechsel adaptiv nutzbar und einfach zuzuordnen sein
Auth-7	Zuordnung von Identität und VZD-Eintrag muss möglich sein
Auth-8	Die Lösung orientiert sich an gängigen Standards und kann von unterschiedlichen Systemen schnell und schlank integriert werden

Auth-9	Identität muss online deaktivierbar sein
Auth-10	Intuitive Nutzerführung mit geringer Nutzerinteraktion (wenige Klicks / Bestätigungen / PIN-Eingaben)
Auth-11	Möglichkeit zur Rücksetzung der PIN durch Nutzenden (annehmlich Funktion der EUDI-Wallet).
Auth-12	Geringe Latenz
Auth-13	Hochverfügbarkeit
Auth-14	Eine Sperrung der kartengebundenen Identität des HBA (z.B. bei Verlust) führt nicht zu einer Sperrung der eID-LE in der EUDI Wallet (und umgekehrt). Die dem HBA und der eID-LE zugrundeliegende Identität ist über beide Bereitstellungsformen unabhängig nutzbar.
Auth-15	Eine kartengebundene Identität in Form eines HBA ist nicht zwingend eine Voraussetzung zum Erhalt einer nicht kartengebundenen digitalen Identität in Form einer LE-eID (und umgekehrt).
Auth-16	Zur Beantragung einer digitalen Identität kann eine kartengebundene Identität verwendet werden (und umgekehrt). Auch für die Beantragung einer Institutionsidentität ist die digitale Identität ausreichend
Auth-17	Zugriffsberechtigungen sind für die kartengebundene Identität als auch die digitale Identität umsetzbar

3.3 Umsetzung eID-LE mittels Wallet-Adapter

Im Folgenden wird als Umsetzungsvorschlag zur Erfüllung der zuvor genannten Anforderungen eine digitale Identitätslösung für Leistungserbringer beschrieben, welche EU-konform im Gesundheitswesen nutzbar ist und gleichzeitig eine Nutzung in der TI erlaubt. Dieser Vorschlag basiert auf der nationalen Bereitstellung der EUDI-Wallet als dezentraler Träger der digitalen Identität und ermöglicht eine umfassende und interoperable Nutzung durch den Leistungserbringer an Diensten seiner Wahl über die Wallet-Schnittstelle. Da die eIDAS 2.0 Verordnung große Teile der Wirtschaft und öffentlichen Stellen zur Integration einer solchen Schnittstelle verpflichtet, sind die Voraussetzungen für ein breites und zur TI rückwirkungsfreies Angebot gegeben.

3.3.1 Systemüberblick

Kern der im Folgenden dargestellten Lösung ist die Bereitstellung der digitalen Identität als dezentrale und EUDI-Wallet basierte Identität ("HBA auf dem Smartphone"). Dadurch müssen keine Gesundheitssystem-spezifischen Lösungen, vergleichbar zur GesundheitsID-Versicherte, bereitgestellt werden. Die EUDI-Wallet wird als hoheitliches System für digitale Identitäten entsprechend der gesetzlichen Vorgaben für Leistungserbringer genutzt.

[illegible]

3.3.1.1 Akteure und Rollen

Leistungserbringer als Hauptakteure. Sie sind gemäß § 340 SGB V berechnete natürliche Person zur Beantragung einer digitalen Identität.

Die Ausgestaltung der technischen Herausgabe (Issuing) ist in der Abbildung und im Folgenden der Einfachheit halber mit Hilfe des Wallet-Adapters dargestellt. Die gematik und ihre Gesellschafter prüfen im weiteren die bestgeeignete Umsetzung der technischen

Herausgabe des VC sowie dafür notwendige Komponenten und Prozesse, dazu siehe auch 6.1.1- Rolle der Attributbestätigenden Stellen und des Wallet Adapters.

Anbieter des Wallet-Adapter handelt im Auftrag der attributbestätigenden Stellen zur Bereitstellung der eID-LE in Form von VC. Die Provisionierung der eID-LE erfolgt nach der Authentifizierung auf Basis der persönlichen Identität im EUDI-Wallet (Personal Identification Data, PID). Daher ist der Wallet-Anbieter Relying Party der PID und potenziell Issuer der VC in die Wallet – tritt also technisch gesehen mit dem Zertifikat des Pub-EAA/QEAA gegenüber der Wallet auf. Wie im vorherigen Abschnitt dargestellt, kann diese Aufgabe nach Abstimmung zur geeigneten Umsetzung auch aus dem Wallet-Adapter ausgegliedert und anderweitig umgesetzt werden.

Nachdem die eID-LE tatsächlich ins EUDI-Wallet eingebracht ist, tritt der Anbieter des Wallet-Adapters als Relying Party der eID-LE auf und prüft die Gültigkeit der präsentierten VC. Aus Sicht der TI-Dienste wiederum agiert der Anbieter des Wallet-Adapters als IDP gemäß OpenIDConnect (OIDC) – hier erfolgt die Protokollumsetzung von der EUDI-Wallet auf OIDC.

Anbieter von Diensten der TI als tatsächliche Versorgungsleistungsanbieter. Im Ökosystem des Gesundheitswesens bauen die Dienste der TI auf den korrekten und berechtigten Zugängen für die Leistungserbringer auf. Konsequenterweise müssen sich diese Dienste als Relying Party registrieren, um die VC der eID-LE anzufordern und zu prüfen.

3.3.1.2 Komponenten und Dienste

Des Weiteren sind im dargestellten Systemüberblick folgende Komponenten und Dienste von zentraler Bedeutung:

- **EUDI Trust Framework** als pan-europäischer Vertrauensraum. Es sichert als Vertrauensraum die Integrität aller registrierten (Q)TSP, QEAA/Pub-EAA und Relying Parties. Das gilt auch auf europäischer Ebene, um z.B. die Versorgung von EU-Bürgern im EU-Ausland gemäß EHDS-VO zu ermöglichen.
- **EUDI-Wallet** als Träger der Identität. Die mobile App auf dem mobilen Endgerät des Leistungserbringers dient der Verwaltung und Nutzung der PID (in Analogie zum nPA) sowie der eID-LE. Die VC der eID-LE enthalten mindestens die Felder Telematik-ID und ProfessionOID, um diese im Rahmen der Authentifizierung gegenüber den Diensten der TI, technisch gesehen via Wallet-Adapter, zu beaskunften.
- **Wallet-Adapter** als zentraler technischer Dienst für die eID-LE in der TI mit den Funktionen:
 - Authentifizierung des Leistungserbringers auf Basis der PID der EUDI-Wallet ggf. im Rahmen der eID-LE Provisionierung.
 - Potenziell die Provisionierung der eID-LE in Form von VC in die EUDI-Wallet.
 - Wallet-basierte Authentifizierung des Leistungserbringers auf Basis der eID-LE Prüfung (Statusprüfung) gegen den (nationalen) Trust Framework im Rahmen der Nutzung von Diensten der TI und Weiteren.
 - Protokollübersetzung zwischen TI-Diensten, die auf OpenID Connect basieren und dem zukünftigen Standard OpenID for Verifiable Presentation (OpenID4VP).

3.3.2 Nutzung der digitalen Identität

Die Interaktionen zum Erlangen und Nutzen der eID-LE in einem Standardablauf ist zunächst an Vorbedingungen geknüpft und gestaltet sich wie nachfolgend beschrieben.

3.3.2.1 Vorbedingungen:

- Die attributbestätigenden Stellen oder durch sie beauftragte Dienstleister sind als im EUDI Wallet Trust Framework registriert.
- Der Anbieter des Wallet-Adapter ist als Relying Party der PID und der eID-LE im EUDI Wallet Trust Framework registriert.
- Die eID-LE nutzenden (TI-)Dienste sind als Relying Party im EUDI Wallet Trust Framework registriert.

3.3.2.2 Interaktionsübersicht

1. Die digitale Identität wird nach erfolgreicher Beantragung bei den attributbestätigenden Stellen an den Wallet-Adapter übermittelt.
2. Der Leistungserbringer ruft den Wallet-Adapter auf und authentifiziert sich mit den PID seiner EUDI-Wallet gegenüber diesem.
3. Der Wallet-Adapter stellt dem Leistungserbringer anschließend die eID-LE als VC in die persönliche Wallet aus. Dies erfolgt mittels Protokoll OpenID for VC Issuing (OpenID4VCI).
4. Die personenbezogene Authentifizierung in der TI erfolgt zentral am Wallet-Adapter. Hierbei wird das einen TI-Dienst mit personenbezogener Zugriffskontrolle aufrufende Frontend (PS oder Browser eines Nicht-TI-Dienstes) von diesem an den Wallet-Adapter weitergeleitet und wie bisher auf Basis des OpenID Connect (OIDC) Standards eine Authentifizierung angefordert.
5. Der Wallet-Adapter initiiert gegenüber der EUDI-Wallet den Authentifizierungsvorgang und der Nutzer erhält die Information, für welche Relying Party seine Authentifizierung angefordert wird und welche Attribute/Nachweise benötigt werden. Daraufhin kann dieser souverän wählen, welche Nachweise übermittelt werden.
6. Die EUDI-Wallet präsentiert dem Wallet-Adapter auf Basis von OpenID4VP (Protokoll OpenID for verifiable presentation) die durch den Leistungserbringer freigegebene eID-LE. Der Wallet Adapter prüft im Rahmen der Authentifizierung als Verifier die Echtheit der eID-LE sowie den Sperrstatus. Weitere konkrete Prüfgegenstände wurden ggf. vorher mit Relying Parties vereinbart.
7. Der Wallet-Adapter leitet bei positivem Prüfungsergebnis das Frontend im Rahmen des OIDC-Flows wieder an den TI-Dienst zurück, worauf dieser den OIDC Identity Token mit der vom Wallet-Adapter attestierten eID-LE von diesem abrufen und dem Leistungserbringer den Zugriff gewährt.

Der Wallet-Adapter agiert aus Sicht der TI-Dienste wie ein OIDC Identity Provider und gegenüber der EUDI-Wallet als VC-Verifier gemäß EU Digital Identity Framework. Da die TI-Dienste den OIDC-Standard schon implementiert haben, ergeben sich keine technischen Änderungsbedarfe an diese und eine Migration und Einführung der eID-LE wird stark vereinfacht.

3.3.2.3 Praktische Aspekte in der Nutzung der digitalen Identität

Ein berechtigter Leistungserbringer beantragt eine digitale Identität bei der gemäß § 340 SGB V entsprechenden Stelle und könnte als Identifikationsmittel die EUDI-Wallet mit der PID nutzen. Als Voraussetzung dafür muss die PID zuvor in die Wallet eingebracht worden sein. Auf die bisher gängigen Verfahren zur Identifikation sind weiterhin möglich, wie z.B. Post-Ident, oder technische Verfahren unter Zuhilfenahme von nPA und ePass. Die Sinnhaftigkeit und Umsetzungsaufwände hängen stark von den Prozessen und der Datengrundlage für die Prüfung der Berechtigung zum Erhalt einer eID-LE ab. Im Rahmen der Authentifizierung als Leistungserbringer mittels eID-LE wird dieserüber die EUDI-

Wallet aufgefordert, die angefragten Identitätsdaten durch Eingabe einer PIN –
möglicherweise auch nur mit Biometrie – freizugeben.

Das EUDI-Wallet wird ausschließlich als App für mobile Endgeräte mit sicheren
Speicherelementen bereitgestellt, da diese für eine sicherheitstechnische Verankerung
essenziell sind. Vereinfacht ausgedrückt werden sogenannte Secure-Elements, auf
Hardwareebene getrennte und gesicherte Bereiche im Chip, genutzt, die bei stationären
Rechnern und anderen Handheld-Geräten so nicht zur Verfügung stehen. Verwendet der
Leistungserbringer für die Nutzung der TI-Dienste ein bzgl. EUDI-Wallet anderes Gerät
(bspw. Primärsystem), so muss er gemäß Architectural and Reference Framework zuvor
einen QR-Code mit der EUDI-Wallet App scannen, um eine Kopplung bzw. Rücksprung
zwischen mobilem Endgerät und dem anderen vorrangig stationären Gerät zu
ermöglichen.

3.3.3 Nutzung der digitalen Identität im Kontext der LEI

3.3.3.1 Systemüberblick

Die Nutzung der digitalen Identität muss auch im Zusammenspiel mit den IT-Systemen
der Leistungserbringerumgebung möglich sein. Zudem muss eine „harte“ Kopplung der
Identität des Leistungserbringers mit der Institutionszugehörigkeit oder -identität
vermieden werden, um Szenarien von einer Mehrfach-Zugehörigkeit,
Arbeitnehmerüberlassung und insb. Tagesaushilfen praxistauglich und ohne langwierige
Verfahren oder Zusatzaufwände gestalten zu können.

Andererseits ergibt sich insb. aus den Anwendungsfällen des Organspende Registers auch
die Anforderung, eine Authentifizierung auf Basis der Identität des Leistungserbringers
und der Leistungserbringerinstitution durchführen zu können. Solch ein Kontext kann nur
situativ durch die (persönliche) digitale Identität des Leistungserbringers unter Nutzung
der IT-Systeme (mit Zugriff auf die SM(C)-B) einer dedizierten
Leistungserbringerinstitution hergestellt werden.

Der Systemüberblick zur Einbettung der eID-LE in die LEI ist in Abbildung 2 dargestellt.

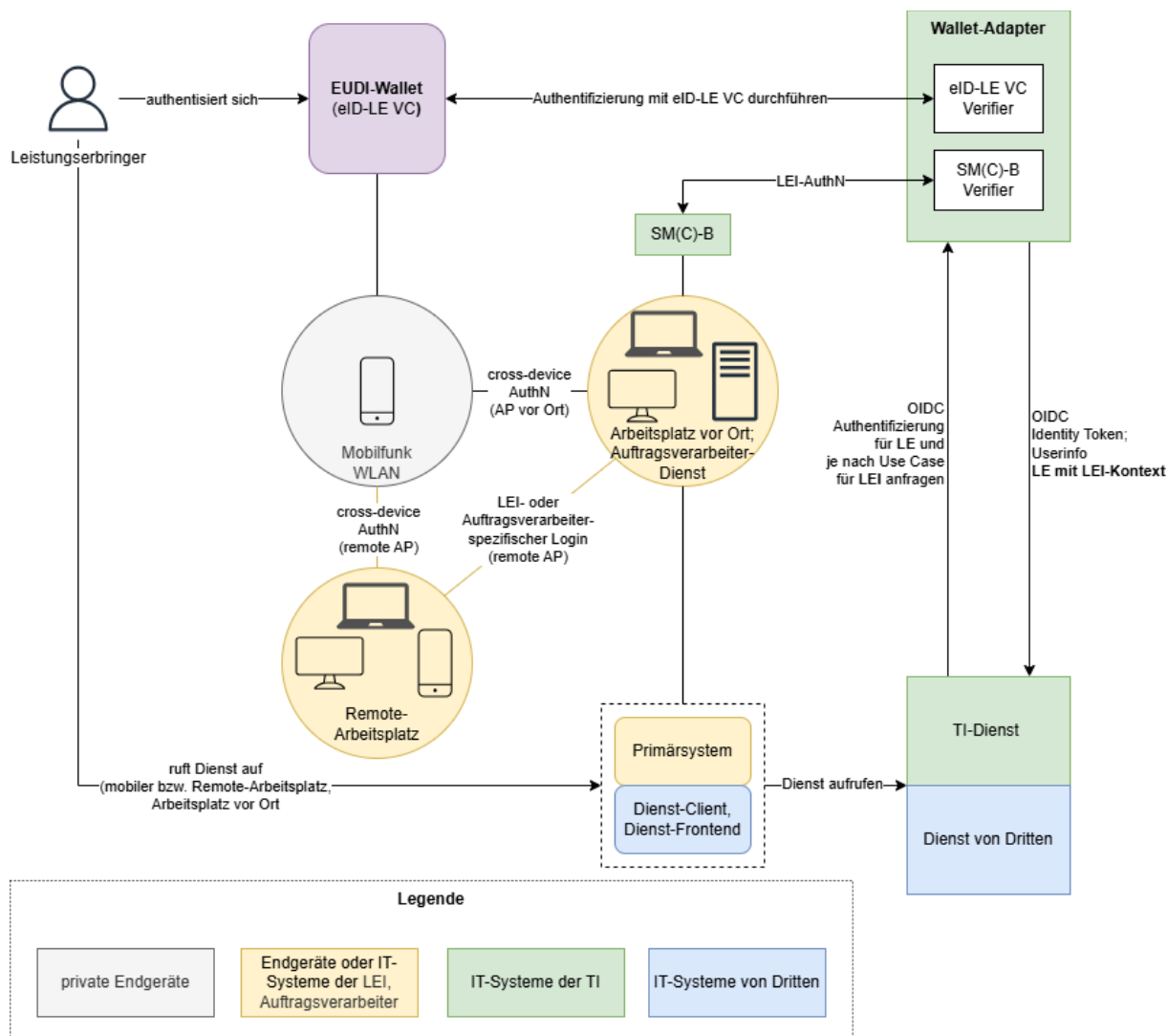


Abbildung 2: Systemüberblick zur digitalen Identität in der LEI

Die hier dargestellte Lösung ermöglicht das Arbeiten in der ortsungebundenen Patientenversorgung und allgemein von Remote-Arbeitsplätzen, falls die Leistungserbringerinstitution die Möglichkeit für Fernzugriffe auf die entsprechenden IT-Systeme ermöglicht oder ein Online-Primärsystem genutzt wird. Solch eine Voraussetzung kann nicht durch die TI geschaffen werden, da nicht alle Versorgungs-, Abrechnungs- und Dokumentations-relevanten Daten über Dienste der TI verarbeitet und somit nur über das Primärsystem synchron gehalten und Geräte- bzw. Orts-übergreifend verfügbar gemacht werden können.

Demzufolge spielt die Leistungserbringerinstitution oder ein Auftragsverarbeiter mit Online-PS eine essenzielle Rolle für mehrwertstiftende und nahtlose Abläufe in der ortsungebundenen Patientenversorgung. Positiv anzumerken ist, dass diese Voraussetzungen je nach Bedarf und Kontext, bspw. in der ambulanten Pflege, häufig bereits umgesetzt sind.

3.3.3.2 Interaktionsübersicht:

Die Interaktionen eines Standardablauf zum Verwenden der eID-LE in einer Institution könnte wie folgt aussehen:

1. Der Leistungserbringer wird durch den Institutionsinhaber für Zugriffe auf (weitere) Dienste der TI durch das Einrichten des Zugriffs auf die IT-Systeme mit Zugriff auf die SM(C)-B der LEI ermächtigt.
2. Der Leistungserbringer ruft einen (weiteren) Dienst der TI mit dem IT-System der LEI auf.
3. Der (weitere) Dienst der TI fordert gemäß seiner Zugriffsrichtlinie eine Leistungserbringer-Authentifizierung und ggf. LEI-Authentifizierung von dem Wallet-Adapter an.
4. Das IT-System der LEI wird zum Wallet-Adapter weitergeleitet.
5. Im Falle einer LEI-Authentifizierung muss die SM(C)-B basierte Authentifizierung durch den Wallet-Adapter (analog der heutigen Funktion des IDP-Dienstes) erbracht werden, der die X.509-basierte Identität verifiziert. Die Leistungserbringer-Authentifizierung wird danach durch Anzeige eines QR-Codes am IT-System der LEI initiiert.
6. Der Leistungserbringer scannt den QR-Code mit seinem Smartphone bzw. der EUDI-Wallet.
7. Die EUDI-Wallet fordert den Leistungserbringer auf, die angefragten Identitätsdaten durch Eingabe einer PIN – möglicherweise auch nur mit Biometrie – freizugeben.
8. Der Wallet-Adapter verifiziert die Identitätsdaten und übermittelt den anfragenden (weiteren) Dienst der TI einen Identity-Token mit den attestierten Identitätsdaten des Leistungserbringer und ggf. der LEI.

Aktuell wird davon ausgegangen, dass ein Dienst-übergreifendes Single Sign-On für die Authentifizierung von Leistungserbringern aufgrund der spezifischen und singulären Anwendungsfälle nicht notwendig und datenschutzrechtlich problematisch wäre.

3.3.4 Nutzung der kartengebundenen Identität (HBA)

3.3.4.1 Systemüberblick

Nutzt der Leistungserbringer keine digitale Identität, steht diesem kein Smartphone zur Verfügung oder ist die Nutzung von Smartphones aufgrund der Arbeitsumgebung grundsätzlich nicht möglich, so ist die Nutzung des HBA im Zusammenspiel mit dem Primärsystem oder einer Authenticator App und einem USB-Kartenterminal an den Arbeitsplätzen zur Authentisierung möglich. Einen Systemüberblick für dieses Szenario gibt Abbildung 3.

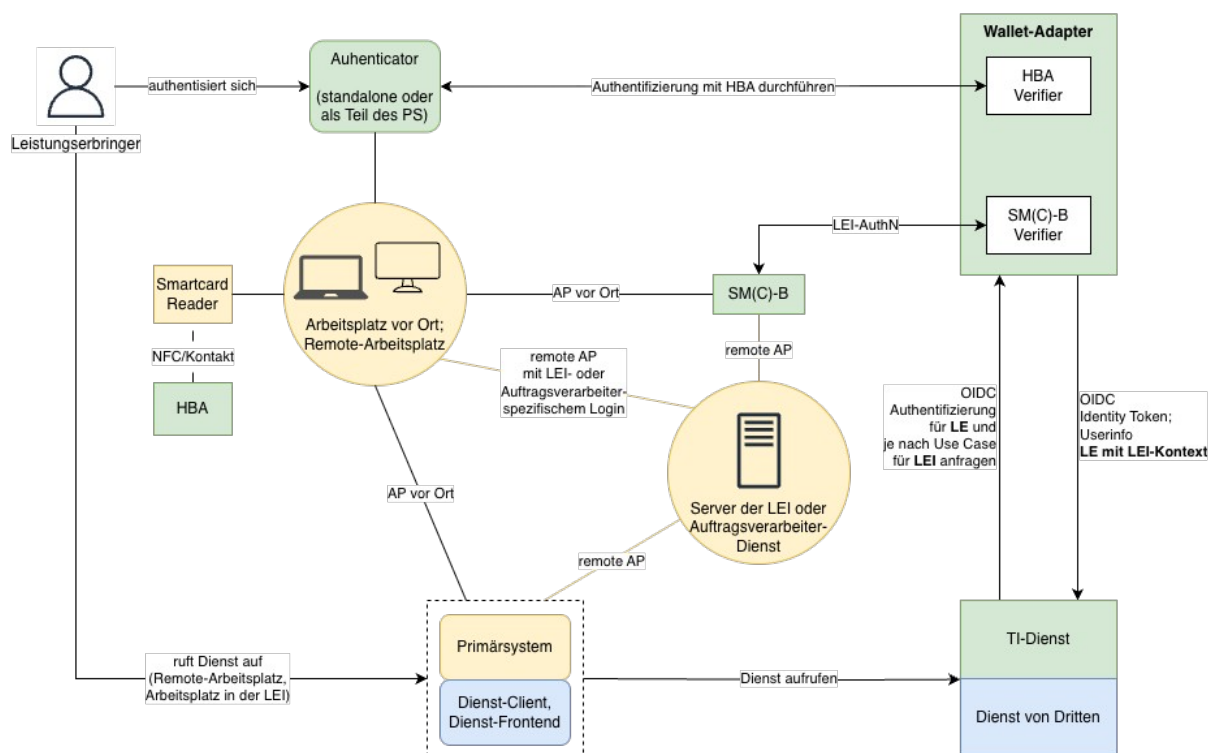


Abbildung 3: Systemüberblick zur kartengebundenen Identität (HBA)

3.3.4.2 Interaktionsübersicht

Da es sich hier – bis auf die ergänzende Einführung eines Standard-Kartenterminal zur Ermöglichung der alternativen Nutzung der kartenbasierten Identität in Remote- bzw. von der LEI unabhängigen Szenarien – um die gleichen Funktionen und Abläufe wie in der aktuellen TI handelt, wird auf die Interaktionen nicht detailliert eingegangen. Das eHealth-KT kann weiterhin als Alternative zum eH-KT für die notwendigen Interaktion bzw. Kommunikation mit dem HBA verwendet werden. Mit der ergänzenden Einführung eines Standard-Kartenterminal werden weiterhin alle HBA-basierten Authentifizierungen möglich sein.

4 Konzeptionelle Umsetzung (Fern-)Signatur

4.1 Rechtliche Grundlagen

Die rechtliche Anforderung zur Bereitstellung einer (Fern-)Signatur wird mittelbar begründet. Zunächst liegt die Motivation zur Bereitstellung von digitalen Leistungserbringer Identitäten gemäß § 340 Abs. 6 SGB V in der ergänzenden, digitalen Bereitstellung einer kartenlosen Identität, demnach als Alternative zum HBA, und damit assoziierter Prozesse. Dies umfasst auch und vor allem die Signatur-Funktion. Die Umsetzung von § 340 Abs. 6 SGB V ist somit ausschließlich durch Schaffung einer (Fern-)Signatur mit den avisierten Mehrwerten möglich.

Gleichermaßen ergibt sich eine mittelbare Anforderung durch § 27 SGB V bzw. § 73 SGB V, welche den Anspruch auf Krankenbehandlung und notwendige (haus-)ärztliche Versorgung samt Verordnungsermächtigung begründen. Auch Hausbesuche gehören zur Pflicht der behandelnden Hausärzte, sofern dem Patienten der Praxisbesuch krankheitsbedingt nicht möglich oder unzumutbar ist und eine ärztliche Behandlung erforderlich ist. Die Versorgung im häuslichen Umfeld ist nur dann vollständig, wenn der Arzt neben der Untersuchung auch alle notwendigen Verordnungen und Bescheinigungen (z. B. eRezept oder eAU) direkt vor Ort ausstellen kann. Ohne praktikable Möglichkeit zur Ausstellung einer Verordnung mit rechtsgültiger (Fern-)Signatur vor Ort wäre dies nicht umsetzbar. Damit gibt es sowohl eine direkte gesetzliche Pflicht zur mobilen Versorgung als auch eine indirekte, aber rechtlich verbindliche Pflicht, die Verordnung (Rezept) dafür zu ermöglichen.

Die eIDAS-VO normiert grundlegende Anforderungen an den elektronischen Signaturprozess (QES).

4.2 Fachliche Anforderungen

In diesem Abschnitt werden die Schmerzpunkte vorgestellt und in welchen Anwendungsumgebungen (Krankenhaus, Praxis, mobile Szenarien) diese vorrangig sichtbar werden. Anschließend werden die daraus resultierenden, zentralen fachlichen Anforderungen an eine möglichst universell einsetzbare Signatur zusammengefasst.

4.2.1 Strukturbedingte Schmerzpunkte

Siehe [3.2.1- Strukturbedingte Schmerzpunkte](#): Die hardware- und kartenbasierten-Signaturprozesse sind grundsätzlich mit den gleichen strukturbedingten Problemen verknüpft, die bereits im Kapitel zur eID-LE aufgeführt werden.

4.2.2 Schmerzpunkte nach Anwenderumgebung

Die zentralen Schmerzpunkte der Signatur-spezifischen Prozesse werden nachfolgend für die drei in [3.2.2- Schmerzpunkte nach Anwendungsumgebungen](#) charakterisierten Anwendungsumgebungen ausgeführt:

Große stationäre Einrichtungen, vor allem Krankenhäuser, nutzen QES-abhängige TI-Anwendungen bislang kaum, da die infrastrukturellen Voraussetzungen nur eingeschränkt vorhanden sind. Sie sind durch die Schmerzpunkte daher **stark betroffen**. An vielen Arbeitsplätzen fehlt ein eHealth-Kartenterminal, dessen flächendeckende Ausstattung hohe Kosten verursachen würde. Zudem ist die kartenbasierte Signatur kaum in die klinischen Abläufe integrierbar und führt zu Medienbrüchen. Ein weiteres Hemmnis ist die unvollständige Ausstattung des ärztlichen Personals mit HBAs, die auch ein eigener Kostenfaktor sind. Dadurch bleibt die praktische Nutzung von QES-Anwendungen im Klinikalltag stark eingeschränkt. Es fallen aufwendige Wegzeiten innerhalb (Arbeitsplatzwechsel) und außerhalb der Organisation (Anreise) nur für Signaturzwecke an.

Für kleine niedergelassene Einrichtungen ist die bestehende Infrastruktur aus Anwendersicht **grundsätzlich geeignet**, elektronische Signaturen zuverlässig auszuführen. Besonders die Komfortsignatur (und Stapelsignatur) sorgt für Akzeptanz und flüssige Arbeitsabläufe.

In **mobilen Szenarien**, etwa bei Haus- oder Heimbefuchen, ist das Signieren mit der heutigen TI **faktisch nicht umsetzbar**. Ärztinnen und Ärzte können E-Rezepte oder andere signaturpflichtige Dokumente nicht direkt vor Ort ausstellen. Stattdessen müssen sie anschließend in die Praxis zurückkehren, die Dokumentation nacharbeiten und die Signaturen mittels gestecktem HBA ausführen.

4.2.3 Anforderungen

Tabelle 3 fasst die zentralen Anforderungen an den (Fern-)Signaturdienst zusammen. Diese ergänzt die Anforderungen der Authentisierung mittels digitaler Identitäten.

Tabelle 3: Fachliche Anforderungen der (Fern-)Signatur

No.	Fachliche Anforderung an die digitale Identität (Signatur)
Sign-1	Mobile Nutzbarkeit innerhalb der Institution (Arbeitsplatzwechsel)
Sign-2	Mobile Nutzbarkeit außerhalb der Institution (remote)
Sign-3	Keine Spezialhardware erforderlich
Sign-4	Wahl des Mittels zur Signaturfreigabe innerhalb der Institution (Smartphone oder physische Smartcard)
Sign-5	Mehrere Dokumente müssen in einem Arbeitsgang digital signiert werden können (analog der Stapelsignatur)
Sign-6	Die Signaturfunktion muss im Hintergrund laufen können, sodass die Weiternutzung des PS möglich ist
Sign-7	Die Signatur muss in „Echtzeit“ erfolgen können (ohne Wartezeit für z.B. zeitnahe Einlösung des eRezepts)
Sign-8	Nicht-ärztliches Personal muss Dokumente für die Aufbringung einer QES durch den Arzt vorbereiten können, um den Arbeitsablauf des Arztes effizienter zu gestalten

Sign-9	Intuitive Nutzerführung mit geringer Nutzerinteraktion (wenige Klicks / Bestätigungen / PIN-Eingaben)
Sign-10	Hochverfügbarkeit
Sign-11	Die Signatur mehrerer Dokumente über einen definierten Zeitraum muss mindestens, analog der Nutzung und Vorgaben zur Komfortsignatur, möglich sein

4.3 Umsetzung (Fern-)Signaturdienst

4.3.1 Systemüberblick

Ziel dieses Konzepts ist die Bereitstellung eines zentralen (Fern-)Signaturdienstes, der die bestehenden Signaturverfahren modernisiert und die spezifischen Anforderungen des Gesundheitswesens erfüllt. Hierzu zählen insbesondere die Unterstützung von Signaturvorgängen sowohl in Remote- als auch in Vor-Ort-Szenarien sowie die Bereitstellung der für das Gesundheitswesen essenziellen Komfortsignatur. Aufgrund der hierfür erforderlichen hohen Sicherheits- und Schutzanforderungen sowie der damit verbundenen komplexen technischen und organisatorischen Maßnahmen ist eine entsprechende Fernsignaturlösung derzeit am Markt nicht verfügbar. Daher ist der Aufbau eines dedizierten (Fern-)Signaturdienstes erforderlich, der speziell auf die Anforderungen des Gesundheitswesens ausgerichtet ist und perspektivisch auch über den Kreis der heutigen HBA-Inhaber hinaus genutzt werden kann.

Die Gesamtarchitektur zur Signaturerstellung über einen (Fern-)Signaturdienst ist in Abbildung 4 dargestellt.

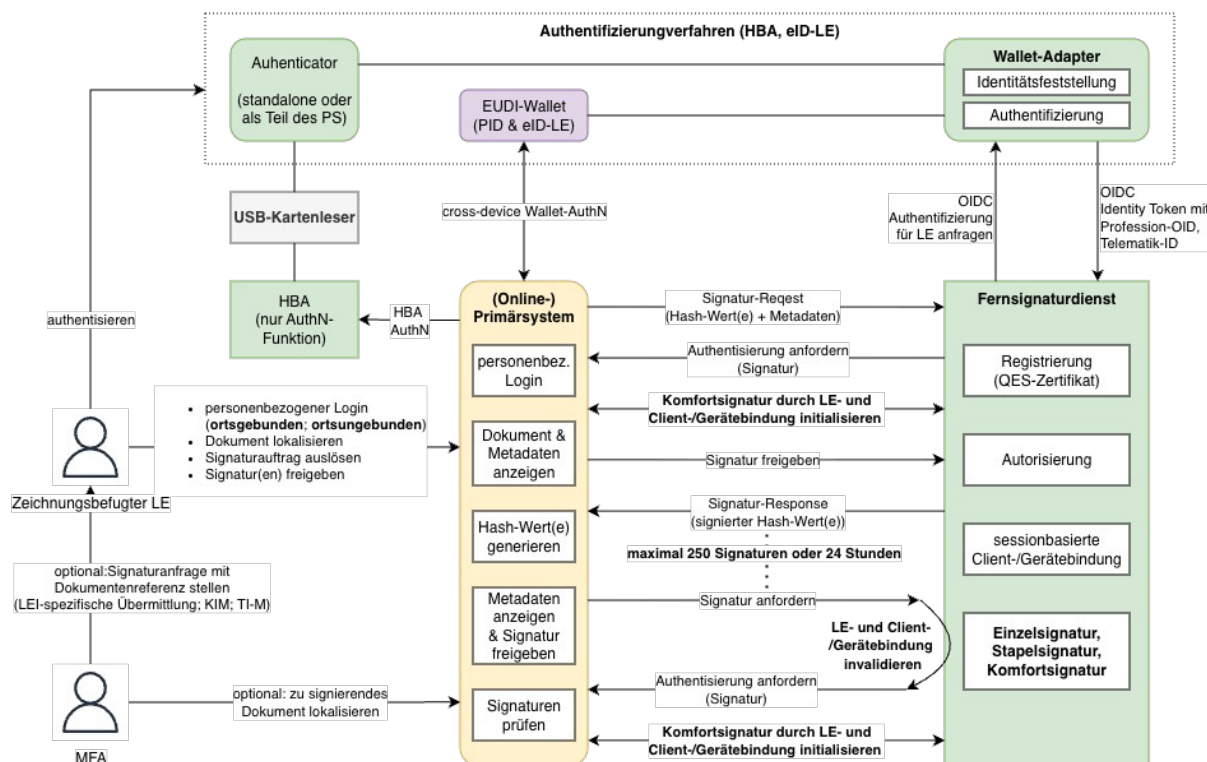


Abbildung 4: Systemüberblick Signaturerstellung über (Fern-)Signaturdienst

4.3.2 Interaktionsübersicht:

Die Einführung eines solchen (Fern-)Signatordienstes ermöglicht das Signieren von Dokumenten sowohl vor Ort als auch von einem Remote-Arbeitsplatz (Rufbereitschaft im Home-Office, beliebiger Arbeitsplatz bspw. in einer Klinik) oder einem beliebigen Ort (Hausbesuch, Pflegeheim).

Die entsprechend zugehörigen Interaktionen eines umfassenden Standardablaufs könnte wie folgt aussehen:

1. Der zeichnungsbefugte Leistungserbringer registriert sich am (Fern-) Signatordienst unter Nutzung der eID-LE (mittels Wallet-Adapter und EUDI-Wallet) oder dem HBA, woraufhin ein entsprechendes Signatur-Zertifikat mit Telematik-ID und ProfessionOID erstellt und auf diesen Leistungserbringer registriert wird.
2. Optional: Delegierung der Signaturanfrage:
 - a. Eine Person (bspw. MFA) mit Zugang zum Primärsystem (PS) löst eine Signaturanfrage für ein oder mehrere med. Dokumente durch Übermittlung (bspw. via PS, KIM o. TI-M) einer Dokumenten-Referenz (bspw. einen Link) an einen zeichnungsbefugten Leistungserbringer aus.
 - b. Der Leistungserbringer öffnet den Link.
3. Der Leistungserbringer meldet sich von seinem Arbeitsplatz (vor Ort, zu Hause, am Ort des Patienten, in einem anderen Gebäude/Raum der LEI) mittels PC, Laptop, Smartphone am (Online-) Primärsystem mit den Authentisierungsmitteln der LEI oder des Auftragsverarbeiters an (die technische Ausgestaltung ist nicht Bestandteil der TI).

4. Der Leistungserbringer lokalisiert das zu signierende Dokument im PS, initiiert einen Signaturauftrag und wählt ggf. den Signaturtyp (Einzel-, Stapel-, Komfortsignatur). Daraufhin erstellt das PS den Hash-Wert des Dokuments, fügt es zusammen mit den Metadaten (bspw. „Arztbrief“ und/oder „Signaturauftragsnummer“ und „Dokumenten-ID“) sowie den Anmeldedaten des LE am PS und löst die Bestätigungsanfrage am (Fern-)Signaturdienst aus.
5. Der (Fern-)Signaturdienst fordert via Wallet-Adapter eine Authentifizierung des Leistungserbringers mit der EUDI-Wallet an.
[Alternativ: Der (Fern-)Signaturdienst fordert via Wallet-Adapter und PS (oder Authenticator App) eine Authentifizierung des Leistungserbringers mit HBA an.]
6. Der Leistungserbringer authentifiziert sich durch die Cross-Device Authentifizierungsmechanismen der EUDI-Wallet (bspw. QR-Code Scan vom PS) sowie der Eingabe einer 6-stelligen Wallet-PIN an seinem persönlichen Smartphone.
[Alternativ: Der Leistungserbringer authentifiziert sich durch Eingabe der 6-stelligen HBA-PIN an einem USB-Kartenterminal (PS oder Authenticator App und jeweils ein USB-Kartenterminal müssen an jedem Arbeitsplatz mit HBA-Authentisierung installiert sein).]
7. Der (Fern-)Signaturdienst etabliert für den Signaturtyp „Komfort“ eine Komfortsignatur-Session durch kryptografische Bindung des Primärsystems an die Authentifizierung des Leistungserbringers. Nun kann der Leistungserbringer mehrere Signaturen über einen längeren Zeitraum durchführen, ohne sich erneut authentifizieren zu müssen.
8. Die Freigabe der einzelnen Signaturen (und Stapel) erfolgt nach Prüfung der Metadaten über das PS mittels Dialogfenster und „One-Click“. Das PS erhält jeweils den signierten Hash-Wert als Antwort vom (Fern-)Signaturdienst und bettet diese in das Dokument ein.
9. Nach Ablauf der Komfortsignatur-Session setzt der (Fern-)Signaturdienst eine erneute Authentifizierung und Neuaushandlung der Komfortsignatur-Sitzung durch.

5 Planung benötigter Produkte und Dienste

Dieses Kapitel beschreibt die Grobplanung der für die eID-LE sowie die (Fern-)Signatur benötigten Dienste als Roadmap für deren schrittweise Einführung. Grundlegende Aspekte wie die Beauftragung und die damit verbundenen Vergabeverfahren für die beiden neuen zentralen Dienste sowie die erforderlichen beziehungsweise gewünschten Zeiträume eines Parallelbetriebs bestehender und neuer Lösungen sind wesentliche Bestandteile der Gesamtplanung.

Zur weiteren Detaillierung der hier beinhalteten Planungen sind weitere Abstimmungsprozesse sowohl mit den Gesellschaftern der gematik als auch mit weiteren Stakeholdern erforderlich. Dies betrifft beispielsweise das BMDS mit der Roadmap zur EUDI-Wallet, das BSI hinsichtlich der sicherheitstechnischen Umsetzung unter anderem der Komfortsignaturfunktion sowie die EHDS-Durchführungsrechtsakte auf EU-Ebene. Diese Abstimmungen sind von zentraler Bedeutung, da sie die fachlichen, regulatorischen und technischen Rahmenbedingungen der Einführung maßgeblich beeinflussen.

Insgesamt verfolgt die gematik das Ziel, bestehende Dienste oder Funktionen erst dann abzulösen, wenn die entsprechenden Nachfolgelösungen ausreichend erprobt und im Realeinsatz etabliert sind. Im Rahmen der Ausgestaltung der Einführungs- und Migrationsplanung für die hier betrachteten neuen TI-Dienste werden daher auch Ressourcenbedarfe, Meilensteine, Risiken sowie Maßnahmen zur Sicherstellung eines geordneten Übergangs berücksichtigt. Vorrangiges Ziel ist es, die Nutzbarkeit der eID-LE und des (Fern-)Signaturdienstes ab 2029 in der Versorgung zu ermöglichen.

5.1 eID-LE: Wallet-Adapter mit VC-Provisionierung

Der in Kapitel [3.3 - Umsetzung eID-LE mittels Wallet-Adapter](#) beschriebene zentrale Dienst "Wallet Adapter" zur Umsetzung der eID-LE soll als Vergabe eines neuen Produkts der TI umgesetzt werden. Die Einführung der eID-LE erfolgt im Rahmen einer schrittweisen Modernisierung und perspektivischen Ablösung des bestehenden IDP-Dienstes. Hierfür ist ein stufenweises Migrationsvorgehen vorgesehen, das einerseits die kontinuierliche Bereitstellung der weiterhin benötigten Bestandsfunktionen des aktuellen IDP-Dienstes sicherstellt und andererseits die Einführung neuer Funktionalitäten ermöglicht.

Eine erste zeitliche Planung zur Umsetzung der vorgeschlagenen Lösung (siehe Abbildung 5) avisiert eine Erlebbarkeit der eID-LE im Wirkbetrieb ab Q1 2029 (Pilotierung Q4 2028). Die Planung sieht vor, dass der derzeitige IDP-Dienst bzw. Teile von dessen Funktionalitäten zur Nutzung von HBA und SM(C)-B im neu zu beschaffenden zentralen Wallet-Adapter aufgehen und daher während einer Migrationsphase ein Parallelbetrieb bestehen wird. Der Parallelbetrieb der erforderlichen Bestandsfunktionen des IDP-Dienstes wird bis zur kompletten Migration aller Anwendungen auf den neuen Dienst aufrecht erhalten. Die funktionale Trennung zwischen neuen Wallet- und Bestandsfunktionen und die regelmäßige Bewertung der Erforderlichkeit von Funktionen ermöglicht eine bedarfsgerechte Bereitstellung des Wallet-Adapters mit Hinblick auf Umfang und Ressourcen.

Eine Ausdifferenzierung der Aufgaben und Präzisierung der Meilensteine ergibt sich im Rahmen der weiteren Spezifikationsphase. Die Detailplanung sieht eine stufenweise Umsetzung der Bestandsfunktionen sowie der neu zu schaffenden Wallet-Funktionen vor, deren Priorisierung sich an der jeweiligen zeitlichen Kritikalität orientiert. Dabei ist zu

beachten, dass die zeitliche Planung durch Änderungen der fachlichen, regulatorischen und technischen Rahmenbedingungen beeinflusst werden kann.

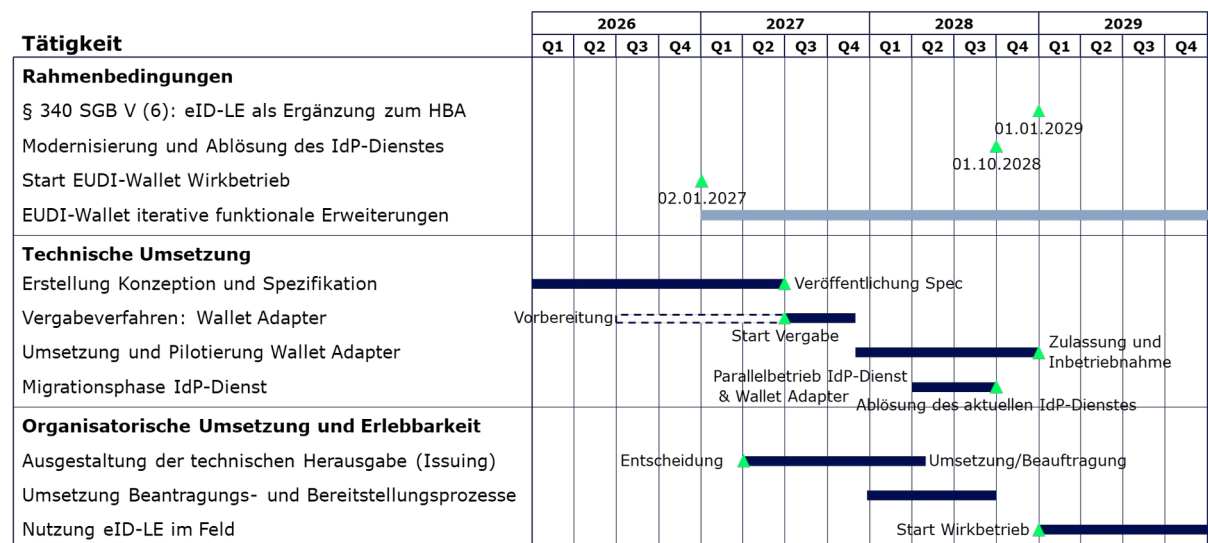


Abbildung 5: Grobplanung eID-LE

5.2 (Fern-)Signaturdienst

Der in [4.3- Umsetzung \(Fern-\)Signaturdienst](#) stellt zwar einen neu zu schaffenden TI-Dienst dar, führt jedoch kein neues fachliches Signaturverfahren ein. Vielmehr basiert er auf den etablierten und im Versorgungsgeschehen bewährten Signaturprozessen der Telematikinfrastruktur und überführt diese in eine modernisierte technische Zielarchitektur. Die heute verfügbare Komfortsignatur dient dabei als fachliches Vorbild. Der (Fern-)Signaturdienst stellt somit primär eine Weiterentwicklung der technischen Umsetzung bestehender Signaturverfahren dar, um diese künftig auch ortsunabhängig und mobil, insbesondere unter Nutzung der eID-LE, bereitstellen zu können. So wird ein bewährtes Verfahren in eine zukunftsfähige Architektur überführt, die langfristig die Ablösung der heutigen HBA- und konnektorbasierten technischen Umsetzung ermöglicht. Eine erste zeitliche Planung zur Umsetzung der vorgeschlagenen Lösung (siehe Abbildung 6) avisiert eine Erlebbarkeit der (Fern-)Signatur ab Q1 2029 (Pilotierung Q4 2028).

Die Nutzung des (Fern-)Signaturdienstes soll mit dem HBA, der SM(C) und eID-LE als Authentisierungsmittel gleichermaßen möglich sein. Die nachstehende Planung berücksichtigt die mittelbare Abhängigkeit des (Fern-)Signaturdienstes zur eID-LE. Die eID-LE stellt eine wesentliche Voraussetzung für die Nutzung des (Fern-)Signaturdienstes in mobilen Versorgungsszenarien dar und ist damit erforderlich, um die angestrebten Mehrwerte ortsunabhängiger Signaturprozesse zu realisieren. Der volle Nutzen des Signaturdienstes kann daher insbesondere in der mobilen Versorgung erst durch die Bereitstellung und Einbindung der eID-LE entfaltet werden. Aus diesem Grund soll der (Fern-)Signaturdienst zeitlich parallel zur eID-LE verfügbar sein, sodass dieses zentrale Anwendungsszenario unmittelbar mit Einführung der eID-LE genutzt werden kann.

Eine Abkündigung der Signaturfunktion des HBA ist erst dann vorgesehen, wenn sich die eID-LE und der neue (Fern-)Signaturdienst im Versorgungsalltag etabliert haben und ihre Praxistauglichkeit sowie Betriebssicherheit nachgewiesen sind. Daran anschließend kann eine Migrationsphase eingeleitet werden, in der die derzeit über HBA und Konnektor bereitgestellten Signaturfunktionen schrittweise und flächendeckend auf den neuen Signaturdienst überführt werden. Mit Abschluss dieser Migration könnte der HBA um

seine Signaturfunktionalität verschlankt werden. Aus Sicht der Migrationsplanung erscheint es dabei naheliegend, die Abkündigung der HBA-basierten Signaturfunktion zeitlich mit der Ablösung des Einbox-Konnektors zu synchronisieren.

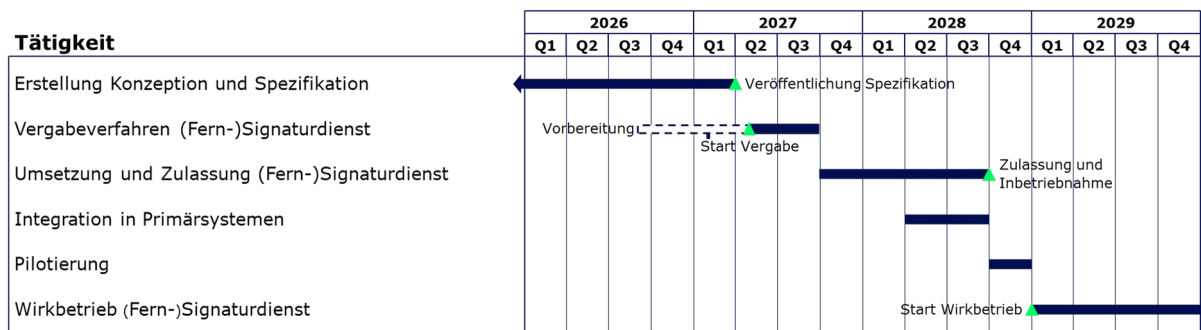


Abbildung 6: Grobplanung (Fern-)Signaturdienst

6 Weiterführende Klärung und thematische Abgrenzung

Das vorliegende Grobkonzept benennt nachstehend Themen, die der weiterführenden Klärung bedürfen oder inhaltlich von diesem Konzept begründet abzugrenzen sind.

6.1 Weiterführende Klärungsbedarfe

Dieser Abschnitt erörtert noch offenen Fragestellungen zur Ausgestaltung des hoheitlichen Wallet-Ökosystems sowie der Umsetzbarkeit von Diensten und zeigt damit Bereiche auf, die im weiteren Verlauf gemeinsam mit den Gesellschaftern der gematik sowie Stakeholdern zu klären bzw. auszugestalten sind.

6.1.1 Rolle der Attributsbestätigenden Stellen und des Wallet Adapters

Nach Auffassung der gematik lässt – aufgrund aktuell noch fehlender offizieller sowie klarer Festlegungen für diesen Fall – die Rolle der attributsbestätigenden Stellen zwei Ausgestaltungsmöglichkeiten zu. Einerseits könnten die gemäß §340 SGB V zu benennenden Stellen, als die zu registrierenden Pub-/QEAA Provider direkt auftreten. Andererseits könnte ein beauftragter Dienstleister als Pub-/QEAA Provider fungieren und die zu benennenden Stelle als Authentische Quelle. Die Klärung der Rollen werden mit dem BMDS und den Gesellschaftern zeitnah vorangetrieben. Dies betrifft auch die Klärung der Details zu Registrierungsverfahren der Relying Partys und Pub-/QEAA Provider.

Für den Bereich des Issuing wäre es technisch möglich, einen zentralen Issuing Dienst des Bundes zu verwenden, wenn dieser entsprechende Pub-EAA-Provider registriert und eine Definition des Nachweisschemas bekannt ist. Ob und unter welchen Rahmenbedingungen so eine Nachnutzung dieses Dienstes möglich ist, wird im Zuge des Aufbaus mit dem BMDS geklärt. Prinzipiell wäre es auch möglich, dass die benannten Stellen nach § 340 SGB V in Eigenverantwortung die eID-LE in Form von VC in die Wallet einbringen und somit auf eine zentrales Issuing mittels Wallet Adapter verzichtet wird. *Die gematik und ihre Gesellschafter prüfen die bestgeeignete Umsetzung der technischen Herausgabe des VC sowie dafür notwendige Komponenten und Prozesse.*

6.1.2 Machbarkeit der Komfort-Fernsignatur

Für die generelle Machbarkeit ist aus der technischen Perspektive die Sicherstellung der alleinigen Kontrolle des Signaturschlüssels durch den Signierenden ohne erneute Authentifizierung für jede einzelne Signatur essenziell. Diese alleinige Kontrolle wird durch die kryptografische Bindung der Komfortsignatur-Sitzung an den Signierenden, das PS und den (Fern-)Signaturdienst ermöglicht. Die Bindung an den Signierenden erfolgt durch das Übermitteln einer vom PS erzeugten und an die PS-Sitzung gebundene User-ID (analog zur heutigen Komfortsignatur) an den (Fern-)Signaturdienst. Die kryptografische Bindung des PS bzw. dessen IT-Gerät kann bspw. mit den Mechanismen des ZETA-Client und ZETA-Guard der TI ermöglicht werden. Konkret werden die Bindungsdaten nach erfolgreicher Authentifizierung Teil der dynamischen und sitzungsspezifischen „Signature Activation Data“ (SAD) zur Freischaltung des entsprechenden Signaturschlüssel im Hardware-Sicherheitsmodul (HSM) für den Komfortsignatur-Anwendungsfall. Die

Bindungen werden nach jeder PS- oder Komfortsignatursitzung invalidiert und nur mit erneuter Authentifizierung des Signierenden erneuert.

Um regulatorische Anforderungen und Herausforderungen zu identifizieren und diesen frühzeitig zu begegnen, wurde bereits der Dialog mit den entsprechenden Stakeholdern aufgenommen. In den kommenden Umsetzungsschritten wird die gematik mit der BNetzA, dem BSI und BfDI weiter in den Austausch treten.

6.1.3 BYOD

Es muss prinzipiell ein persönliches Gerät genutzt werden, welches mit der Wallet App eine Gerätebindung eingeht und dadurch dem Nutzer eindeutig zugeordnet werden kann. Die Wallet richtet sich dabei an natürliche Personen und kann grundsätzlich entweder auf einem beruflichen oder auch dem privaten Smartphone genutzt werden. Der Klärungsprozess des BMDS zum Gestaltungs- bzw. Nutzungsspielraum der EUDI-Wallet dauert an: es steht zur Entscheidung, ob es Nachweise (Credentials) auf einem hohen Vertrauensniveau geben soll, die so spezifiziert sind, dass diese nur einmal oder n-mal genutzt werden können. Letzteres würde eine Nutzung der (gleichen) Nachweise in mehreren Wallets bzw. auf mehreren Endgeräten ermöglichen – privater und oder dienstlicher Natur. Zum aktuellen Zeitpunkt liegen Informationen vor, welche die Nutzbarkeit solcher Nachweise in einer begrenzten Anzahl Wallets ermöglichen soll. Die finale Entscheidung ist jedoch noch ausstehend.

6.1.4 Signaturfunktion des HBA

Der HBA könnte mit dem Wegfall der Notwendigkeit für ein Signaturzertifikat auf der Chipkarte perspektivisch verschlankt bzw. neu ausgestaltet werden. Der HBA wäre dann lediglich Authentisierungsmittel. Ob eine Verschlinkung des HBA stattfinden soll, gilt es im Weiteren zu bewerten. In jedem Fall wird eine Abkündigung der HBA-Signaturfunktion erst geplant, wenn die eID-LE und Fernsignatur sich im Feld etabliert und bewährt haben.

6.1.5 Verschlüsselungsfunktion des HBA

Aktuell sind knapp 230.000 HBA im Einsatz. Davon sind lediglich 379 mit einem KIM-Postfach verknüpft (KIM-Postfach mit HBA-VZD Eintrag inkl. ENC-Zertifikat). Es gibt demnach rund 400 potentielle Nutzende der HBA-Verschlüsselung. Abseits davon liegen keine weitere Anwendungsfälle für die Verschlüsselung vor. Vor diesen Hintergrund wurde die Verschlüsselungsfunktion insgesamt auf Kosten und Nutzen hin bewertet und wird im Ergebnis für die eID-LE nicht fortgeführt.

6.2 Thematische Abgrenzung

6.2.1 Digitale Institutionsidentitäten (SMC-B)

Das vorliegende Konzept fokussiert auf die eID-LE, für die als Träger die EUDI-Wallet positioniert wird, dessen Nutzung sich ausschließlich an natürliche Personen richtet. Die EUDI-Wallet wird annehmlich zu Jahresbeginn 2027 nutzbar sein. Dahingegen sind die institutionsbezogenen Identitäten und deren digitale Weiterentwicklung nicht Teil der Betrachtung, da diese mit der HSM-B bereits Mitte dieses Jahres rechtskonform umgesetzt werden.

Die Europäische Business Wallet (EBW) kommt grundsätzlich als eine mögliche zukünftige Lösung in Betracht. Allerdings liegen aktuell weder hinreichend konkrete rechtliche und fachliche Vorgaben noch belastbare Spezifikationen zu ihrer Ausgestaltung und den vorgesehenen Zielgruppen vor. Ungeachtet dessen könnte die EBW perspektivisch eine tragfähige Grundlage für die Weiterentwicklung und Etablierung digitaler Institutionsidentitäten, beispielsweise in Form einer eID-LEI, bieten.

Obwohl das EBW derzeit noch mit Unsicherheiten verbunden ist, wird die Einführung einer eHealth Business Wallet im Gesundheitswesen zurzeit als strategisch bevorzugte Zielarchitektur für die digitale Identität von Leistungserbringerinstitutionen bewertet. Eine eHealth Business-Wallet bietet potenziell die beste Perspektive, eine nachhaltige, standardisierte Architektur zu schaffen, die über nationale Insellösungen hinausgeht und zusätzliche Mehrwerte wie z.B. das Teilen digitaler Nachweise, qualifizierte Siegel oder die Verwendung europäischer Zustelldienste ermöglicht. Des Weiteren wäre eine eHealth Business-Wallet EU-weit anschlussfähig und interoperabel, sodass es damit die Anforderungen aus eIDAS und EHDS langfristig adressiert. Das ermöglicht auch Synergieeffekte und die Wiederverwendung bestehender EU-Infrastrukturen, um langfristig systemische Kostensenkungen zu ermöglichen.

Unabhängig von einer zukünftig gewählten Lösungsarchitektur sollte mittelfristig über ein Ausphasen der SMC-B aufgrund der Kosten für Erneuerung und Austausch nachgedacht werden. Des Weiteren ist die SMC-B für den Dauerbetrieb als Identitätsträger nicht mehr zeitgemäß (PIN-Eingabe bei Unterbrechung/Fehler) und die weitere Abhängigkeit zu einem Kartenleser ist für den Server-Betrieb der TI 2.0 stabilitätskritisch. Eine Reduzierung der SMC-B Nutzer durch das TI-Gateway in Kombination mit dem HSM-B ist zu erwarten. Die heute noch wahrgenommene Notwendigkeit und Attraktivität der SMC-B wird durch die anderweitige Bereitstellung der Funktionen OSIG (durch den (Fern-)Signaturdienst) sowie ENC (durch eine einheitlich Kommunikationsplattform oder ggf. qualifizierte eIDAS-Dienste) gesenkt.

Die Zukunft digitaler Identitäten wird maßgeblich durch das EUDI-Ökosystem bestimmt. Eine konzeptionelle Umgestaltung der LEI-IDs wird daher die digitalen eID-LEs zukünftig berücksichtigen, um weitere Vorteile der Wallet und dessen Ökosysteme zu nutzen sowie z.B. flexible Organisationszugehörigkeiten und -wechsel zu unterstützen. Bis dahin ist es aus Sicht der gematik das primäre Ziel, die Verfügbarkeit der institutionsbezogenen digitalen Identität in Ausprägung HSM-B im Markt und damit eine nahtlose Kompatibilität zu gewährleisten. Insbesondere, um mobile Versorgungsprozesse einer breiten Anwendergruppe verfügbar zu machen.

6.2.2 Protokollierung

Die EHDS-VO verlangt von Electronic Health Record (EHR)-Systemen eine gemäß Artikel 9 und in Anhang II konkretisierte Identifizierung und Authentifizierung von Angehörigen der Gesundheitsberufe (AdGB). Dies dient dem Zweck einer personenbezogenen Protokollierung als Basis für die Wahrnehmung des Auskunftsrechts durch einen Patienten. Etwaige normative Änderungen sind zeitlich abhängig von noch ausstehenden Durchführungsrechtsakten auf europäischer Ebene, deren Finalisierung für März 2027 vorgesehen ist.

Die Konzeption der eID-LE und auch deren weitere Spezifikation kann unabhängig davon erfolgen, ob die rechtlichen Rahmenbedingungen sich im Weiteren ändern. Eine Klärung der nach EHDS-VO geforderten Protokollierung wird daher separat und unabhängig vom diesem Konzept erfolgen.

7 Anhang A - FAQ: Weiterführende Aspekte der eID-LE

Im Folgenden finden sich Fragen zu weiterführenden Aspekten der eID-LE, die im Konzept aufgrund des Umfangs der Lesbarkeit nicht verortet wurden.

A1 - Allgemeine Aspekte

A1.1 Wer profitiert von einer digitalen eID-LE?

Die Nutzung der eID-LE in der TI steht den gleichen Zielgruppen zu, die auch derzeit einen Heilberufs- und Berufsausweis beantragen können. Vor allem profitieren LE, die in Institutionen mit räumlichen Distanzen bzw. Wegen oder in Versorgungsszenarien außerhalb einer Institution tätig sind. Davon profitieren gleichermaßen auch die Institutionen selbst.

Krankenhäuser können diesen Vorteil nutzen, um weniger Personal am Ort der Versorgung zu benötigen oder kurzfristig dorthin bewegen zu müssen. Dies ist auch bereits auf einem verteilten Campus mit Distanzen von wenigen hundert Metern relevant. Konkret betrifft das z.B. Diensthabende Fachärzte oder anderweitige Bereitschaft sowie den a-priori mobilen Kontext einer Versorgung.

Profitieren werden auch vor allem ambulante Leistungserbringer, die Anwendungsfälle in der mobilen Versorgung durchführen oder in unterschiedlichen Institutionen tätig sind. Um in diesem Umfeld Dokumente signieren zu können, ist die Umsetzung der digitalen Leistungserbringeridentität und einer nicht physisch-verankerten Signatur notwendig.

A1.2 Wurden konkrete Nutzenden Erfahrungen zu den Vor- und Nachteilen einer eID-LE aus Vorarbeiten eingeholt?

Die gematik hat mit dem Proof of Concept (Pilotierung) eines TI-(Fern-)Signaturdienstes im Klinikumfeld bereits Feedback der Nutzenden sammeln können. Dieses Feedback lässt sich wie folgt zusammenfassen:

- Die Bereitstellung einer digitalen Identität wird als praktisch umsetzbar wahrgenommen.
- Die Beantragung und Nutzung einer Möglichkeit zum Signaturauslösen werden als niederschwellig wahrgenommen.
- Die Möglichkeit einer mobilen Nutzung der Signatur wird geschätzt.
- Die Möglichkeit einer Nutzung ohne Bindung an weitere Hardwarekomponenten (TI-Spezialhardware, z.B. eHealth-KT) wird geschätzt.

A1.3 Wie ordnet sich die eID-LE in die weiteren Entwicklungen der TI 2.0?

Die eID-LE ist Teil der Entwicklung zur TI 2.0 und unterstützt die Ablösung der LE-Authentifizierung von TI 1.0 Komponenten wie eHealth-KTs und Konnektortechnologien. Mit der aktuell vorgeschlagenen Lösungsoption bestehen keine Abhängigkeiten zur Roadmap zukünftiger TI 2.0 Komponenten.

Der hier empfohlene Lösungsansatz leistet der Strategie der TI 2.0 sowohl im Gesamtbild als auch im Hinblick auf die Stabilität Vortrieb. Es ist theoretisch begründet und Stand der aktuellen Diskussion, dass die Stabilität der TI besser zu kontrollieren ist, je weniger Dienste und Komponenten im Sinne der Identitätsbereitstellung und Abfrage genutzt werden. Folglich ist auch aus betrieblich-technischer Sicht die hier skizzierte Reduktion von Komplexität zu empfehlen.

A1.4 Werden durch die eID-LE Mehrbelastungen für LE im Alltag auftreten?

Die Freigabe einer Authentisierung erfolgt über die EUDI-Wallet App auf dem (persönlichen) Smartphone des Leistungserbringers. Die Freigabe von Signaturen erfolgt über den (Fern-)Signaturdienst, d.h. für die mobilen Use Cases auch mittels Authentisierung durch die Wallet App, ansonsten über das Primärsystem. Auch eine Komfortfunktion, bei der Signaturen über einem bestimmten Zeitraum ohne erneute Freigabe ausgelöst werden können, soll ermöglicht werden. Die zusätzlichen Handgriffe in der Wallet, welche Leistungserbringer mit der eID-LE ausführen müssten, sind als gering anzusehen oder ersetzen bestehende Interaktionen. Das Teilen oder Weitergeben von Geheimnis- (z.B. PIN) und Besitzfaktoren (z.B. des persönlichen Smartphones) bleibt, wie bereits heute, untersagt.

A1.5 Sieht die aktuelle Lösung eine potenzielle Einbindung weiterer Berufsgruppen ohne HBA, wie MFA und PTA als berufsmäßige Gehilfen vor?

Die Einbindung weiterer Berufsgruppen (z.B. MFA, PTA und weitere berufsmäßige Gehilfen) ist aus technischer und betrieblicher Perspektive leicht umzusetzen. Das bringt allerdings organisatorische Aufgaben und Hürden mit sich, die mit den entsprechenden Dachorganisationen, sofern solche existieren, zu klären sind. Im Zuge einer Betrachtung der adressierten Use Cases würde sich dabei im Zuge dessen auch die Frage nach der Handhabbarkeit stellen, wenn diese Use Cases nicht mehr wie heute über Organisationsidentitäten (SMC-B & HSM-B) abgebildet würden. Des Weiteren stellt sich insbesondere für nicht-verkammerte Berufsgruppen die Frage nach einer Attributbestätigenden Stelle und die Ausgabe von HBA für solche Berufsgruppen. Im Ergebnis wäre einer solchen Einbindung wohl umfassender gesetzlicher Regelungsbedarf vorlagert.

A1.7 Können „Doppel“-Approbationen abgebildet werden?

Aktuell benötigen doppel-approbierte Ärzte, z.B. aus der Mund-Kiefer-Gesichtschirurgie, zwei HBA, um in beiden Kontexten (Arzt und Zahnarzt) aktiv zu sein. In einer Wallet orientierten Lösung können in solchen Fällen zwei Nachweise in das Wallet eingebracht werden. Die Nutzung im Vergleich zum Handling zweier physischer Karten vereinfacht sich voraussichtlich leicht.

A2 - (Organisatorische) Voraussetzungen und Kosten

A2.1 Müssen den Leistungserbringern standardmäßig Dienst-Smartphones oder andere mobile Endgeräte zur Verfügung gestellt werden?

Nein. Es muss jedoch prinzipiell ein persönliches Gerät genutzt werden, welches mit der Wallet App, und damit der digitalen Identität, eine Gerätebindung eingeht und dadurch dem Nutzer eindeutig zugeordnet werden kann. Die Wallet richtet sich dabei an natürliche Personen und kann grundsätzlich auf einem beruflichen oder auch dem privaten Smartphone genutzt werden.

Die Wallet bietet dem Nutzer viele Funktionen, wie z.B. im digitalen Bürgerservice. Anwendungsfälle sind dabei vorwiegend von privater Natur. Freiberufler, wie Juristen aber eben auch Ärzte, sind dabei allerdings auch eher durch das private Wallet adressiert und nicht durch das Business Wallet, da sie im Gesundheitswesen vorwiegend als natürliche Person aktiv werden. Aufgrund der Gerätebindung kann ein Leistungserbringer die eID-LE (oder PID) für seine Identität auf nur wenigen verschiedenen Geräten gleichzeitig aktiv nutzen bzw. verwalten. Insofern ist es wahrscheinlich, dass ein Nutzer die EUDI-Wallet direkt auf seinem privaten Endgerät nutzen möchte.

A2.2 Bleibt die Konstellation der beteiligten Akteure an der Herausgabe und Attributs Bestätigung vergleichbar zum heutigen Stand (analog zum HBA)?

Idealerweise ändert sich am Herausgabeprozess der Leistungserbringeridentitäten wenig, um parallel HBA und eID-LE aus einer Hand bereitstellen zu können. Die attributbestätigenden Stellen, bei denen auch derzeit der Beantragungsprozess der HBAs

erfolgt, können – wie auch bisher – entweder selbst Kartenhersteller - und Attributs Provider bleiben bzw. werden oder Dienstleister damit beauftragen. Die gematik und ihre Gesellschafter prüfen die Ausgestaltung der technischen Herausgabe der eID-LE (Issuing) sowie dafür notwendige Komponenten und Prozesse. Eine zentrale Aufgabe der Attributsbestätigenden Stellen bleibt die Sicherstellung der Integrität der Telematik-ID und ProfessionOID.

A2.3 Wird der HBA weiter Bestand haben oder soll er mit der Einführung der eID-LE abgelöst werden?

§ 340 Abs. 6 SGB V gibt vor, die digitale Identität für Leistungserbringer *ergänzend* zum HBA bereitzustellen. Es wird davon ausgegangen, dass der HBA in einer explizit physischen Variante zunächst für bestimmte Zielgruppen und Anwendungsfälle notwendig bzw. vorteilhaft bleibt.

A2.4 Kann ein Leistungserbringer in Zukunft zwei Authentisierungsmittel für die TI erhalten, HBA und eID-LE?

Ja, laut gesetzlicher Vorgaben kann ein Leistungserbringer HBA und digitale Leistungserbringeridentität besitzen. Die Authentifizierung an den TI-Diensten muss mit beiden Authentisierungsmitteln möglich sein und wird über einen zentralen Dienst umgesetzt.

A2.5 Entstehen Leistungserbringern, die zukünftig beide Authentisierungsmittel nutzen wollen, doppelte Kosten? Wie werden diese refinanziert?

Bei einer parallelen Nutzung von HBA und digitaler Identität entstehen den Leistungserbringern Kosten für die Nutzung beider Ausprägungen der Identitäten. Da dies funktional nicht notwendig ist, ist die Annahme begründet auch weiterhin nur ein Authentisierungsmittel (HBA oder eID-LE) pro Leistungserbringer zu finanzieren. Da die präferiert vorgeschlagene eID-LE prinzipiell auch in anderen Kontexten außerhalb der TI verwendet werden kann, ergeben sich daraus ggf. dennoch Kostenvorteile für das Gesundheitswesen und den individuellen Nutzer.

A3 - Sicherheit

A3.1 Sind die Sicherheitsanforderung an die EUDI-Wallet hinreichend, um das in der TI notwendige Sicherheitsniveau zu gewährleisten?

Über das EUDI Trust Framework wird garantiert, dass die EUDI-Wallet und die Ökosystemteilnehmer das für die Anwendungen entsprechende Sicherheitsniveau, z.B. auch das Level of Assurance „high“, erfüllen. In die Entwicklung des Frameworks ist Deutschland als Mitgliedsstaat der EU involviert (z.B. über das BMDS). Die nationale Umsetzung wird zentral durch die SPRIN-D gesteuert und das EUDI-Wallet kostenlos aus einer hoheitlichen Infrastruktur heraus bereitgestellt.

Die genauen Sicherheitsanforderungen an die EUDI-Wallet, z.B. um ab 2028 eigene Entwicklungen aus der Industrie heraus zuzulassen, sind noch nicht bekannt. Jedoch wird die laufende Entwicklung für das zu nutzende nationale EUDI-Wallet (SPRIN-D Entwicklung mit Bundesdruckerei als PID-Provider) bereits jetzt durch unabhängige Stellen wie dem BSI begleitet und vor der Inbetriebnahme geprüft.

Auch in die Fragestellung auf welchen Geräten das EUDI-Wallet, abhängig von konkreten Hardwareparametern wie z.B. dem Secure Element, installiert werden kann sind auf nationaler Ebene die Experten, z.B. das BSI, involviert.

A3.2 Wie können eID-LEs gesperrt werden?

Die EUDI-Wallet sieht sowohl im europäischen Rahmen als auch ihrer nationalen Ausprägung bereits Mechanismen für die Verwaltung des Status und die Revokation von digitalen Identitätsdaten (PID) sowie der attestierten Nachweise vor.

Die Gültigkeit eines Nachweises (hier die eID-LE) wird durch den Aussteller (Pub-EAA/QEAA) oder eines in seinem Namen handelnden Dienstleisters über den Lebenszyklus des Nachweises verwaltet. Die Aussteller können einen Nachweis widerrufen, wenn die zugrunde liegenden Daten nicht mehr gültig sind oder die Identität aus sonstigen Gründen (z.B. vermutete Kompromittierung) gesperrt werden soll. Dies erfolgt über OCSP/CRL-ähnlichen Verfahren wie Statuslisten.

Im Rahmen der Authentifizierung der eID-LE durch den Wallet-Adapter prüft dieser die Gültigkeit und den Status der eID-LE mithilfe von standardisierten Methoden wie synchronisierter Statuslisten.

A3.3 Können Leistungserbringer eine eID-LE auf mehreren Geräten nutzen?

Ein LE kann voraussichtlich die eID-LE (oder PID) für seine Identität nur auf wenigen verschiedenen Smartphones gleichzeitig aktiv haben. Die staatliche EUDI-Wallet ist so konzipiert, dass sie eine sichere, eindeutige und vertrauenswürdige digitale Identität gewährleistet, die in der Regel an ein spezifisches, sicheres Gerät gebunden ist, um Missbrauch und Identitätsdiebstahl zu verhindern. Generell ist für die Nutzung auf mehreren Geräten, u.a. auch Desktop-PCs, die sogenannte Cross-Device-Authentifizierung vorgehen.

Die Implementierung der digitalen Identität beinhaltet starke Sicherheitsmechanismen, die das Wallet an das spezifische mobile Endgerät (z.B. Smartphone) koppeln, auf dem es aktiviert wurde. Eine gleichzeitige Speicherung und Nutzung derselben eID-LE auf beliebig vielen Geräten würde die für das Gesundheitswesen notwendigen Sicherheitsmechanismen untergraben.

8 Anhang B - Verzeichnisse

B1 - Abkürzungen

Kürzel	Erläuterung
AdGB	Angehörige der Gesundheitsberufe
ARF	Architecture Reference Framework
eAU	elektronische Arbeitsunfähigkeitsbescheinigung
EBK	Einbox-Konnektor
EBW	European Business-Wallet
eGK	elektronische Gesundheitskarte
EHDS	Europäischer Gesundheitsdatenraum (European Health Data Space)
eHealth-KT	eHealth-Kartenterminal
EHR-System	Electronic Health Record (EHR)-System
eIDAS	Verordnung über elektronische Identifizierung und Vertrauensdienste
eID-LE	Digitale Leistungserbringeridentität
EUDI-Wallet	Europäische digitale Identitäts-Wallet
HBA	Elektronischer Heilberufsausweis
HSK	Highspeed-Konnektor
HSM-B	Institutionsidentität (Hardware Security Module)
IDP	Identity Provider (Teilkomponente eines IAM)
LE	Leistungserbringer
LEI	Leistungserbringerinstitution
MFA	Medizinische Fachangestellte
MVZ	medizinisches Versorgungszentrum
NFC	Near Field Communication

OIDC	OpenID Connect
OpenID4VC	OpenID for Verifiable Credentials
OpenID4VCI	OpenID for Verifiable Credential Issuing
OpenID4VP	OpenID for Verifiable Presentation
PID	Personal Identification Data
Profession OID	ID der Berufsgruppe
PS	Primärsystem
Pub-EAA	Public Electronic Attestation of Attributes Provider
QEAA	Qualified Electronic Attestation of Attributes
QES	Qualifizierte elektronische Signatur
QSCD	Qualified Signature Creation Device
QTSP	Qualified Trust Service Provider
SAD	Signature Activation Data
SM(C)-B	Security Module (Card) Typ B (Institutionskarte, Praxiskarte)
SPRIN-D	Bundesagentur für Sprunginnovation in Deutschland
SSO	Single Sign-On
VC	Verifiable Credentials
VCI	Verifiable Credentials Issuing
VP	Verifiable Presentation
VZD	Verzeichnisdienst
ZETA	Zero Trust Access

B2 - Abbildungsverzeichnis

Abbildung 1: Systemüberblick zur eID-LE.....	16
Abbildung 2: Systemüberblick zur digitalen Identität in der LEI.....	20
Abbildung 3: Systemüberblick zur kartengebundenen Identität (HBA).....	22
Abbildung 4: Systemüberblick Signaturerstellung über (Fern-)Signaturdienst.....	26
Abbildung 5: Grobplanung eID-LE.....	29

1153	Abbildung 6: Grobplanung (Fern-)Signaturdienst.....	30
------	---	----

1154

1155

1156 **B3 - Tabellenverzeichnis**

1157	Tabelle 1: <i>Rechtliche Vorgaben an die digitale Identität (Authentisierung)</i>	12
------	---	----

1158	Tabelle 2: <i>Fachliche Anforderungen an die digitale Identität (Authentisierung)</i>	14
------	---	----

1159	Tabelle 3: <i>Fachliche Anforderungen der (Fern-)Signatur</i>	24
------	---	----

1160

1161