Elektronische Gesundheitskarte und Telematikinfrastruktur

Implementierungsleitfaden Primärsysteme ePA für alle

Version:	3.2.0
Revision:	950781
Stand:	12.07.2024
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemILF_PS_ePA

Dokumenteninformationen

Änderungen zur Vorversion

Anpassungen des vorliegenden Dokumentes im Vergleich zur Vorversion können Sie der nachfolgenden Tabelle entnehmen.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
3.0.0	30.01.2024		ePA für alle	gematik
3.1.0	28.03.2024		ePA für alle - Release 3.0.1	gematik
3.2.0	12.07.2024		ePA für alle - Release 3.0.2 (Ergänzung Kapitel1 und 2, Überarbeitung Kapitel 6)	gematik

Inhaltsverzeichnis

1 Einordnung des Dokumentes

1.1 Zielsetzung

Die vorliegende Spezifikation definiert Anforderungen zu Erstellung, Test und Betrieb derjenigen Anteile eines Primär- oder Clientsystems, die zur Nutzung der ePA für alle erforderlich sind.

Technische Standards werden in der ePA verwendet, um Interoperabilität zu steigern und die technischen Voraussetzungen zur Nutzung der Anwendung zu legen. Auf Seiten der Primärsystemhersteller eröffnet die Verwendung von Standards die Chance, wiederverwendbare Schnittstellen zu entwickeln bzw. zu nutzen und einzelne Module austauschbar zu gestalten.

Zum Zweck der Implementierungshilfe werden grundlegende Konzepte und Anwendungsfälle der ePA für alle aus der Sicht der PS-Hersteller erläutert. Dabei werden nicht nur Anwendungsfälle der ePA erläutert, sondern auch praktische Umsetzungshinweise gegeben und auf entsprechende Beispiele verwiesen.

1.2 Zielgruppe

Das Dokument ist maßgeblich für Hersteller von Primärsystemen, welche die Schnittstellen der ePA für alle nutzen. Dieses Dokument kann ebenfalls als Referenz genutzt werden von TI-Verantwortlichen in Leistungserbringerinstitutionen, von Produktmanagern, UX/UI-Designern und von Schulungsverantwortlichen.

Falls ein Primärsystem bisher das technische Framework von IHE noch nicht verwendet, wird es durch diesen Implementierungsleitfaden in die Lage versetzt, die ePA-Schnittstellen IHE-konform zu verwenden.

Falls ein Primärsystem das technische Framework von IHE bereits verwendet, schildert der Implementierungsleitfaden ihm die relevanten Einschränkungen des IHE-Frameworks, die für die ePA der Telematikinfrastruktur von Relevanz sind. Die IHE-Konformität dieser Schnittstellen ermöglicht ihm die Anbindung weiterer Anwendungen.

Mit der ePA für alle werden viele Schnittstellen als REST-Schnittstellen angeboten. Der Implementierungsleitfaden beschreibt die Umsetzung dieser Schnittstellen und der genutzten FHIR-Ressourcen.

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Bestätigungs- Zulassungs- oder Abnahmeverfahren wird durch die gematik GmbH in gesonderten Dokumenten (z. B. [gemPTV_ATV_Festlegungen], AFO-Steckbrief, Leistungsbeschreibung) festgelegt und bekannt gegeben.

Schutzrechts-/Patentrechtshinweis

Die nachfolgende Spezifikation ist von der gematik allein unter technischen Gesichtspunkten erstellt worden. Im Einzelfall kann nicht ausgeschlossen werden, dass

die Implementierung der Spezifikation in technische Schutzrechte Dritter eingreift. Es ist allein Sache des Anbieters oder Herstellers, durch geeignete Maßnahmen dafür Sorge zu tragen, dass von ihm aufgrund der Spezifikation angebotene Produkte und/oder Leistungen nicht gegen Schutzrechte Dritter verstoßen und sich ggf. die erforderlichen Erlaubnisse/Lizenzen von den betroffenen Schutzrechtsinhabern einzuholen. Die gematik GmbH übernimmt insofern keinerlei Gewährleistungen.

1.4 Abgrenzungen

Benutzte Schnittstellen werden in der Spezifikation desjenigen Produkttypen normativ beschrieben, der diese Schnittstelle bereitstellt. Auf die entsprechenden Dokumente wird referenziert (siehe auch Anhang 8.5).

Nicht Bestandteil des vorliegenden Dokumentes sind:

- Festlegungen zum Themenbereich Semantik von Metadaten, insoweit sie im Dokument [gemSpec_Aktensystem_ePAfueralle] beschrieben sind;
- Rendering-Vorschriften zur Form, in der ePA-Dokumente zur Anzeige gebracht werden (ggf. wird auf externe Festlegungen referenziert).

Die ePA fungiert als Sekundärdokumentation von Daten der Versicherten. Die Primärdokumentation der Versichertendaten im Primärsystem wird nur insoweit thematisiert, wie es für die Anbindung der ePA an das Primärsystem erforderlich ist.

1.5 Methodik

Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID sowie die dem RFC 2119 [RFC2119] entsprechend, in Großbuchstaben geschriebenen deutschen Schlüsselworten MUSS, DARF NICHT, SOLL, SOLL NICHT, KANN gekennzeichnet.

Anforderungen werden im Dokument wie folgt dargestellt:
<AFO-ID> - <Titel der Afo>
Text / Beschreibung
[<=]

Dabei umfasst die Anforderung sämtliche zwischen Afo-ID und Textmarke [<=] angeführten Inhalte.

1.6 Referenzen für die technische Entwicklung

Für die technische Entwicklung bietet die gematik Absprungpunkte an mehreren Stellen an:

- https://gematik.github.io/universal/index.html
- Dieses Projekt gibt einen Überblick über die Unterstützungsleistungen, die durch die gematik im Rahmen der Entwicklungen in der Telematikinfrastruktur bereitgestellt werden.
- https://gematik.github.io/universal/specifications.html
- In diesem Projekt befinden sich die Verlinkungen zu allen ePA relevanten Spezifikationsinhalten.

Der ePA liegen mehrere Dokumente zugrunde, die verschiedene Aspekte beschreiben:

- Das Fachkonzept [gemKPT_FK_ePAfueralle_V1.0.0_RC2] beschreibt die fachlichen Anforderungen an die ePA unter Berücksichtigung der geltenden Gesetzeslage.
- Die Konzeption und Spezifikationen beschreiben die normativen Festlegungen auf Produktebene, u.a.:
- https://github.com/gematik/ePA-Basic/tree/ePA-3.0
- https://github.com/gematik/ePA-Basic/blob/ePA-3.0/concept/concept.adoc
- https://github.com/gematik/ePA-XDS-Document/blob/ePA-3.0/concept/concept.adoc
- https://github.com/gematik/ePA-Medication/blob/ePA-3.0/concept/concept.adoc
- [gemSpec_Aktensystem_ePAfueralle_V1.1.0.pdf]
- Für Primärsystemhersteller werden die Anforderungen an die Umsetzung der ePA in den jeweiligen Clients zusammengefasst unter:
- Praxisverwaltungssysteme und Krankenhausinformationssysteme: [gemSST_PS_ePA_V_3.0.1-0_V1.0.0.pdf]
- Apothekenverwaltungssystem: [gemSST_PS_ePA_Apotheke_V_1.0.1-0_V1.0.0.pdf]
- DiGA: [gemSST_CS_ePA_DiGA_V_1.0.1-0_V1.0.0.pdf]
- Kostenträger: [gemSST_CS_ePA_KTR_V_1.0.1-0_V1.0.0.pdf]
- Ombudsstelle: [gemSST_CS_ePA_Ombudsstelle_V_1.0.1-0_V1.0.0.pdf]

Für die Softwareentwicklung kann auf das Repository der gematik zugegriffen werden:

- https://github.com/gematik/epa-deployment
- Das Projekt enthält einen Mock-Up des ePA Aktensystems (konkret VAU-Aufbau, IDP-Flow, Information-Service, Entitlement-Service und Medication-Service), welches zu Test- und Entwicklungszwecken genutzt werden.

1.7 Namenskonvention und IHE

Das IT Infrastructure Technical Framework von Integrating the Healthcare Enterprise (IHE) ist unter anderem Stand der Technik. Auf Basis der von IHE definierten Transaktionen des XDS.b-Integrationsprofils werden Anwendungsfälle über Schnittstellen zwischen den beteiligten Produkttypen und Komponenten umgesetzt.

Beim Einstellen eines Dokuments muss dieses gemäß IHE mit Metadaten (Autor, eindeutige Dokumentenkennung, Dateiformat etc.) versehen werden, die zusammen mit dem Dokument im XDS Document Service gespeichert werden. Ein oder mehrere Dokumente werden in IHE immer als Paket (sog. SubmissionSet) übertragen. Die Zugehörigkeit eines Dokuments zu einem SubmissionSet wird auch im XDS Document Service gespeichert, d.h., es ist ersichtlich, welche Dokumente von wem eingestellt wurden. Für die Anwendungsfälle zum Herunterladen und Löschen von Dokumenten muss zunächst eine Abfrage der Metadaten erfolgen, da in den Metadaten eine Referenz auf die Dokumente enthalten ist. Über diese Referenz können ein oder mehrere Dokumente heruntergeladen oder gelöscht werden. Ebenfalls kann der Anwendungsfall Aktualisieren von Metadaten umgesetzt werden.

Für einen Zugriff auf einmal eingestellte Dokumente stellt ein Client eine Suchanfrage ("Registry Stored Query" gemäß IHE), die sich immer auf das aktuelle ePA-Aktenkonto und die Metadaten der Dokumente bezieht. Eine Versicherten- bzw. ePA-Aktenkontenübergreifende Suche ("alle Versicherten mit den Eigenschaften...") ist nicht möglich. Der XDS Document Service liefert auf Wunsch pro Treffer den vollen Satz der

zum Dokument zugehörigen Metadaten oder eine Referenz zurück. Die Ergebnismenge kann vom Client nach den Wünschen des Nutzers nachgefiltert und sortiert werden.

1.8 Formate beim Einstellen von Dokumenten

Der XDS Document Service des ePA-Aktensystems unterstützt gemäß [gemSpec_Aktensystem_ePAfueralle#A_24854] folgende MIME-Type-Formate und Dateiendungen:

- application/pdf (nur PDF/A-1 und 2) (pdf)
- image/jpeg (jpeg oder jpg)
- image/png (png)
- image/tiff (tiff)
- text/plain (txt)
- application/xml (xml)
- application/hl7-v3 (xml)
- application/pkcs7-mime (p7)
- application/fhir+xml (xml)
- application/fhir+json (json)

Dokumente im PDF-Format werden vom XDS Document Service abgelehnt, da sie ausführbaren Code enthalten können. Daher müssen die Clients, falls sie Dokumente im PDF-Format einstellen wollen, diese gemäß A_24967-01 zunächst in ein PDF/A-Format konvertieren.

1.9 Medizinische Informationsobjekte

Die strukturiert in die ePA einzustellenden Inhalte werden nach § 355 SGB V von der Kassenärztlichen Bundesvereinigung (KBV) in der Form von medizinischen Informationsobjekten (MIO - https://mio.kbv.de/site/mio#tab-Rund+um+die+MIOs) festgelegt. Im Fachkonzept und in den Spezifikationen der gematik zur ePA werden zudem weitere Anwendungsfälle und strukturierte Datenformate beschrieben und benannt, die ebenfalls einzustellen sind (bspw. der eArztbrief der KBV oder auch Verordnungs- und Dispensierdaten des E-Rezepts).

1.10 Die ePA nach § 341 SGB V

Bei der elektronischen Patientenakte nach § 341 SGB V handelt es sich um eine Anwendung der Telematikinfrastruktur. Sie ist verpflichtend von den gesetzlichen Krankenkassen anzubieten. Die ePA setzt sich u.a. aus einem Server (ePA-Aktensystem) und einem Client zusammen (aus Sicht eines Leistungserbringers ist dies das Primärsystem). Für Leistungserbringer stellt ihr Primärsystem ihre Primärdokumentation zur Verfügung, während die ePA als versorgungsbegleitende Sekundärdokumentation anzusehen ist. Die gerichtete Kommunikation zwischen Leistungserbringern ist nicht der primäre Fokus der ePA; hierfür können u.a. die TI-Anwendungen Kommunikation im Medizinwesen (KIM) und der TI-Messenger genutzt werden. Für den Versicherten kann die

ePA ihre Primärdokumentation und ihren Speicherort für ihre eigenen Gesundheitsdaten und -dokumente darstellen. Der Systemüberblick der ePA wird in Kapitel 2 beschrieben.

Wenn ein Versicherter der ePA widersprochen hat, dann ergeben sich keine Nutzungsszenarien für Leistungserbringer im Umgang mit der ePA, wenngleich das Primärsystem auf das Vorhandensein einer ePA prüft. Wenn ein Versicherter der ePA nicht widersprochen hat, dann ergeben sich Lese- und Schreibmöglichkeiten und -pflichten für Leistungserbringer im Umgang mit der ePA. Die ePA ersetzt nicht die lokale Behandlungsdokumentation.

Aus Nutzersicht soll das Hochladen von Dokumenten in die ePA so einfach und schnell wie möglich gestaltet sein sowie doppelte Arbeitsschritte vermieden werden. Das PS soll den Nutzer dabei unterstützen. In der Benutzerführung soll für den Nutzer daher bei der Erstellung dieser Dokumentenarten sichergestellt werden, dass diese Dokumente standardmäßig ohne nachträgliche Metadateneingaben in die ePA eingestellt werden können.

Aufgrund gesetzlicher Vorgaben gibt es bestimmte Daten und Dokumentenkategorien, die verpflichtend von einem Leistungserbringer in die ePA des Versicherten hochgeladen werden müssen. Die Grundlage dafür findet sich je nach Leistungserbringergruppe u.a. in §§ 347, 348 und 349 SGB V.

Mit Verabschiedung des Digital-Gesetzes sind Leistungserbringer künftig zum Hochladen folgender Dokumente verpflichtet, wenn diese im Rahmen der Behandlung entstehen:

- Verordnungs- und Dispensierdaten (dies geschieht automatisch über den E-Rezept-Fachdienst, mit Implementierung des E-Rezepts muss aus Sicht des Primärsystems nichts weiter getan werden)
- Medikationsplan (mit Einführung der ePA 3.1)
- Krankenhaus-Entlassbrief (nach stationärer Behandlung, sowohl vorläufige als auch endgültige Version) (im PDF/A Format)
- Laborbefund (im PDF/A Format)
- Bildbefund (im PDF/A Format)
- Befundberichte aus invasiven oder chirurgischen sowie aus nicht-invasiven oder konservativen Maßnahmen (im PDF/A Format)
- eArztbrief (nach ambulanter Behandlung) (im PDF/A Format) (Empfehlung: aus dem KIM-Workflow heraus)

Die Verpflichtung zum Hochladen eines Dokuments steht in Abhängigkeit von dessen Inhalt. Enthalten Dokumente sensible Informationen, dann muss der Leistungserbringer seinen Patienten darüber informieren und sicherstellen, dass einem Hochladen nicht widersprochen wird. Gemäß §§ 347 und 348 SGB V handelt es sich hierbei um Informationen, die stigmatisierende Auswirkungen haben können wie beispielsweise sexuell übertragbare Infektionen, psychische Erkrankungen und Schwangerschaftsabbrüche. Bei Ergebnissen genetischer Untersuchungen oder Analyse muss gemäß § 353 (3) SGB V eine ausdrückliche Einwilligung zum Hochladen in schriftlicher oder elektronischer Form vorliegen.

Falls der Versicherte dem Hochladen eines Dokuments widerspricht, muss diese Entscheidung im Primärsystem nachprüfbar in der Behandlungsdokumentation protokolliert werden. Zusätzlich soll das betroffene Dokument im Primärsystem gekennzeichnet werden. Eine solche Kennzeichnung soll einfach hinterlegt und ebenso wieder entfernt werden können. Bevor eine Kennzeichnung entfernt wird, soll dem Nutzer des Primärsystems eine Warnung angezeigt werden. Beim Versuch des Hochladens eines gekennzeichneten Dokuments in ein ePA-Aktenkonto soll eine Hinweismeldung angezeigt und das Hochladen unterbunden werden.

Für Leistungserbringer mit einem unmittelbaren Patientenkontakt sollen von ihnen erstellte Dokumente direkt in das ePA-Aktenkonto hochgeladen werden. Für Leistungserbringer mit einem mittelbaren Patientenkontakt liegt unter Umständen kein technisch nachgewiesener Behandlungskontext vor und damit keine Möglichkeit Dokumente in das ePA-Aktenkonto einzustellen. Daher wird empfohlen, dass erstellte Dokumente von dem Leistungserbringer in das ePA-Aktenkonto hochgeladen werden, der den Befundbericht mit der Patient:in bespricht. Eine gesetzliche Regelung gibt es nicht, ob der Versender oder Empfänger eines Dokuments dieses in das ePA-Aktenkonto hochlädt.

Die Auflistung der Verpflichtungen wird mit den neueren Versionen dieses Implementierungsleitfadens stets aktualisiert.

2 Systemüberblick

2.1 Einführung

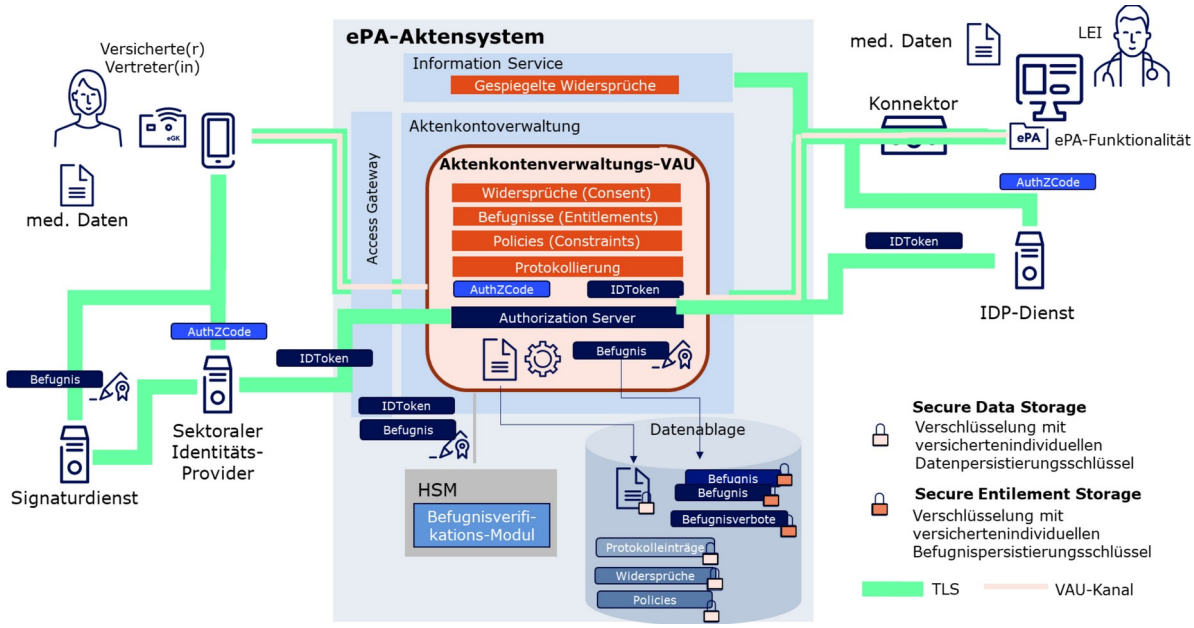

Abbildung 1: Überblick ePA für alle

Die zentralen Funktionen der ePA für alle sind das integre Management von wohl definierten Metadaten und den medizinischen Dokumenten als auch die Unterstützung von digitalen Versorgungsprozessen. Initial bedient das Aktensystem den **digital gestützten Medikationsprozess** durch die Bereitstellung einer elektronischen Medikationsliste (eML) an Leistungserbringer.

Das Primärsystem bietet einem Leistungserbringer, als Nutzer, den Zugang zur elektronischen Patientenakte des gesetzlich Versicherten an. Dabei greifen Leistungserbringer und Primärsystem über eine vertrauenswürdige Ausführungsumgebung (VAU) geschützt auf die elektronische Patientenakte zu und nicht mehr gekapselt über ein Konnektor-Fachmodul. Das in der ePA 2.x genutzte ePA-Fachmodul im Konnektor entfällt in der ePA für alle. Ein Zugang zur TI (mittels Konnektor oder TI-Gateway) ist zum Erreichen der Aktensysteme allerdings weiterhin erforderlich.

Wenn von dem "Aktenkonto" im Folgenden gesprochen wird, ist die ePA als Sekundärakte des Versicherten gemeint, nicht die "Primärakte" für den Versicherten im Primärsystem. Mit "Aktenanbieter" ist im Folgenden immer der Anbieter des ePA-Aktensystems gemeint. ePA-Aktensysteme können von mehreren Anbietern zur Verfügung gestellt werden, wobei die Dokumente eines einzelnen Versicherten immer genau bei einem Anbieter ePA-Aktensystem hinterlegt werden.

Die Nutzer der Primärsysteme der Leistungserbringer teilen sich die technische Infrastruktur der ePA in der Telematikinfrastruktur, folgen dabei den hier geschilderten Regeln der TI und bilden in diesem Sinne eine IHE-Affinity Domain, um ePA-Daten gesteuert durch die Befugnisvergabe des Versicherten auszutauschen. Dieser Datenaustausch erfolgt in vielerlei Hinsicht gemäß Festlegungen von IHE.

Die technische Infrastruktur der ePA besteht beim Leistungserbringer vor allem aus dem Konnektor, den Kartenlesegeräten und den Smartcards. Mit dem Konnektor stehen auch die Komponenten der Basis-TI, die zentrale TI und der Fach- und Basisdienste der TI zur Verfügung, etwa die Signaturfunktionalität, deren Nutzung durch das PS in [gemILF_PS] beschrieben sind.

Die Authentifizierung für die Zugriffe auf die ePA erfolgt durch den Identity Provider (IDP). Der Identity Provider (IDP) ist ein Nutzerdienst der TI-Plattform, welcher die Authentifizierung von Nutzern, die sich über eine Institutionskarte (SMC-B) ausweisen können, und die Bereitstellung bestätigter Identitätsmerkmale der Nutzer als Plattformleistungen ermöglicht. Der IDP authentifiziert den Nutzer anhand der kartenbasierten Identität und einer Signatur durch das Schlüsselmaterial auf der Karte (SMC-B) und stellt bei Erfolg einen IDP-Token für den Zugriff auf den Fachdienst aus.

Für einen Leistungserbringer liegt die Befugnis zur Nutzung der ePA des Versicherten vor, wenn ein **Behandlungskontext** besteht oder eine Befugnis über das ePA-FdV erteilt wurde.

Der Behandlungskontext wird im Rahmen von VSDM festgestellt, d. h. mit dem Stecken der eGK im Rahmen von VSDM.

Das Dokument [gemKPT_ePAfueralle] bietet einen Überblick zur ePA für alle.

2.2 Prozesssichten und Funktionsumfänge der Primärsysteme

Das Ziel der ePA für alle ist es, dass Informationen über Einrichtungs- und Sektorengrenzen hinweg ausgetauscht werden können, indem Daten und Dokumente in die ePA eingestellt werden. Die hierunter aufgeführten Prozessmodelle stellen generisch dar, wie digital gestützte Versorgungsprozesse in der Telematikinfrastruktur und unter Berücksichtigung der ePA in den jeweiligen Sektoren aussehen können. Die Darstellungen lehnen sich u.a. an die Ergebnisse des Arbeitskreises zur Analyse der Medikationsprozesse des Interop Councils und dem dort erarbeiteten Positionspapier (https://www.ina.gematik.de/mitwirken/arbeitskreise/analyse-der-medikationsprozesse) a n.

2.2.1 Behandlungskontext und Zugriffsbefugnisse

Damit eine Leistungserbringerinstitution mit der ePA arbeiten kann, braucht sie eine Zugriffsbefugnis. Befugnisse werden im Entitlement Management des ePA-Aktensystems verwaltet. Eine erstellte Befugnis muss im Primärsystem nicht vorgehalten werden. Die Befugnis liegt im ePA-Aktensystem vor und dieses prüft im Zuge des Aktenzugriffs aus einer LEI, ob diese zugriffsbefugt ist.

Eine Befugnis wird in einer einer Leistungserbringerumgebung erstellt, indem die eGK von einem gesetzlich Krankenversicherten eingelesen, eine Prüfziffer vom VSDM erzeugt und dieser HMAC signiert in das ePA-Aktensystem eingestellt wird. Das ePA-Aktensystem liefert eine Antwortnachricht validTo zurück, womit das zeitliche Ende der Befugnis bekannt gemacht wird. In der ePA-App können Befugnisse gelöscht oder in ihrer Gültigkeit angepasst werden, ebenso können dauerhafte gültige Befugnisse eingerichtet werden. Diese Einstellungen können vom Versicherten und von seinen Vertretern vorgenommen werden. Eine Änderung der Befugnis wird der LEI nicht aktiv mitgeteilt.

Eine Befugnis, die über das ePA-FdV eingestellt wird, wird mit dem Signaturdienst (SigD) signiert. Über die ePA-App und die Ombudsstelle kann auch ein Widerspruch gegen die Nutzung der Akte durch eine Leistungserbringerinstitution eingerichtet werden. Aus dieser Leistungserbringerinstitution heraus kann danach keine Befugnis mehr in die ePA eingestellt werden.

Bei Privatversicherten erfolgt die Berechtigungsvergabe für die ePA ausschließlich über die ePA-App. Um sicherzustellen, dass die für den Zugriff auf die ePA notwendige Krankenversicherungsnummer (KVNR) im Primärsystem vorliegt, führen die Versicherten einmal pro Einrichtung einen Online Check-in durch. Dabei initiieren sie über eine App-Funktionalität den Versand einer standardisieren KIM-Nachricht an die Einrichtung.

Im ePA-Aktenkonto liegt immer nur eine gültige Zugriffsbefugnis vor. Ein Primärsystem soll in jedem Fall den Versuch unternehmen eine Zugriffsbefugnis einzustellen. Das ePA-Aktenkonto nimmt immer die Zugriffsbefugnis an, für die eine längere Dauer vorliegt. Wenn ein Primärsystem bspw. versucht eine Zugriffsbefugnis für 90 Tage einzustellen und eine Zugriffsbefugnis vom Versicherten bereits eingestellt wurde, die über einen längeren Zeitraum Gültigkeit hat, dann gilt die Zugriffsbefugnis vom Versicherten.

Die Berechtigungsdauer für die Leistungserbringerinstitution steht im Zusammenhang mit der Berufsgruppe. Für Arztpraxen, Zahnarztpraxen und psychotherapeutische Praxen sowie Krankenhäuser, Reha-Kliniken und Pflegeeinrichtungen beträgt die Berechtigungsdauer standardmäßig 90 Tage. In Apotheken, für den öffentlichen Gesundheitsdienst und die Arbeits- und Betriebsmedizin beträgt die Berechtigungsdauer standardmäßig 3 Tage.

Beim Einlesen der eGK soll die Berechtigung automatisch erzeugt werden, d.h. die VSDM-Prüfziffer wird automatisch in das ePA-Aktenkonto des Versicherten eingestellt, damit die Leistungserbringerinstitution mit der ePA arbeiten kann. Der Prozess soll im Hintergrund laufen und das Primärsystem währenddessen weiterhin bedienbar sein. Eine grundsätzliche Notwendigkeit zum mehrfachen Einlesen der eGK während eines Quartals ergibt sich nicht. Mit dem erneuten Einlesen der eGK kann jedoch die Berechtigungsdauer erneuert und damit verlängert werden.

Wenn ein aktueller Behandlungskontext nicht (mehr) gegeben ist, weil z.B. die Berechtigungsdauer abgelaufen oder die Berechtigung entzogen wurde, können keine Dokumente in ein ePA-Aktenkonto eingestellt werden. Aus ärztlicher Sicht könnte bei Bedarf Kontakt zum Versicherten aufgenommen und um eine erneute Berechtigungsvergabe gebeten werden. Für langfristige oder permanente Behandlungssituationen wird das Erstellen einer Dauerbefugnis durch den Versicherten über die ePA-App empfohlen. Das Primärsystem kann zur Arbeitserleichterung eine Erinnerungsmöglichkeit anbieten, indem ein hochzuladendes Dokument auf eine Aufgabenliste gestellt oder zur Wiedervorlage gekennzeichnet wird.

2.2.2 Niedergelassener Sektor

2.2.2.1 Prozesssicht

In einer Arztpraxis, Zahnarztpraxis und psychotherapeutischen Praxis beginnt der Behandlungskontext grundsätzlich mit dem Einlesen der eGK bei der Anmeldung. Danach kann bei einer vorliegenden Berechtigung nach Dokumenten und nach Medikationsdaten in der ePA gesucht werden, um die Informationslage in der Anamnese zu verbessern. Nach der Formulierung einer Therapieempfehlung und der Erstellung der lokalen Dokumentation können oder müssen Dokumente in die ePA gestellt, je nach Dokumentenart und -inhalt (siehe Abbildung 2). Ein Hochladen entfällt, wenn der Versicherte widersprochen hat.

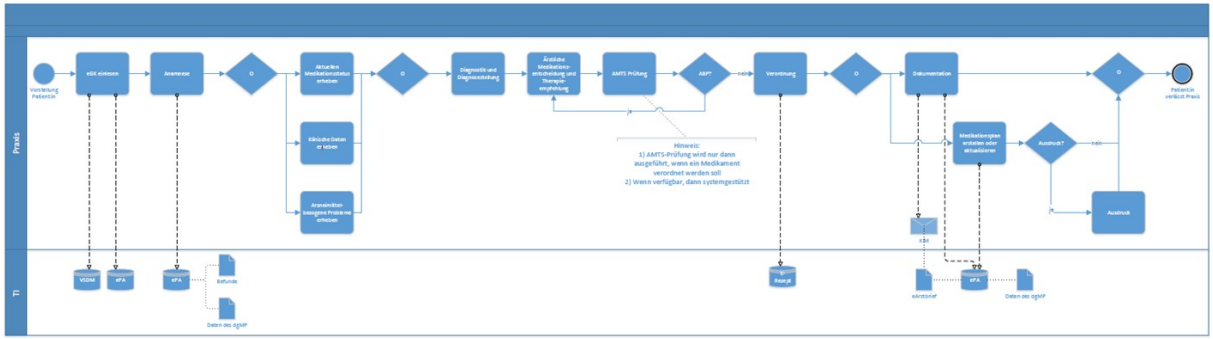

Abbildung 2: Schematisches Prozessmodell zur ePA für Arztpraxen, Zahnarztpraxen und psychotherapeutische Praxen

2.2.2.2 Anwendungsfälle

Für Leistungserbringer in Arztpraxen, Zahnarztpraxen und psychotherapeutische Praxen sowie im öffentlichen Gesundheitsdienst und der Arbeitsmedizin besteht die Möglichkeit Dokumente mit folgenden Inhalten zu lesen und zu schreiben:

- Diagnosen, Befunde, Therapiemaßnahmen
- Medikationsplan
- Notfalldaten
- eArztbrief
- Zahnbonusheft
- Kinderuntersuchungsheft
- Mutterpass
- Impfpass
- Pflegedokumentation
- elektronische Arbeitsunfähigkeitsbescheinigung
- Sonstige Daten, bspw. eDMP gemäß § 137 f SGB V
- Daten der Heilbehandlung und Rehabilitation

Darüber hinaus besteht die Möglichkeit Dokumente mit folgenden Inhalten zu lesen:

- Versichertendokumente
- Abrechnungsdaten
- DiGA-Daten

Eine detaillierte Auflistung der CRUD-Zugriffsrechte ist abrufbar unter https://github.com/gematik/ePA-Basic/blob/ePA-3.0.1/concept/chapters/legal_policy.adoc.

2.2.3 Apotheken

2.2.3.1 Prozesssicht

Für eine Apotheke wird der Zugriff auf die ePA durch das Einlesen der eGK eröffnet oder durch das Aufrufen von einem Stammkunden, der vorhergehend eine Berechtigung per ePA-App erteilt hat. Bei einer vorliegenden Berechtigung erhält die Apotheke mit ePA 3.0 einen Überblick über die Medikationsliste und damit einen einrichtungsübergreifenden Blick über verordnete und dispensierte Medikamente ebenso wie über weitere Dokumente, die sich in der ePA befinden (siehe Abbildung 3).

AVS-Herstellern wird empfohlen die Medikationsliste bereits mit ePA 3.0 nativ auf FHIR Daten umzusetzen, auch optional einen systemgestützten AMTS-Check anzubieten. Mit ePA 3.1 wird der elektronische Medikationsplan auf FHIR im ePA-Aktenkonto realisiert.

In eine Apotheke kann es darüber hinaus zur Abgabe eines OTC-Präparats kommen, ohne dass der Abverkauf eines apothekenpflichtigen Arzneimittels auf Grundlage eines Rezepts geschieht. Mit ePA 3.1 wird es den Apotheken möglich sein die dazugehörigen Dispensierinformationen direkt in die ePA zu schreiben.

Für Apotheken gibt es ebenso die Möglichkeit gemäß § 129 SGB V im Rahmen der assistierten Telemedizin den Versicherten bei der Einsichtnahme in die ePA zu unterstützen. Hierzu können die Dokumente der ePA angezeigt werden.

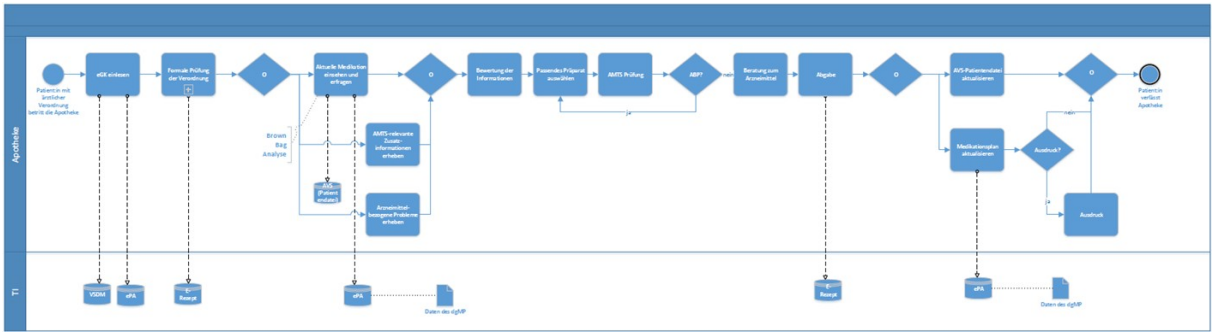

Abbildung 3: Schematisches Prozessmodell zur ePA für Apotheken

2.2.3.2 Anwendungsfälle

Für Leistungserbringer in Apotheken besteht die Möglichkeit Dokumente mit folgenden Inhalten zu lesen und zu schreiben:

- Medikationsplan
- Impfpass
- Verordnungs- und Dispensierdaten

Darüber hinaus besteht die Möglichkeit Dokumente mit folgenden Inhalten zu lesen:

- Diagnosen, Befunde, Therapiemaßnahmen
- Notfalldaten
- eArztbrief
- Kinderuntersuchungsheft
- Mutterpass
- Versichertendokumente
- Abrechnungsdaten
- DiGA-Daten
- Pflegedokumentation

Eine detaillierte Auflistung der CRUD-Zugriffsrechte ist abrufbar unter https://github.com/gematik/ePA-Basic/blob/ePA-3.0.1/concept/chapters/legal_policy.adoc.

2.2.4 Stationärer Sektor

2.2.4.1 Prozesssicht

Für die Versorgung innerhalb eines Krankenhauses gibt es in drei bestimmten Prozessen einen Bezug zur ePA. Zu diesen Prozessen gehören der Aufnahmeprozess (siehe Kapitel 2.2.4.2), der Versorgungsprozess (siehe Kapitel 2.2.4.3) und der Entlassprozess (siehe 2.2.4.4). Die hier aufgeführten fachlichen Beschreibungen der ePA kommen dementsprechend mitunter mehrfach vor. Die Vorgaben zur Benutzung der ePA sollte an die Gegebenheiten vor Ort angepasst sein.

Die Versorgung innerhalb eines Krankenhauses kann in verschiedenen Konstellationen erfolgen:

1. Für eine ambulante Versorgung, bspw. in einer Ambulanz bei einem für die ambulante Versorgung ermächtigten Arzt;
2. In einer zentralen Notaufnahme oder Rettungsstelle für eine Akutversorgung, bspw. durch Einlieferung per Rettungswagen oder Selbsteinweisung durch den Versicherten;
3. Für eine stationäre Versorgung für Elektivpatienten auf Grundlage eines Einweisungsscheins nach § 301 SGB V, bspw. für einen chirurgischen Eingriff oder eine wiederkehrende geriatrische Komplexbehandlung.

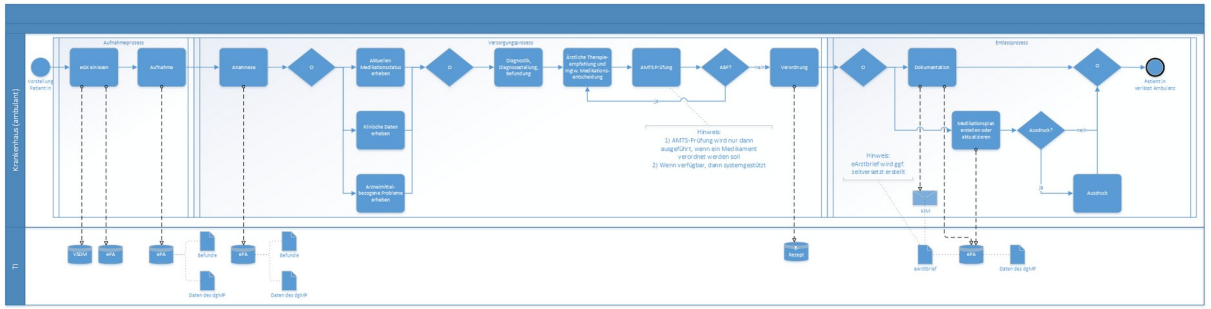

Abbildung 4: Schematisches Prozessmodell zur ePA für Krankenhäuser - ambulant

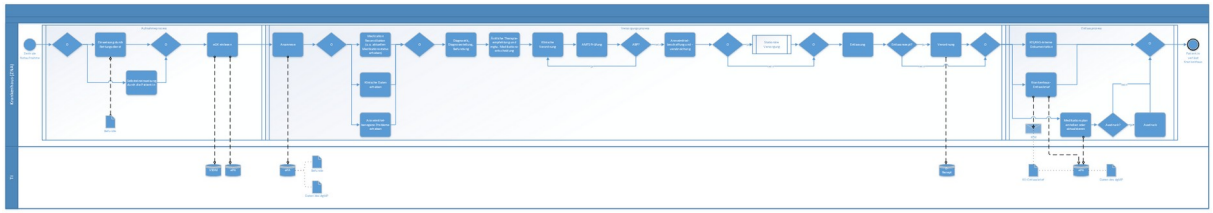

Abbildung 5: Schematisches Prozessmodell zur ePA für Krankenhäuser - zentrale Notaufnahme

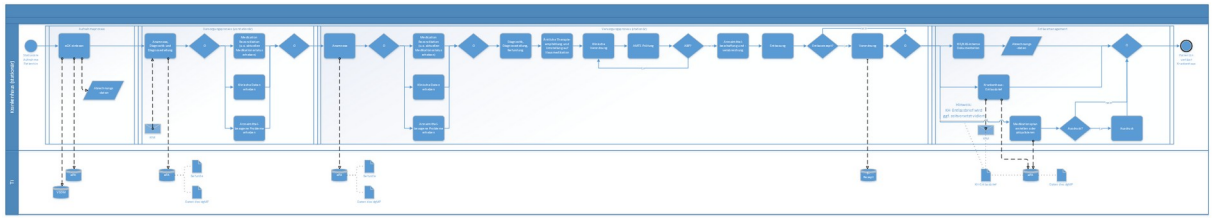

Abbildung 6: Schematisches Prozessmodell zur ePA für Krankenhäuser - stationär

In Krankenhäusern ist die Konstellation anzutreffen, dass es eine zentrale Aufnahme für mehrere Organisationseinheiten (OE) gibt oder dass ein Versicherter nach der Aufnahme in einer anderen Organisationseinheit weiterbehandelt wird. Dabei kann es dazu kommen, dass der aufnehmenden OE eine andere Telematik-ID zugewiesen ist als der weiterbehandelnden OE. Die Benutzung der ePA ist für alle Konstellation vorgesehen.

2.2.4.2 Aufnahmeprozess

Der administrative Aufnahmeprozess wird bereits heute und soll auch künftig in allen der drei o.g. Konstellationen durch VSDM unter Benutzung der eGK unterstützt werden. Die Anwendung VSDM wird genutzt, um die Stammdaten des Versicherten zu erfassen, die Gültigkeit des Versicherungsstatus zu prüfen sowie mithilfe des VSDM einen Nachweis über einen aktiven Behandlungskontext zu erzeugen und diesen im ePA-Aktenkonto als Zugriffsbefugnis zu hinterlegen. Zu diesem Zweck muss die ePA-Funktion „Erstellen einer Befugnis“ (siehe Kapitel 3.9) ebenfalls von dem System ausgeführt werden, welches das VSDM durchführt. Das hierfür genutzte System soll auch für ein nachträgliches ReadVSDM zur Befugniserstellung genutzt werden können, falls die eGK zum Zeitpunkt der Aufnahme nicht vorlag.

Der Behandlungskontext bezieht sich auf den Behandlungsfall. Im Sinne der Orientierungshilfe KIS (https://www.datenschutzkonferenz-online.de/media/oh/201403_oh_krankenhausinformationssysteme.pdf) umfasst ein Behandlungsfall eine medizinische Behandlung inklusive der Anamnese-, Diagnose-, Therapie- und Nachbehandlungsmaßnahmen zu derselben Krankheit, Verdachtsdiagnose oder Symptomatik. Die ePA-Zugriffsbefugnis gilt für eine Telematik-ID und nicht für ein bestimmtes technisches System. Zur Versorgung des Versicherten innerhalb des Behandlungsfalls kann die Zugriffsbefugnis auf das ePA-Aktenkonto von allen berechtigten Mitarbeiter:innen und den dort zum Einsatz kommenden Subsystemen nachgenutzt werden.

Damit ein Subsystem die erzeugte Zugriffsbefugnis nutzen kann, muss es diese nicht persistieren. Das Subsystem spricht das ePA-Aktenkonto des Versicherten direkt an und setzt die gewünschte Operation um, bspw. eine Suche für zur Dokumentenübersicht oder das Hochladen eines Dokuments in ein ePA-Aktenkonto. Das ePA-Aktenkonto prüft zum Zeitpunkt des Zugriffsversuchs, ob für die Telematik-ID, mit der eine Authentisierung vorgenommen wird, auch eine Zugriffsbefugnis vorliegt.

Die Eröffnung des Behandlungskontexts und die Erstellung einer Zugriffsbefugnis soll mit der administrativen Aufnahme umgesetzt werden, damit die Daten und Dokumente aus dem ePA-Aktenkonto zum Zwecke der (vorstationären) Anamnese heruntergeladen werden können. Zusätzlich können für die Anamnese auch im Kontext des Behandlungsfalls stehende und per KIM empfangene Informationen für die Anamnese genutzt werden. Falls der Versicherte ausgewählte Dokumente in seiner ePA verborgen hat, sind diese für das Krankenhaus nicht einsehbar. Wenn ein verborgenes Dokument vom Versicherten zu einem späteren Zeitpunkt sichtbar gemacht wird, wird das Krankenhaus vom ePA-Aktensystem nicht aktiv benachrichtigt und darüber informiert. Darauf sollte der Versicherte im Rahmen des Aufnahmeprozesses hingewiesen werden und sich das Krankenhaus absichern, da vom Krankenhaus nicht einsehbare Dokumente der ePA u.U. für die Behandlung relevante Informationen enthalten können.

Es gibt Fälle, in denen der Versicherte das Krankenhaus eigenständig durch die ePA-App aktiv befugen kann, bspw.

- vor dem Krankenhausaufenthalt, oder
- wenn eine administrative Aufnahme nicht in Präsenz durchgeführt wird, bspw. durch die Benutzung eines Patientenportals, oder

- der Versicherte zum Zeitpunkt der Aufnahme seine eGK nicht mit sich führt, oder
- der Versicherte PKV versichert ist, über keine eGK verfügt und ein ePA-Aktenkonto hat.

2.2.4.3 Versorgungsprozess

Aus Sicht des Klinikpersonals können das Krankenhausinformationssystem (KIS) oder auch ein Patientendatenmanagementsystem (PDMS) das führende System sein, in dem während eines stationären Aufenthalts dokumentiert wird. Bei der Benutzung der ePA am Klinischen Arbeitsplatzsystem (KAS) kann mithilfe einer Dokumentensuche im verwendeten System kenntlich gemacht werden, wenn neue Dokumente in der ePA seit dem letzten Zugriff hinzugekommen sind.

So lange eine Zugriffsbefugnis vorliegt, kann auf die ePA während des Krankenhausaufenthalts durchgehend zugegriffen werden, insbesondere bei der klinischen Aufnahme während der ärztlichen oder psychotherapeutischen Anamnese. In Anlehnung an die OH KIS sollten die Dokumente aus der ePA heruntergeladen werden, die auch einen inhaltlichen Fallbezug zum Krankenhausaufenthalt haben. Der gleichzeitige Download mehrerer Dokumente in das KIS innerhalb eines Arbeitsschritts soll eine effiziente Bedienung ermöglichen. Das KIS sollte eine Dokumentenvorschau umsetzen, damit Nutzer die Dokumente bewerten und bewusst in das KIS herunterladen oder nicht herunterladen.

Ein Zugriff auf die ePA kann zu Behandlungszwecken durch Ärzte und durch den pflegerischen Stationsdienst der berechtigten Telematik-ID erfolgen. Gemäß OH KIS erfolgt die Erweiterung des Kreises der Zugriffsberechtigten innerhalb des KIS auf der Grundlage einer fachlichen Entscheidung eines bereits berechtigten Arztes (z.B. Zuweisung zu einer weiteren OE). Bei einer internen Verlegung erhalten die neuen Behandler dadurch Zugriff auf die Daten, die bis dahin im KIS übernommen wurden. Ebenso kann auf die ePA zugegriffen und nach Dokumenten gesucht werden, die seit dem Datum des letzten Zugriffs aus der Klinik auf die ePA neu hinzugekommen sind. Diese Dokumente können dann einem Befundkorb hinzugefügt, bewusst bewertet und bei Bedarf in das KIS heruntergeladen werden.

Eine Zugriffsbefugnis kann nicht an Dritte weitergegeben oder für sie im ePA-Aktenkonto hinterlegt werden, bspw. wenn eine Verlegung zwischen Kliniken stattfindet (bspw. Anschlussbehandlung in einer Reha-Einrichtung oder Weiterbehandlung bei einem Maximalversorger) oder im Falle eines Konsils mit einer externen Leistungserbringersinstitution (bspw. einer Tele-Stroke-Unit oder einer Partnereinrichtung für Telekonsile oder Telemonitoring). Um diesen Einrichtungen den direkten Zugriff auf das ePA-Aktenkonto zu ermöglichen, ist es erforderlich, dass diese die eGK einlesen oder sie vom Versicherten bzw. einem Vertreter über die ePA-App berechtigt werden.

Die weiteren Festlegungen und Anforderungen an Rollen- und Berechtigungskonzepte innerhalb der OH KIS bleiben hiervon unberührt.

2.2.4.4 Entlassprozess

Die Zugriffsbefugnis für ein ePA-Aktenkonto ist standardmäßig auf 90 Tage festgelegt und berechtigt zum Zugriff auf in der ePA sichtbare Dokumente, für die auch ein gesetzlich legitimierter Zugriff vorgesehen ist. Die Verlängerung einer Zugriffsbefugnis ist möglich, indem die eGK erneut gesteckt wird; eine eigenständige Verlängerung der Zugriffsbefugnis über die Nutzung einer Verlängerungs- und Kostenübernahmeanfrage im Rahmen des elektronischen Datenaustauschs nach § 301 SGB V ist nicht möglich. Die Zugriffsbefugnis kann vom Versicherten vorzeitig über seine ePA-App beendet werden. Vor dem Beenden einer Berechtigung soll der Versicherte einen Warnhinweis in seiner ePA-App erhalten bezüglich der Konsequenzen für die Patientensicherheit aufgrund einer

möglicherweise lückenhaften Dokumentation. Eine Zugriffsbefugnis wird auch benötigt, um ein Dokument in die ePA hochzuladen zu können.

Im Zuge der Entlassung ist das Krankenhaus verpflichtet einen Krankenhaus-Entlassbrief in das ePA-Aktenkonto einzustellen. Das fachliche Ziel ist, dass diese Informationen für weiterbehandelnde Institutionen im ambulanten Sektor oder in der Pflege einseh- und nutzbar sind. Aus Sicht des Versicherten ist die Bereitstellung einer patientenverständlichen Version eines Entlassbriefs wünschenswert [siehe https://innovationsfonds.g-ba.de/downloads/beschluss-dokumente/130/2022-01-21_PASTA.pdf]. Mit KIM und dem TI-Messenger stehen zusätzlich gerichtete Kommunikationskanäle bereit, die einen direkten Austausch von Informationen zwischen Leistungserbringerinstitutionen ermöglichen.

Im ePA-Aktensystem ist eine Unterscheidung zum Status des Dokuments mit dem EventCode auf Metadatenebene erkennbar. Eine Unterscheidung muss auch menschenlesbar im Dokument erkenntlich sein, ob es sich um einen vorläufigen oder finalen Krankenhaus-Entlassbrief handelt. Der vorläufige und der finale Krankenhaus-Entlassbrief sollten als separate Dokumente in die ePA hochgeladen werden.

Der Nutzer eines Primärsystems erhält eine sprechende Fehlermeldung, wenn eine Zugriffsbefugnis nicht (mehr) vorliegt und das Hochladen eines Dokuments in dem Moment des Zugriffs nicht möglich (siehe Kapitel 3.9), bspw.:

- „Es ist in einer bestehenden User Session kein Zugriff auf ein ePA-Aktenkonto möglich, weil kein ePA-Aktenkonto (mehr) existiert (der Versicherte hat der ePA widersprochen).“
- „Es ist in einer bestehenden User Session kein Zugriff auf ein ePA-Aktenkonto möglich, weil keine Berechtigung vorliegt (noch nicht oder auch nicht mehr). Bitte lesen Sie die eGK ein.“
- „Es ist in einer bestehenden User Session kein Zugriff auf ein ePA-Aktenkonto möglich, weil der Versicherte diese Leistungserbringerinstitution von der Benutzung der ePA ausgeschlossen hat.“

Vor dem Hintergrund, des zeitlichen Versatzes zwischen der Entlassung des Versicherten und der Finalisierung der Dokumentation soll der Versicherte im Entlassprozess darauf hingewiesen werden, dass eine Zugriffsbefugnis über die Entlassung hinaus erforderlich ist. Wenn das Datum der Aufnahme eine bestimmte Zeit zurückliegt, kann es empfehlenswert sein, dass die eGK erneut eingelesen wird, um die Zugriffsbefugnis im ePA-Aktenkonto zu erneuern. Für die Nutzer des Primärsystems können dabei verschiedene Wege genutzt werden, um auf die Notwendigkeit des erneuten eGK Einlesen hinzuweisen, bspw. über ein Ampelsystem oder eine Erinnerung anhand von Tagesgrenzen. Die Leistungserbringerinstitution soll im Primärsystem für sich konfigurieren können, welche Schwellenwerte hier zum Einsatz kommen sollen. Die eGK sollte ebenfalls bei Versicherten erneut eingelesen werden, deren stationärer Aufenthalt über 90 Tage nach Aufnahme hinausgeht.

Im Rahmen des Aufnahmeprozesses kann bereits die Einwilligung bzw. der Widerspruch zum Hochladen des Krankenhaus-Entlassbriefs am Ende des stationären Aufenthalts eingeholt werden. Dies ermöglicht eine automatisierte Datenverarbeitung im Entlassprozess. Das Hochladen von Dokumenten in die ePA kann aus einem beliebigen (Sub-)System ausgeführt werden. Der gesetzte Wert zum automatisierten Hochladen muss überschrieben und dadurch bspw. ein Hochladen unterbunden werden können. Im Entlassprozess muss der Versicherte nach wie vor die Möglichkeit haben, dem Hochladen eines Dokuments widersprechen zu können. Ebenso muss das einstellende (Sub-)System die Funktion anbieten, dass ein Dokument verborgen in das ePA-Aktenkonto hochgeladen werden kann. Das Nähere legt das Krankenhaus per Richtlinie fest.

Über den E-Rezept-Fachdienst ausgestellte Entlassrezepte werden automatisch über den E-Rezept-Fachdienst in die Medikationsliste der ePA übertragen. Die Erstellung oder eine Aktualisierung des Medikationsplans in der ePA ist in einer Ausbaustufe mit dem ePA-Release 3.1 möglich.

Die gesetzliche Grundlage dafür finden sich insbesondere in § 339, 342 und 348 SGB V.

2.2.4.5 Anwendungsfälle

Für Leistungserbringer in Krankenhäusern – Ärzte, Zahnärzte und Psychotherapeuten sowie Apotheker, Hebammen, Gesundheits-, Kranken- und Altenpfleger – besteht je nach Berufsgruppenzugehörigkeit die Möglichkeit Dokumente in die ePA zu lesen und zu schreiben:

- Diagnosen, Befunde, Therapiemaßnahmen
- Medikationsplan
- Notfalldaten
- eArztbrief
- Zahnbonusheft
- Kinderuntersuchungsheft
- Mutterpass
- Impfpass
- Pflegedokumentation
- elektronische Arbeitsunfähigkeitsbescheinigung
- Sonstige Daten, bspw. eDMP gemäß § 137 f SGB V
- Daten der Heilbehandlung und Rehabilitation

Darüber hinaus besteht je nach Berufsgruppenzugehörigkeit die Möglichkeit Dokumente anderer Inhalte zu lesen:

- Versichertendokumente
- Abrechnungsdaten
- DiGA-Daten

Eine detaillierte Auflistung der CRUD-Zugriffsrechte ist abrufbar unter https://github.com/gematik/ePA-Basic/blob/ePA-3.0.1/concept/chapters/legal_policy.adoc.

2.2.5 Pflege

2.2.5.1 Prozessmodell

In der ePA erfasste Behandlungsinformationen sollten gesichtet und auf Relevanz geprüft werden (siehe Abbildung 4). Aus Sicht der Pflege ist es wichtig, dass sie Kenntnis über den aktuellen Zustand zur Aufnahme der Patient:in und zur Versorgung erlangen kann. Insbesondere den Informationen zur aktuellen Medikation kommt eine hohe Relevanz zu. Der Medikationsplan spielt bei Aufnahme der Patient:in in der Pflegeeinrichtung eine zentrale Rolle. Er ist eine aktuelle Zusammenstellung der Medikation, die eine Patient:in über einen bestimmten Zeitraum einnehmen soll, umfasst Einnahmehinweise zum Medikament sowie Dispensierangaben der Apotheke. In der ePA ist darüber hinaus eine Medikationsliste vorhanden, die Aufschluss darüber geben kann, ob in der Vergangenheit weitere Medikamente verordnet wurden, die bspw. aufgrund von Unverträglichkeiten

mittlerweile abgesetzt worden sind. Die Abbildung eines Insulinplans ist bislang nicht Gegenstand des digital gestützten Medikationsprozesses.

Die ePA kann darüber hinaus für ausgewählte Dokumente der Pflegedokumentation genutzt werden und damit bspw. einen einrichtungsübergreifenden Informationsaustausch zwischen ambulanter Pflege und Palliativversorgung oder zwischen Pflegeinrichtung und betreuendem Hausarzt unterstützen. Vitaldaten, die vom Leistungserbringer erfasst werden, können in einem Dokument abgebildet werden. In der ePA kann im Datensatz Persönlicher Erklärung die Angabe hinterlegt werden, ob eine Patientenverfügung vorhanden ist. Die Angabe des Datums kann vom Versicherten selber oder einem Vertreter hinterlegt werden.

Das Pflegepersonal kann grundsätzlich auch auf Dokumente in der ePA zugreifen, die von anderen Leistungserbringern eingestellt worden sind und diese im Rahmen der Erbringung der Pflegeleistung berücksichtigen. Hierunter fallen bspw. Entlass- und Arztbriefe oder auch Therapiedokumentationen der Physio-, Logo- und Ergotherapie. Je nachdem, ob Daten in strukturierter Form vorliegen, können diese auch in die Primärdokumentation übernommen werden, bspw. künftig für Diagnosen.

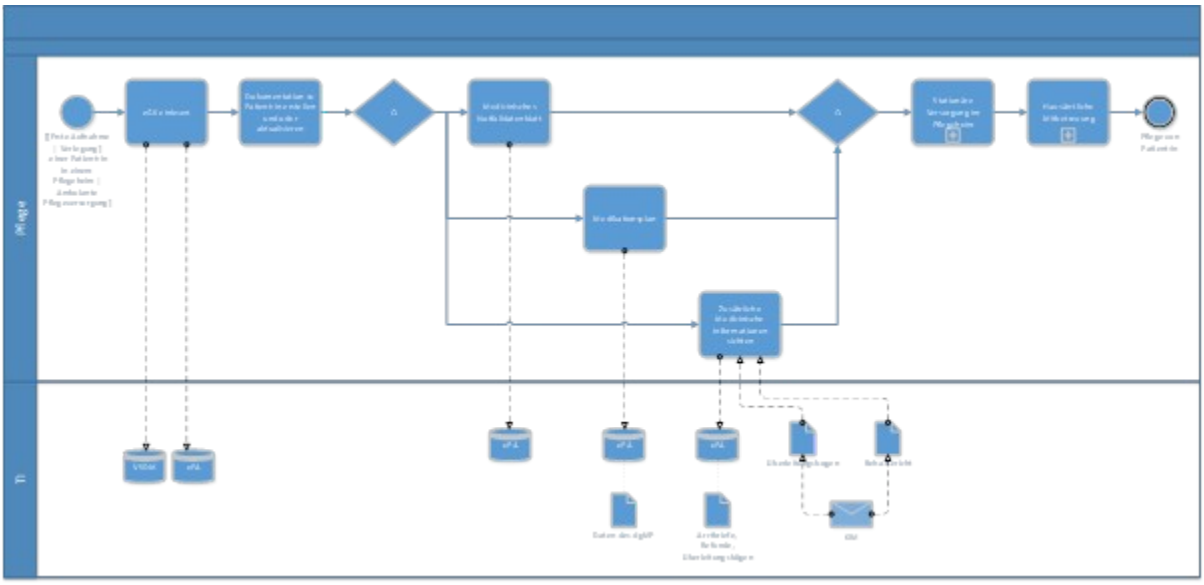

Abbildung 7: Schematisches Prozessmodell zur ePA für die Pflege

2.2.5.2 Anwendungsfälle

Für Leistungserbringer in der Pflegeversorgung besteht die Möglichkeit Dokumente mit folgenden Inhalten zu lesen und zu schreiben:

- Impfpass
- Pflegedokumentation

Darüber hinaus besteht die Möglichkeit Dokumente mit folgenden Inhalten zu lesen:

- Diagnosen, Befunde, Therapiemaßnahmen
- Medikationsplan
- Notfalldaten
- eArztbrief

- Kinderuntersuchungsheft
- Mutterpass
- Versichertendokumente
- DiGA-Daten

Eine detaillierte Auflistung der CRUD-Zugriffsrechte ist abrufbar unter https://github.com/gematik/ePA-Basic/blob/ePA-3.0.1/concept/chapters/legal_policy.adoc.

2.2.6 Heilmittelerbringer

2.2.6.1 Prozessmodell

Die ePA kann auch in der Versorgung von Heilmittelerbringern genutzt werden. Ausgewählte Daten und Dokumente der ePA dürfen von Heilmittelerbringern gelesen und genutzt werden, wenn die eGK eingelesen wird und eine Zugriffsbefugnis erzeugt wird. Zu den Heilmittelerbringern zählen Physiotherapeuten, Ergotherapeuten, Logopäden, Podologen und Ernährungstherapeuten, die sich nach heutigem Stand an die TI anbinden können.

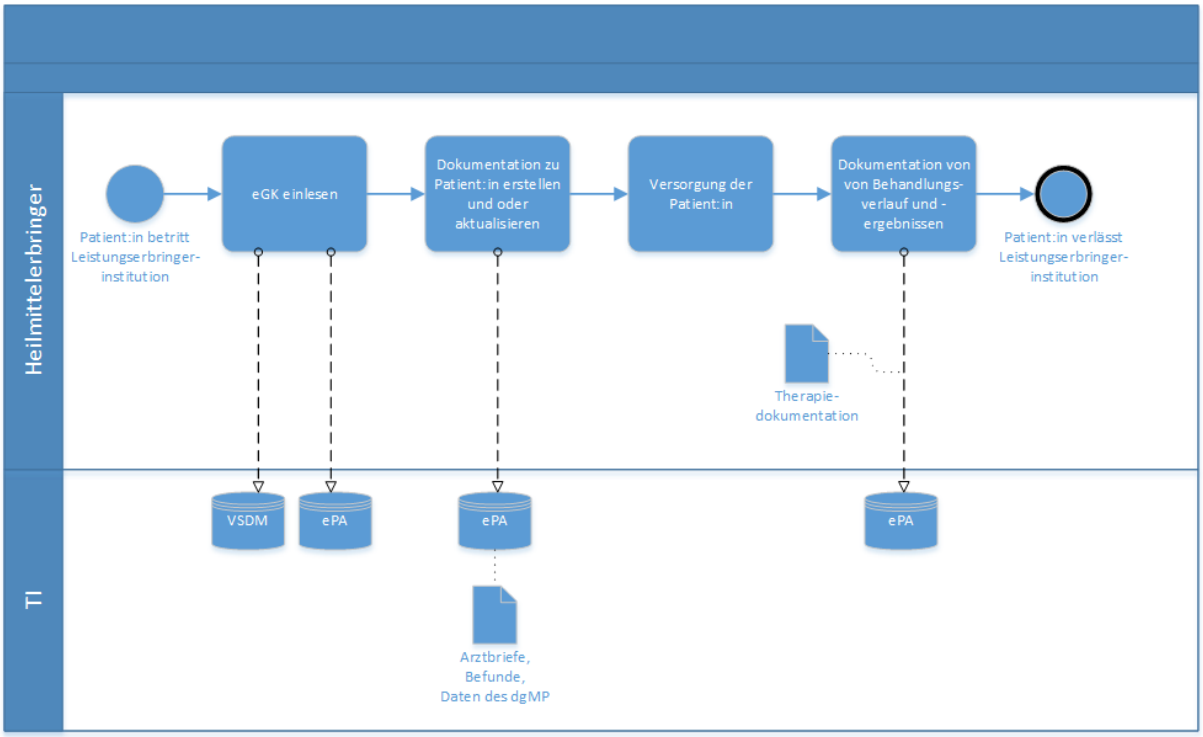

Abbildung 8 : Schematisches Prozessmodell zur ePA bei Heilmittelerbringern

2.2.6.2 Anwendungsfälle

Für Heilmittelerbringer besteht die Möglichkeit Dokumente mit folgenden Inhalten zu lesen und zu schreiben:

- Diagnosen, Befunde, Therapiemaßnahmen

Darüber hinaus besteht die Möglichkeit Dokumente mit folgenden Inhalten zu lesen:

- Medikationsplan
- Notfalldaten
- eArztbrief
- Kinderuntersuchungsheft
- Mutterpass
- Versichertendokumente
- Abrechnungsdaten
- DiGA-Daten
- Pflegedokumentation

Eine detaillierte Auflistung der CRUD-Zugriffsrechte ist abrufbar unter https://github.com/gematik/ePA-Basic/blob/ePA-3.0.1/concept/chapters/legal_policy.adoc.

2.3 Akteure und Rollen

Das vorliegende Dokument richtet sich vorrangig an Hersteller von Systemen, die von Leistungserbringern genutzt werden und formuliert Anforderung, die für die Nutzung der ePA implementiert werden müssen. Darüber hinaus werden in Kapitel 4 weitere Arten ePA-nutzender Systeme aufgeführt, deren Nutzer keine Leistungserbringer sind. Die großen Überschneidungen in den Anforderungshaushalten dieser Systeme mit den Systemen der Leistungserbringer sind in den AFO-Steckbriefen dieser Nutzer abgebildet, s. TabILF_Kurzübersicht_PS-CS-Typen.

Leistungserbringer agieren in zwei ePA-Szenarien:

- als Einsteller und Konsument im bilateralen Dokumentenaustausch zwischen LE und Versichertem
- als Einsteller und Konsument in der Interaktion zwischen Leistungserbringern über die ePA

Das PS tritt somit in der Consumer Zone der TI sowohl als Document Consumer als auch als Document Source auf, beim Löschen auch als Document Administrator.

Gemäß [gemILF_PS#3.1.3] können Heilberufler ihren SM-B selbst nutzen oder ihre Gehilfen im Allgemeinen dafür autorisieren, auf die Anwendungen der eGK mit ebendiesen Rechten zuzugreifen. Dies gilt für das SM-B der TI-Rollenprofile 2, 3, 4 (SM-B Leistungserbringer). Eine Ausnahme hierzu bilden ausschließlich die Gehilfen der nichtärztlichen Psychotherapeuten. Das PS darf die berufsmäßigen Gehilfen der nichtärztlichen Psychotherapeuten nicht mit denjenigen Zugriffsberechtigungen auf die ePA ausstatten, über die der nichtärztliche Psychotherapeut verfügt.

Die Versicherten agieren in der Rolle des Akteninhabers und in der Rolle des Vertreters des Akteninhabers.

Auch innerhalb größerer Leistungserbringer-Institutionen ist ein Akteur gegenüber der ePA mittels seiner Telematik-ID als eigenständiger Nutzer identifiziert, nicht als Mandant einer übergreifenden Institution. Die Mandantenverwaltung innerhalb einer größeren Institution, etwa einem Krankenhaus, muss ggf. dafür genutzt werden, um den Prüfungsnachweis des Mandanten nutzen zu können, der aktuell in der ePA aktiv ist.

Unterschiedliche Arten von Primärsystemen (PS) und Clientsystemen (CS) haben je nach ihren fachlichen Nutzungsprofilen unterschiedliche Anforderungshaushalte.

- PS = Client gegenüber dem Aktensystem mit Userinteraktion

- CS = Client gegenüber dem Aktensystem potentiell ohne Userinteraktion

Normative Anforderungshaushalte unterschiedlicher Systeme sind jeweils in speziellen AFO-Steckbriefen aufgeführt. Der AFO-Steckbrief hat im Zweifelsfall Priorität gegenüber der Unterscheidung zwischen Primärsystem und Clientsystem im Fließ- und Anforderungstext.

Tabelle 1: TabILF_Kurzübersicht_PS-CS-Typen

Nutzer	Kurzbeschreibung der Nutzungsszenarien	Typ	AFO-Steckbrief
Leistungs-erbringer	Leistungserbringer benutzen das Aktensystem, um Daten für Behandlungsprozesse bereitzustellen und zu nutzen.	**PS** (alle PS-AFOs, keine CS-AFOs)	gemSST_PS_ePA
Kostenträger	Einstellen von Abrechnungsdaten, eAUs und eingescannten Papierdokumenten. Im Rahmen eines betreiberübergreifenden Aktenumzugs: • Herstellung des Exportpakets • Import des Exportpakets	**CS** (Untermenge PS-AFOs, Untermenge CS-AFOs)	gemSST_CS_ePA_KTR
Ombudstelle	Auf Wunsch eines Versicherten für sein Aktenkonto: • Sperren und Entsperren von spezifischen LEI für die Nutzung eines Aktenkontos • Widerspruch gegen den Medikationsprozess aussprechen und diesen zu widerrufen • Protokolldaten aus dem Aktenkonto herunterladen.	**CS** (Untermenge PS-AFOs, Untermenge CS-AFOs)	gemSST_CS_ePA_Ombudstelle
DiGA	Einstellen von DiGA-Daten	**CS** (Untermenge PS-AFOs, Untermenge CS-	gemSST_CS_ePA_DiGA

		AFOs)	

2.4 IT-Sicherheit in den Systemen der Leistungserbringerinstitution

Zum Schutz der Daten der Patienten in den Systemen der Leistungserbringerinstitution sind die Sicherheitsziele der Vertraulichkeit, Integrität und Verfügbarkeit zu gewährleisten. Die Verantwortlichkeit zur Sicherstellung der IT-Sicherheit der Systeme der Leistungserbringerinstitution liegt in der Leistungserbringerinstitution. Hersteller von Primärsystemen können sicherheitstechnische Vorkehrungen in ihre Produkte integrieren, um die Sicherheitsziele zu unterstützen wie bspw. die Implementierung einer ICAP-Schnittstelle.

Insbesondere einschlägige Vorgaben sollten für die IT-Sicherheit von der Leistungserbringerinstitution berücksichtigt werden, bspw.:

- Leitfaden zur Basis-Absicherung nach IT-Grundschutz des BSI (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Leitfaden_zur_Basis-Absicherung.html?nn=128634)
- Abschlussbericht Projekt CyberPraxMed – Sicherheit in Arztpraxen des BSI (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/DigitaleGesellschaft/CyberPraxMed_Abschlussbericht.html)
- IT-Sicherheitsrichtlinie der KBV (https://www.kbv.de/media/sp/RiLi___75b_SGB_V_Anforderungen_Gewaehrleistung_IT-Sicherheit.pdf)

Insbesondere sollte eine verwaltete Virenschutzlösung implementiert werden, die vor ggf. in Daten bzw. Dokumenten der ePA enthaltenen Schadcode schützt. Die gematik mitigiert das Risiko von Schadcode in ePA-Daten bzw. Dokumenten durch die Einschränkung der zulässigen Datenformate, bei denen das Risiko von enthaltenem Schadcode stark reduziert ist (z.B. keine Office-Dokumente). Beim Einstellen in die ePA werden die Daten bzw. Dokumente auf die zulässigen Formate geprüft und unzulässige Formate abgelehnt.

Es gibt keinen zentralen Virenscanner in der ePA oder in der TI.

3 Übergreifende Festlegungen

In diesem Kapitel werden die übergreifenden Festlegungen zum erfolgreichen Kommunikationsaufbau zwischen Primärsystem und einem Aktenkonto beschrieben.

A_24680 - User Agent im Nachrichtenheader
Das PS MUSS die HTTP Header Elemente "ClientID" und "Versionsnummer" bei jedem Request sowohl im HTTP-Header der VAU-Nachricht, als auch im HTTP-Header der Nachricht an den Service einfügen gemäß [gemSpec_Aktensystem_ePAfuerAlle#2].**[<=]**

Hinweis zum Erhalt der ClientID: die ClientID wird durch die gematik vergeben und übermittelt, sobald sich ein (Client-)Produkthersteller unter idp-registrierung@gematik.de registriert hat. Dazu ist im Rahmen dieser Registrierung der Name des Herstellers und der Name des zu registrierenden Produktes zu übermitteln. Sollte im Rahmen einer anderen TI-Anwendung bereits eine Registrierung vorgenommen worden sein, kann die ClientID auch im ePA-Kontext genutzt werden (sofern es sich um das gleiche Softwareprodukt handelt).

3.1 TLS

Das Primärsystem benutzt für die Kommunikation im Rahmen der Anwendungsfälle der ePA für alle ausschließlich TLS.

Es gelten die Vorgaben aus [gemSpec_Krypt] für TLS.

A_24500 - Kommunikation über TLS-Verbindung
Das PS MUSS für die Anwendungsfälle der ePA für alle mit den Diensten der TI ausschließlich über TLS mit serverseitiger Authentisierung kommunizieren.**[<=]**

A_24502 - Vorgaben für TLS-Verbindungen
Das PS MUSS als ePA-Client für die TLS-Kommunikation die Vorgaben aus [gemSpec_Krypt#3.15.3] umsetzen.**[<=]**

3.2 Aktensystem- und Service-Lokalisierung

Die Lokalisierung der Services der ePA für das Primärsystem erfolgt über die übergreifenden Domäne epa4all.de. Diese Domäne kann sowohl im Internet als auch im DNS der TI aufgelöst werden und verweist immer auf IP-Adressen der TI. Für die verschiedenen Umgebungen der TI werden third-level Domänen eingerichtet: .ref (RU1), .dev (RU2), .test (TU) und .prod (PU).

Das Primärsystem muss die FQDNs der ePA-Aktensysteme wissen (diese werden fest definiert, vgl. A_24592-*).

Diese sind Host und IP-Adressen für den Endpunkt I_Information_Service und der Services in der VAU:
epa-as-<ePA-Anbieter-Zahl>.<Umgebung>.epa4all.de.

Das Vorgehen der festvorgegebenen FQDNs ist analog zum E-Rezept-Vorgehen.

A_24447 - FQDN der Aktensysteme als konfigurierbarer Wert

Das PS MUSS die FQDN der Aktensysteme als einen konfigurierbaren Wert umsetzen, damit ein Wechsel der Umgebungen und ein Hinzufügen weiterer Aktensysteme administrativ möglich ist.**[<=]**

A_24380 - Endpunkt Schnittstelle ePA-Aktensysteme
Das Primärsystem MUSS die URL für die Kommunikation mit den ePA-Aktensystemen gemäß `https://<FQDN aus DNS Lookup>:443/` bilden.**[<=]**

Falls die Services innerhalb einer ePA-VAU liegen, werden die Dienste an den HTTPS-Schnittstellen unter den in den OpenAPI-Spezifikationen aufgeführten Pfadnamen erreicht. Der Pfad wird im inneren HTTP-Request genutzt (innerhalb des Vau-Kanals). Das Primärsystem benutzt den Pfadnamen /VAU für die Intiierung des VAU-Kanals.

Für Schnittstellen, die außerhalb einer VAU liegen, gelten ebenfalls die jeweilige ePA-OpenAPI-Spezifikation mit den dort aufgeführten Pfadnamen.

Pfadbeispiele:

Abfrage eines Kontostatus beim Information-Service (außerhalb der VAU):

https://epa-as-<ePA-Anbieter-Zahl>.<Umgebung>.epa4all.de:443/information/api/v1/ehr

Aufbau der VAU, z.B.: getriggert durch GetNonce:

https://epa-as-<ePA-Anbieter-Zahl>.<Umgebung>.epa4all.de:443/VAU

Einstellen eines Entitlements innerhalb der VAU:

URL, die der Client aufruft für die Übermittlung des äußeren HTTP-Request:

https://epa-as-<ePA-Anbieter-Zahl>.<Umgebung>.epa4all.de:443 /<VAU-CID>

Pfad des inneren HTTP-Request:

/epa/basic/api/v1/ps/entitlements

Die Informationen zu den Endpunkten des Identity Providers ermittelt das Primärsystem aus dem Discovery Document, siehe auch [gemSpec_IDP_Dienst#Registrierung von Endgerät und Anwendungsfrontend]. Das Discovery Document ist vom IDP-Dienst unter der URL /.well-known/openid-configuration abrufbar.

Das Primärsystem erreicht die ePA-Aktensysteme und den IDP über den Konnektor geroutet. Es ist sinnvoll den Konnektor als Default-Gateway zu nutzen.

3.3 Aufbau der User Session zum Aktensystem

Das Primärsystem kommuniziert als ePA-Client mit dem ePA-Aktensystem in einer Vertrauenswürdige Ausführungsumgebung (VAU). Diese stellt sicher, dass sensible Klartext-Daten wie z. B. die medizinischen Daten des Versicherten sicher vor Angriffen verarbeitet werden können. Die Daten werden ausschließlich über sichere VAU-Kanäle vom PS in die VAU transportiert bzw. aus der VAU abgerufen.

Das Primärsystem initiiert den Aufbau eines VAU-Kanals in die VAU des Aktensystems. Dabei authentisiert sich die VAU mit ihrem Zertifikat als authentische VAU des Aktensystems. Anschließend wird für den Nutzer, repräsentiert durch die SMC-B, mit Hilfe des IDP-Dienstes eine User Session angelegt. Diese User Session ermöglicht den Zugriff auf alle Aktenkonten des Aktensystems, in denen eine Befugnis für die LEI hinterlegt ist.

Die User Session zu den Aktensystemen kann aufgebaut werden ohne den direkten Zugriff auf eine Akte z.B. beim morgendlichen Start des PS.

Durch eine Anfrage an eine bestimmte Akte wird diese Akte in der User Session als Health Record Context geladen und man kann darauf arbeiten.

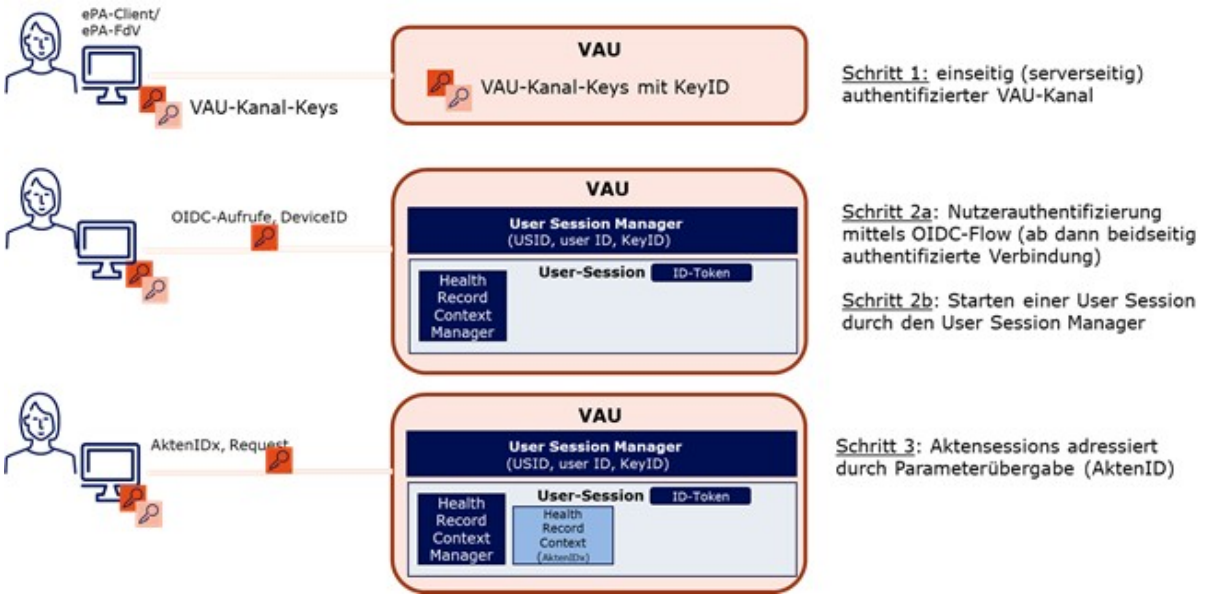

Abbildung 9: Überblick über Aufbau VAU, User Session und Aktensession

3.3.1 VAU

Für Informationen zum Kommunikationsprotokoll zwischen dem Primärsystem und einer VAU siehe [gemSpec_Krypt#3.15 ePA-spezifische Vorgaben] und [gemSpec_Krypt#7].

A_24494 - Kommunikation mit der Vertrauenswürdigen Ausführungsumgebung (VAU)
Das PS MUSS als ePA-Client für die Kommunikation mit der Vertrauenswürdigen Ausführungsumgebung (VAU) die Vorgaben aus [gemSpec_Krypt#7,3.15] umsetzen.**[<=]**

A_24926 - Umsetzung sicherer Kanal zur Aktenkontoverwaltung
Das PS MUSS die im Rahmen des sicheren Verbindungsaufbaus zur Aktenkontoverwaltung ausgehandelten Sitzungsschlüssel verwenden, um den HTTP Body aller über den sicheren Kanal zu sendenden Requests an die Aktenkontoverwaltung zu verschlüsseln und alle über den sicheren Kanal gesendeten Responses von der Aktenkontoverwaltung zu entschlüsseln.**[<=]**

Die gematik wird Beispielimplementierungen des VAU-Protokolls der ePA für alle auf GitHub veröffentlichen.

3.3.2 Nutzerauthentifizierung per IDP-Dienst mittels OIDC-Flow

Die Authentifizierung der LEI erfolgt mittels zentralem IDP-Dienst. Dieser steht bereits u.a. für das e-Rezept zur Verfügung:

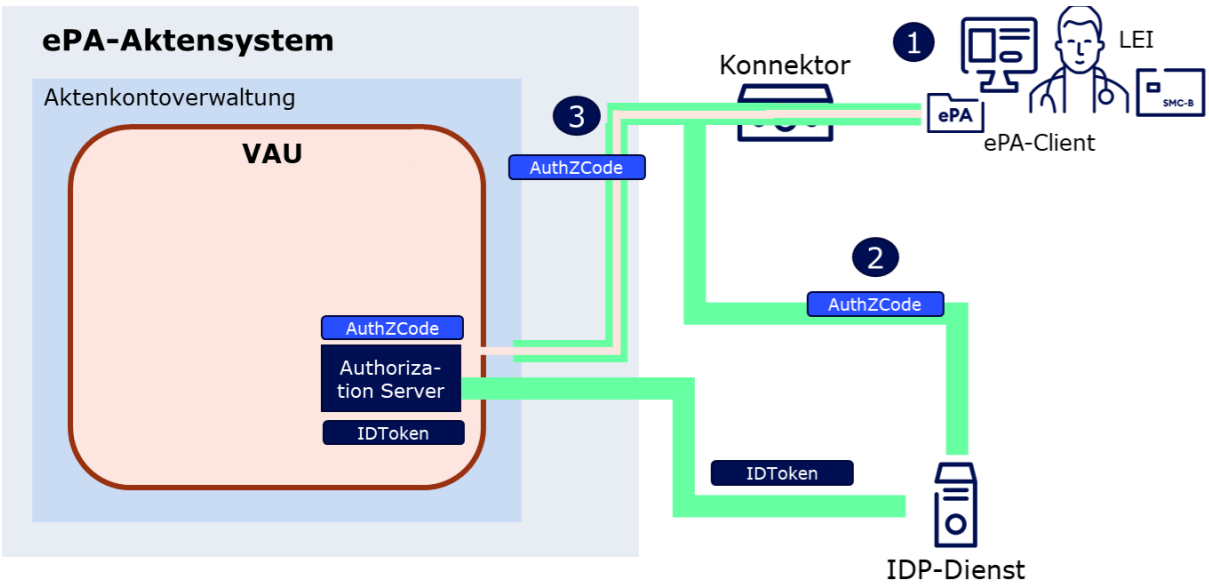

Abbildung 10: Überblick über Nutzerauthentifizierung

1. Die Nutzerauthentifizierung wird durch einen Zugriff des Primärsystems auf das ePA-Aktensystem getriggert.

2. Da der Nutzer noch nicht angemeldet ist, leitet der Authorization Server des ePA-Aktensystem an den IDP-Dienst weiter. Am IDP-Dienst authentisiert sich der Nutzer mittels SMC-B und PIN. Bei erfolgreicher Authentisierung erhält das Primärsystem einen Authorization Code.

3. Das Primärsystem übermittelt den Authorization Code an das ePA-Aktensystem.

Der Authorization Server im ePA-Aktensystem ruft mittels des Authorization Codes das ID-Token für den Nutzer vom IDP-Dienst ab. Das ID-Token ist vom IDP-Dienst signiert. Als Ergebnis ist ein ID-Token des Nutzers in der VAU vorhanden. Liegt ein ID-Token des Nutzers in der VAU vor, wird durch den User Session Manager eine User Session für den Nutzer gestartet und die LEI kann auf die Aktenkonten (sofern eine Befugnis vorhanden ist) zugreifen.

Die folgende Abbildung zeigt den Nachrichten-Flow im Detail:

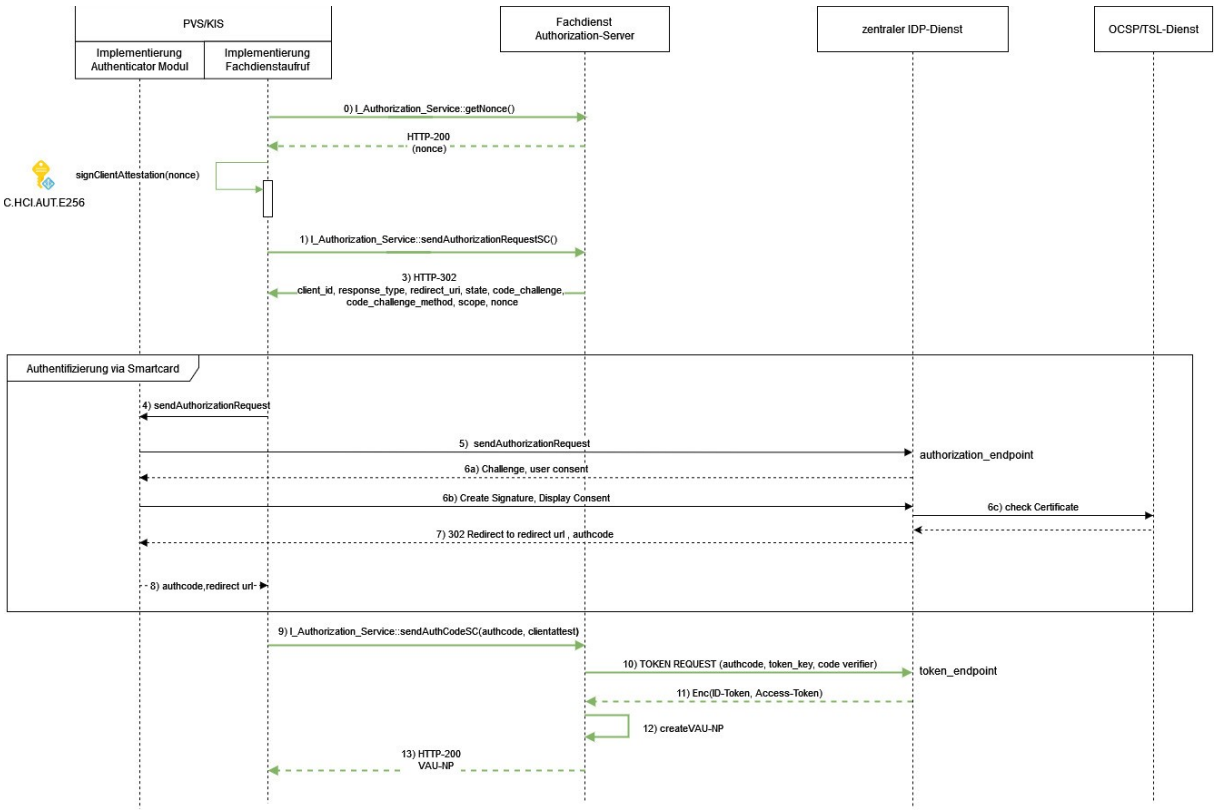

Abbildung 11: Detaillierter Nachrichten-Flow für die Nutzerauthentifizierung mit dem IDP-Dienst

Vorbereitend zum OIDC-Flow fragt das PS eine Nonce ab (0), die es mit der SMC-B signiert als "Attestation der Umgebung".

Dazu nutzt es folgende Operation:

Tabelle 2: I_Authorization_Service::getNonce

REST-Schnittstelle des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)	
I_Authorization_Service	
getNonce	Diese Operation liefert eine Nonce für die Erstellung der Attestation (clientAttest).

A_24881 - Nonce anfordern für Erstellung "Attestation der Umgebung"
Das PS MUSS, um die Nutzerauthentifizierung zu starten, die Operation *getNonce* nutzen gemäß [I_Authorization_Service].**[<=]**

A_24882-01 - Signatur clientAttest
Das PS MUSS zum Signieren des clientAttest-JWT mit der SMC-B die Konnektorschnittstelle `AuthSignatureService::ExternalAuthenticate` nutzen gemäß [gemSpec_Kon] und als zu signierende Daten den BinaryString den SHA-256-Hashwert des clientAttest-JWT in Base64-Codierung übergeben. **[<=]**

A_24883-02 - clientAttest als ECDSA-Signatur
Das PS MUSS beim Signieren des clientAttest-JWT mit Operation *ExternalAuthenticate* den Signatur-Typ ECDSA-Signatur verwenden. Dazu MUSS im Element `dss:SignatureType` die URI urn:bsi:tr:03111:ecdsa übergeben werden. Nur wenn der Signaturversuch

scheitert, weil noch eine SMC-B G2 vorliegt, darf das PS auf eine PKCS#1-Signatur ausweichen.**[<=]**

A_24884-01 - clientAttest signieren als PKCS#1-Signatur
Das PS MUSS beim Signieren des clientAttest-JWT nach einem gescheiterten Versuch eine ECDSA-Signatur zu erzeugen, eine PKCS#1-Signatur erzeugen. Dazu MUSS im Element `dss:SignatureType` die URI urn:ietf:rfc:3447 übergeben werden. Als Signatur-Schema MUSS der Default-Wert für `SIG:SignatureSchemes` RSASSA-PSS genutzt werden.**[<=]**

A_24886-02 - clientAttest als ClientAttest
Das PS MUSS die signierte clientAttest-JWT als Parameter ClientAttest im sendAuthCodeSC setzen.**[<=]**

A_20666-02 - Auslesen des Authentisierungszertifikates
Das Primärsystem MUSS das Zertifikat `C.HCI.AUT` der SM-B über die Operation `ReadCardCertificate` des Konnektors gemäß [gemSpec_Kon#4.1.9.5.2] bzw. [gemILF_PS#4.4.4.2] auslesen.**[<=]**

A_25720 - Auslesen des Authentisierungszertifikates aus einem HSM
Das CS des Kostenträgers MUSS das Zertifikat `ID.HCI.AUT` der SM-B über die Operation `CardCertificate` des Basis-Consumers gemäß [gemSpec_Basis_KTR_Consumer#4.1.9.5.2] auslesen. **[<=]**

Hinweis: Damit das bei der Signatur bevorzugt zu verwendende ECC-Zertifikat gelesen wird, muss bei der Operation `ReadCardCertificate` (oder aber im Falle des CS des KTR bei der Operation `ReadCertificate`) der Parameter `Crypt` auf "ECC" gesetzt werden. Nur bei einer Karte der Generation G2 kann der Default (RSA) genutzt werden.

Der eigentliche IDP-Flow startet mit der Anfrage des PS an den Authorization Service (1). Dazu nutzt es folgende Operation:

Tabelle 3: I_Authorization_Service::send_Authorization_Request_SC

REST-Schnittstelle des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)	
I_Authorization_Service	
sendAuthorizationRequestSC	Mit dieser Operation wird die Authentifizierung eines Leistungserbringers durch einen IDP initiiert.

A_24760 - Start der Nutzerauthentifizierung
Das PS MUSS, um die Nutzerauthentifizierung zu starten, die Operation *sendAuthorizationRequestSC* nutzen gemäß [I_Authorization_Service].**[<=]**

Die Response enthält "clientID" (des Aktensystems),"response_type", "redirect_uri", "state", "code_challenge", "code_challenge_method", "scope" und "nonce" (3 und 4).

Das Authenticator Modul des PS stellt nun einen GET: AUTHORIZATION REQUEST an den zentralen IDP mit den vom Authorization Service erhaltenen Parametern (5).

A_24944-01 - Anfrage des "AUTHORIZATION_CODE" für ein "ID_TOKEN"
Das Primärsystem MUSS in Form eines HTTP/1.1 GET AuthorizationRequest beim Authorization-Endpunkt (URI_AUTH) den Antrag zum Erhalt eines "AUTHORIZATION_CODE" für ein "ID_TOKEN" stellen. Dabei übermittelt es die folgenden Attribute, die aus der Response von send_Authorization_Request stammen:

- "response_type"
- "scope"

- "nonce"
- "client_id"
- "redirect_uri"
- "code_challenge" (Hashwert des "code_verifier") [RFC7636 # section-4.2]
- "code_challenge_method" HASH-Algorithmus (S256) [RFC7636 # section-4.3]
- "state"

[<=]

Der Authorization-Endpunkt legt nun eine "session_id" an, stellt alle nötigen Informationen zusammen und erzeugt das "CHALLENGE_TOKEN".
Darüber hinaus stellt der Authorization-Endpunkt den im Claim des entsprechenden Fachdienstes vereinbarten "Consent" zusammen, welcher die für dessen Funktion notwendigen Attribute beinhaltet.

Der IDP-Dienst antwortet dem PS dann mit dem Challenge-Token und dem User Consent (6a).

A_20662 - Annahme des "user_consent" und des "CHALLENGE_TOKEN"
Das Primärsystem MUSS den "user_consent" und den "CHALLENGE_TOKEN" vom Authorization-Endpunkt des IDP-Dienstes annehmen. Der Authorization-Endpunkt liefert diese als Antwort auf den Authorization-Request des Primärsystems.**[<=]**

A_20663-01 - Prüfung der Signatur des CHALLENGE_TOKEN
Das Primärsystem MUSS die Signatur des "CHALLENGE_TOKEN" gegen den aktuellen öffentlichen Schlüssel des Authorization-Endpunktes "PUK_IDP_SIG" prüfen. Liegt dem Primärsystem der öffentliche Schlüssel des Authorization-Endpunktes noch nicht vor, MUSS es diesen gemäß dem "kid"-Parameter "puk_idp_sig" aus dem Discovery Document abrufen.**[<=]**

Das Primärsystem verwendet nun die AUT-Identität der SM-B der LEI und deren Konnektor, um das gehashte "CHALLENGE_TOKEN" des IDP-Dienstes zu signieren. Wenn es sich um eine erstmalige Anmeldung des Benutzers bei diesem Fachdienst handelt, werden diesem darüber hinaus die für den Zugriff übermittelten Daten der LEI angezeigt.

A_20665-01 - Signatur der Challenge des IdP-Dienstes
Das Primärsystem MUSS für das Signieren des CHALLENGE_TOKEN des IdP-Dienstes mit der Identität ID.HCI.AUT der SM-B die Operation ExternalAuthenticate des Konnektors gemäß [gemSpec_Kon#4.1.13.4] bzw. [gemILF_PS#4.4.6.1] verwenden und als zu signierende Daten `BinaryString` den SHA-256-Hashwert des CHALLENGE_TOKEN in Base64-Codierung übergeben.
[<=]

A_24751 - Challenge signieren als ECDSA-Signatur
Das PS MUSS beim Signieren der Challenge mit Operation *ExternalAuthenticate* den Signatur-Typ ECDSA-Signatur verwenden. Dazu MUSS im Element `dss:SignatureType` die URI urn:bsi:tr:03111:ecdsa übergeben werden. Nur wenn der Signaturversuch scheitert, weil noch eine SMC-B G2 vorliegt, darf das PS auf eine PKCS#1-Signatur ausweichen.**[<=]**

A_24752 - Challenge signieren als PKCS#1-Signatur
Das PS muss beim Signieren der Challenge nach einem gescheiterten Versuch eine ECDSA-Signatur zu erzeugen, eine PKCS#1-Signatur erzeugen. Dazu MUSS im Element `dss:SignatureType` die URI urn:ietf:rfc:3447 übergeben werden. Als Signatur-Schema MUSS der Default-Wert für `SIG:SignatureSchemes` RSASSA-PSS genutzt werden.**[<=]**

Anschließend werden die signierte "challenge" und das verwendete Authentisierungszertifikat der Smartcard an den IDP-Dienst übermittelt (6b).

A_20667-01 - Response auf die Challenge des Authorization-Endpunktes
Das Primärsystem MUSS das eingereichte "CHALLENGE_TOKEN" zusammen mit der von der Smartcard signierten Challenge-Signatur "signed_challenge" (siehe A_20665) und dem Authentifizierungszertifikat der Smartcard (siehe A_20666), mit dem öffentlichen Schlüssel des Authorization-Endpunktes "PUK_IDP_ENC" verschlüsselt, in Form eines HTTP-POST-Requests senden.**[<=]**

Hinweis: Der Aufbau der Anfrage und der einzureichenden Objekte entspricht [gemSpec_IDP_Dienst#7.3 Authentication Request].

Hinweis: Das Signieren und Verschlüsseln des "CHALLENGE_TOKEN" ist durch die Verwendung eines Nested JWT [angelehnt an den folgenden Draft: https://tools.ietf.org/html/draft-yusef-oauth-nested-jwt-03, zu realisieren. Im cty-Header ist "NJWT" zu setzen, um anzuzeigen, dass es sich um einen Nested JWT handelt. Das Signieren wird dabei durch die Verwendung einer JSON Web Signature (JWS) [RFC7515 # section-3 - Compact Serialization] gewährleistet. Die Verschlüsselung des signierten Token wird durch die Nutzung der JSON Web Encryption (JWE) [RFC7516 # section-3] sichergestellt. Als Verschlüsselungsalgorithmus ist ECDH-ES (Elliptic Curve Diffie-Hellman Ephemeral Static key agreement) vorgesehen.

Der Authorization-Endpunkt validiert nun die "session" sowie die "signed_challenge" und prüft das Zertifikat der LEI. Anschließend verknüpft er die "session" mit der Identität aus dem Authentisierungszertifikat und erstellt einen "AUTHORIZATION_CODE", welchen er als Antwort zurücksendet.

Das Primärsystem empfängt nun diesen "AUTHORIZATION_CODE" vom IDP-Dienst (7).

A_20668 - Annahme des "AUTHORIZATION_CODE"
Das Primärsystem MUSS den vom Authorization-Endpunkt als Antwort auf die signierte Challenge gesendeten "AUTHORIZATION_CODE" verarbeiten. Das Primärsystem MUSS das "AUTHORIZATION_CODE" ablehnen, wenn dieser außerhalb der mit dem Authorization-Endpunkt etablierten TLS-Verbindung übertragen wird.**[<=]**

Das PS sendet diesen Authorization Code an den Authorization Service des Aktensystems (9). Dazu nutzt es die Operation sendAuthCodeSC:

Tabelle 4: I_Authorization_Service::sendAuthCode

REST-Schnittstelle des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)	
I_Authorization_Service	
sendAuthCodeSC	Diese Operation sendet den vom IDP-Dienst erhaltenen Auth-Code an den Authorization Service.

A_24766 - Abschluss der Nutzerauthentifizierung
Das PS MUSS, um die Nutzerauthentifizierung abzuschließen, die Operation *sendAuthCode* nutzen gemäß [I_Authorization_Service].
[<=]

Mit der *send_AuthCode*-Response erhält das Primärsystem die Zugriffserlaubnis auf das Aktensystem. Die User-Session ist dann etabliert und fachliche Operationen sind möglich.

3.3.2.1 Übergreifende Festlegungen zur Nutzung des IDP-Dienstes

Zur Nutzung des IDP-Dienstes gelten einige grundlegende Voraussetzungen, welche das PS erfüllen muss:

A_20655 - Regelmäßiges Einlesen des Discovery Document
Das Primärsystem MUSS das Discovery Document (DD) [RFC8414] regelmäßig alle 24 Stunden einlesen und auswerten, und danach die darin aufgeführten URI zu den benötigten öffentlichen Schlüsseln (PUKs) und Diensten verwenden.
Der Downloadpunkt wird als Teil der organisatorischen Registrierung des Primärsystems beim IDP-Dienst übergeben.
Das Primärsystem MUSS den Downloadpunkt des Discovery Document als konfigurierbaren Parameter speichern. **[<=]**

A_20656-01 - Prüfung der Signatur des Discovery Document
Das Primärsystem MUSS die JWS (JSON Web Signature) [RFC7515 # section-3 - Compact Serialization] Signatur des Discovery Document auf mathematische Korrektheit sowie über die Funktion "VerifyCertificate" des Konnektors gemäß [gemSpec_Kon#4.1.9.5.3] bzw. [gemILF_PS#4.4.4.3] auf Gültigkeit des ausstellenden Zertifikates innerhalb der TI prüfen.
[<=]

Hinweis: Der genaue Aufbau entspricht [gemSpec_IDP_Dienst#7.7 Aufbau des Discovery Document].

Bei Aufruf der Funktion "VerifyDocument" an der Außenschnittstelle des Konnektors ist es nicht möglich, direkt auch eine Prüfung des Zertifikatstyps und der Rollen-OID durchzuführen.

A_20657 - Prüfung der Signatur des Discovery Document
Das Primärsystem MUSS die Signatur des Discovery Document auf ein zeitlich gültiges C.FD.SIG-Zertifikat mit der Rollen-OID "oid_idpd" zurückführen können.**[<=]**

Hinweis: Zur Durchführung der Prüfungen gemäß A_20657 und ähnlicher Anforderungen ist zu verifizieren, ob im Feld certificatePolicies (2.5.29.32) des Zertifikates der richtige Zertifikatstyp FD.SIG (1.2.276.0.76.4.203) gemäß [gemSpec_OID#Tabelle Tab_PKI_405] eingetragen ist und sich in der Admission (1.3.36.8.3.3) des Zertifikats die richtige "oid_idpd" (1.2.276.0.76.4.260) findet.

3.4 Lokalisierung der Akte eines Versicherten

Wenn dem Primärsystem nicht bekannt ist, bei welchem Aktensystembetreiber ein Aktenkonto liegt, muss es den zuständigen Service-Endpunkt ermitteln. Dazu wendet sich das PS an den **Information Service** außerhalb der VAU eines Aktensystems, um dort nach der Akte zu fragen.

Konnte das Aktenkonto ermittelt werden, wird der zuständige Service-Endpunkt gespeichert. Gibt der Informationsdienst den Aktenkonto-Status "Unknown" zurück, wiederholt das Primärsystem den Aufruf beim nächsten Aktensystem.

Kennt kein Aktensystem die Akte, hat der Versicherte der ePA widersprochen und es existiert keine Akte.

Dazu wird folgende Operation genutzt:

Tabelle 5: I_Information_Service::getRecordStatus

REST-Schnittstelle des Aktensystems (Nutzung ohne VAU-Kanal)	
I_Information_Service	
`getRecordStatus`	Diese Operation ermittelt, ob für die übergebene KVNR ein Aktenkonto existiert und in welchem Status

	es ist.

A_24499 - Nutzung der Schnittstelle I_Information_Service
Das PS MUSS die Operation getRecordStatus nutzen gemäß [I_Information_Service].**[<=]**

A_24435-01 - Ermitteln des zuständigen Service-Endpunkts zu einem Aktenkonto
Das PS MUSS für die Lokalisierung eines freigeschalteten Aktenkontos eine Mappingliste heranziehen, in der IK-Nummern den Service-Endpunkten der Aktensystembetreiber zugeordnet sind, um im Regelfall zuerst das Aktensystem aufzurufen, bei dem das Aktenkonto mit hoher Wahrscheinlichkeit zu finden ist. Ergibt die Abfrage des ersten Aktensystembetreibers ein negatives Ergebnis (http 404), sind die weiteren Aktensystembetreiber in zufälliger Reihenfolge aufzurufen. **[<=]**

Die Zuordnung zwischen KVNR und IK-Nummer des Versicherten erfolgt primärsystemspezifisch und ist nicht weiter vorgegeben.
Sind auch die weiteren Abfragen negativ, liegt kein Aktenkonto vor (z.B. weil der ePA widersprochen wurde).

A_26258 - Aktualisierung der Mapping-Liste
Das PS MUSS die Mappingliste aktualisieren, wenn ein Aktenkonto bei einem anderen, als dem ursprünglich vermuteten, Service-Endpunkt lokalisiert werden konnte.**[<=]**

A_26259 - Lokalisierung eines Aktenkontos mit bekanntem Service-Endpunkt
Das PS MUSS sicherstellen, dass es den Service-Endpunkt eines Aktenkontos nur dann erneut ermittelt, wenn der Zugriff auf den bekannten Endpunkt mit dem Status "Unknown" (http-Fehler 404) beantwortet wurde.**[<=]**

A_26260 - Häufigkeit der Lokalisierung eines Aktenkontos
Das PS DARF die Lokalisierung eines Aktenkontos je KVNR NICHT häufiger als einmal täglich automatisiert (ohne Nutzerinteraktion) durchführen. Konnte für eine KVNR kein Aktenkonto lokalisiert werden, ist es zulässig diese Information zu persistieren und keine automatisierte erneute Lokalisierung durchzuführen.**[<=]**

A_25146 - Aktenlokalisierung als Hintergrundprozess
Das PS MUSS die Lokalisierung der Akte ohne Nutzeraktion im Rahmen eines ePA-Zugriffs durchführen, wenn noch kein Service-Endpunkt zur Akte vorliegt. Dieses soll im Hintergrund ablaufen und darf nicht die Weiterarbeit behindern.**[<=]**

A_24439-02 - Speichern und Nutzen des zuständigen Service-Endpunkts zu einem Aktenkonto
Das PS MUSS den zuständigen Service-Endpunkt zu einem Aktenkonto speichern und verwenden.**[<=]**

A_24445 - Fehlermeldung Akte existiert nicht
Das PS MUSS dem Nutzer eine verständliche Fehlermeldung oder eine eindeutige Statusinformation anzeigen, wenn alle verfügbaren Aktensysteme angefragt wurden und alle den Status "Unknown" zurückgeben.**[<=]**

3.4.1 Aktenkontokennung

Das PS adressiert das gewünschte Aktenkonto über die KVNR des Versicherten. Diese wird als HTTP-Header-Element mit dem Namen "x-insurantId" gesendet. Dies gilt für alle Services der ePA für alle.

A_24998 - InsurantID im Nachrichtenheader
Das PS MUSS bei Aufrufen ein HTTP Header Element mit dem Namen "x-insurantId" senden, um das Aktenkonto zu adressieren.**[<=]**

3.4.2 Logout

Das Primärsystem muss sich nicht explizit aus dem ePA-Aktensystem ausloggen. Ein implizites Logout findet statt,

- wenn die User Session endet,
- wenn der VAU-Kanal geschlossen wird.

Eine VAU schließt nach 20 Minuten Inaktivität automatisch die "UserSession" (gemSpec_Aktensystem#A_25006). Die VAU-Schlüssel (und damit auch die Nutzer-Authentisierung) müssen davon unabhängig mindestens alle 24 Stunden erneuert werden (neuer Verbindungsaufbau VAU-Protokoll + anschließende Nutzerauthentisierung). Eine VAU-Verbindung kann bspw. über alle 15 Minuten Abfragen von /VAU-Status [gemSpec_Krypt#A_25143] ohne anliegende fachliche Operation offen gehalten werden. Das ID-Token besitzt eine maximale Gültigkeitsdauer von 24 Stunden.

3.4.3 Zertifikate

Die kryptographischen Vorgaben im TLS-Bereich sind für das E-Rezept und ePA für alle ähnlich. Das VAU-Protokoll der ePA für alle unterscheidet sich vom E-Rezept-VAU-Protokoll, weil eine andere Authentisierungsvariante von OIDC/OAuth2/PCKE verwendet wird. Diese wird in einer späteren Ausbaustufe vom E-Rezept ebenfalls verwendet. Ab dann verwenden beide Anwendungen das VAU-Protokoll von ePA-für-alle.

A_24578 - Kryptografische Vorgaben für TLS- und VAU-Clients
Das PS MUSS alle Anforderungen zur Benutzung von Zertifikaten bei den Kommunikationsprotokollen TLS und VAU-Protokoll für die Kommunikation mit dem ePA-Aktensystem umsetzen, die in [gemSpec_Krypt#3.15.3] (ePA-spezifische TLS-Vorgaben) und in [gemSpec_Krypt#7] (VAU-Protokoll für ePA-für-alle) für einen ePA-Client definiert sind.
[<=]

A_24556 - Verpflichtende Zertifikatsprüfung
Das PS MUSS als ePA-Client alle Zertifikate der Tabelle TAB_ILF_Zertifikate, die es aktiv verwendet (bspw. TLS-Verbindungsaufbau), auf Integrität und Authentizität prüfen. Falls die Prüfung kein positives Ergebnis ("gültig") liefert, so MUSS es die von dem Zertifikat und den darin enthaltenen Attributen (bspw. öffentliche Schlüssel) abhängenden Arbeitsabläufe ablehnen.
Das Primärsystem MUSS alle öffentlichen Schlüssel, die es verwenden will, auf eine positiv verlaufene Zertifikatsprüfung zurückführen können.**[<=]**

Tabelle 6: TAB_ILF_Zertifikate

Aktivität	Zertifikat der TI	Zertifikatstyp	Rollen-OID	Nutzung
TLS-Verbindungsaufbau zum ePA-Aktensystem	ja	C.FD.TLS-S	oid_epa_dvw	aktiv
TLS-Verbindungsaufbau zum Verzeichnisdienst der TI	nein	TLS Internet Zertifikat	n/a	aktiv

TLS-Verbindungsaufbau zum IDP	nein	TLS Internet Zertifikat	n/a	aktiv
Aufbau sicherer Kanal zur VAU des ePA-Aktensystems	ja	C.FD.AUT	oid_epa_vau	aktiv

A_24900 - Prüfung TI-Zertifikate
Das Primärsystem MUSS X.509-Zertifikate der TI auf eine der beiden folgenden beiden Arten prüfen:

1. Verwenden des `CertificateService` des Konnektors mit der Operation `VerifyCertificate` gemäß [gemSpec_Kon#4.1.9.5.3], wobei das zu prüfende Zertifikat als Parameter `X509Certificate` und die aktuelle Systemzeit als Parameter `VerificationTime` verwendet werden. Das Primärsystem MUSS bei Prüfung von TI-Zertifikaten der TAB_ILF_Zertifikate den Rückgabewert in `RoleList` gegen die erwartete Rollen-OID prüfen.
2. Das Primärsystem prüft die TI-Zertifikate selbst ohne Nutzung des Konnektors nach [gemSpec_PKI#TUC_PKI_018] mit folgenden Parametern:

Parameter	**Wert**
Zertifikat	C.FD.TLS-S (für TLS) bzw. C.FD.AUT (für VAU-Kanal)
PolicyList	oid_epa_dvw bzw. oid_epa_vau
intendedKeyUsage	digitalSignature
intendedExtendedKeyUsage	id-kp-serverAuth bzw. leer
OCSP-Graceperiod	60 Minuten
Offline-Modus	nein
Prüfmodus	OCSP

Ist die Zertifikatsprüfung nicht erfolgreich, ist der Verbindungsaufbau abzulehnen.**[<=]**

A_24906 - lokales Caching von Sperrinformationen und Toleranzzeiten
Das Primärsystem, welches im Rahmen von Zertifikatsprüfungen Sperrinformation für nonQES-Zertifikate einholt, MUSS folgende Vorgaben umsetzen:

1. Die Sperrinformationen (bspw. OCSP-Responses) müssen lokal gespeichert werden (caching), solange sie noch zeitlich gültig sind.
2. Definition zeitliche Gültigkeit: Sei p die Zeit zu der die Sperrinformation vom TSP erzeugt wurde. Im Fall von OCSP-Responses ist diese Zeit die productedAt-Angabe [RFC-6960]. Sei s die lokale Systemzeit des prüfenden Systems. Eine Sperrinformation ist zeitlich gültig, wenn gilt s - D <= p <= s + 5 Minuten, wobei D im default-Fall eine Stunde beträgt.
   (Es gibt anwendungsspezifische Verlängerungen der Gültigkeitsdauer D, die dann explizit in den entsprechenden Spezifikationen definiert werden.
   D. h. die Sperrinformation können im default-Fall maximal eine Stunde alt sein und

maximal für fünf Minuten "aus der Zukunft kommen". (Da nicht alle Produkttypen ihre Systemzeit in der TI synchronisieren, erlauben wir hier eine fünfminutige fehlerhafte Abweichung der lokalen Zeit.)

3. Das prüfende System muss, bevor es Sperrinformationen (bspw. für ein Zertifikat) einholt, prüfen, ob im Cache (vgl. Punkt 1) zeitlich gültige Sperrinformationen schon vorliegen. Falls ja, muss es diese Informationen verwenden und darf diese nicht neu beziehen.
4. Bei einer evtl. Abarbeitung von TUC_PKI_006 muss der optionale Eingabeparameter "OCSP-Graceperiod" ignoriert werden und für die zeitliche Gültigkeit ist Punkt 2 maßgeblich. Bei OCSP-Antworten ist in diesem Kontext die Konsistenzprüfung, wie in TUC_PKI_006 in Schritt 6 aufgeführt, fachlich unnötig und deshalb nicht durchzuführen.
5. Zeitlich ungültige Sperrinformation im Cache dürfen nicht für Zertifikatsprüfvorgänge verwendet werden und müssen mindestens alle 24h aus dem Cache aktiv entfernt werden.

[<=]

Kontext OCSP: Die aufgrund der historischen Entwicklung von OCSP als Abfragemechanismus einer CRL-Abfrage bei einem TSP stammenden Werte thisUpdate und nextUpdate sind für A_24906- irrelevant. Was zählt ist, dass der bestmögliche Informationsstand eines TSP zum Zeitpunkt producedAt in der Antwort dokumentiert ist. Dieser Informationsstand wird im Cache für die in A_24906-* aufgeführte Zeit als maßgeblich betrachtet und im prüfenden System verwendet.*

Falls Sperrinformationen grundsätzlich vom zu authentifizierenden System mit gesendet werden (bspw. TLS-OCSP-stapling, OCSP-Anwort der VAU innerhalb des VAU-Protokolls), so holt der Client diese nicht aktiv ein, d. h., A_24906- greift in Bezug auf das Caching nicht als MUSS-Bestimmung.*

3.5 SOAP

In der ePA für alle nutzt das Primärsystem SOAP für den Zugriff auf die IHE-Schnittstellen des XDS Document Service.

Die SOAP-Schnittstellen werden nachrichtenbasiert über SOAP1.2 mit [BasicProfile2.0] angesprochen.

Die Bildung der SOAP-Nachrichten durch das Primärsystem wird in diesem Dokument technologie-neutral geschildert. Dabei werden die Voraussetzungen für unterschiedliche Strategien zur Nachrichtenerzeugung geliefert, darunter:

- Nutzung von Template Engines
- Codegenerierung mittels WSDL und XSD.

Die ePA nutzt bei bestimmten Operationen den SOAP-Header, um Informationen über den Aktenkontext und die Telematik-ID zu erhalten.

A_14510 - Setzen erforderlicher Parameter im SOAP-Header
Das PS MUSS Parameter im SOAP-Header setzen, wenn diese in der jeweiligen Signatur der Operation gefordert sind.**[<=]**

A_15569 - Verwendung von Byte Order Mark in SOAP-Nachrichten
Das PS KANN einen UTF-8 Unicode Byte Order Mark (BOM) gemäß [BasicProfile1.2#3.1.2] setzen.**[<=]**

A_15570-02 - Content-Type und Charset im http-Header

Das PS MUSS abweichend von R1012 in [BasicProfile1.2] und [BasicProfile2.0] ausschließlich das Character Encoding UTF-8 in der Nachricht benutzen und das charset im http-Header auf UTF-8 setzen.**[<=]**

3.6 REST

In der ePA für alle werden die vom Primärsystem angesprochenen Dienste wie der Information Service, Entitlement Management und den Medication Service über OpenAPI- sowie FHIR-Profildefinitionen festgelegt. Die Schnittstellen und Operationen sind funktional in den Beschreibungen der jeweiligen Schnittstelle vermerkt.

3.7 Mandantenverwaltung

Sowohl Befugnisse, VAU als auch ID-Token verwenden dedizierte anwendungsfallübergreifend identische Telematik-IDs. In größeren Einrichtungen muss dabei unter Datenschutz-Gesichtspunkten die Einrichtung einer Mandantenverwaltung für die Nutzung der ePA sowie ein ausreichendes Logging von Aktenzugriffen beachtet werden.

Die Nutzung ePA-fähiger Aufrufkontexte ist in kleineren Einrichtungen mit nur einer einzigen verwendeten SMC-B einfacher umzusetzen als in großen Einrichtungen, in denen es viele verwendete SMC-Bs zu konfigurieren gilt. Eine Voraussetzung für eine funktionierende ePA besteht darin, dass die Leistungserbringerinstitution so konfiguriert ist, dass die Telematik-ID der signierten Befugnis , die Telematik-ID aus der VAU-Instanz, sowie die Telematik-ID aus dem IDP-Token gleich sind.

A_24401 - Mandantenweite Verwendung der korrekten SMC-B
Das PS MUSS sicherstellen, dass bei Vorhandensein mehrerer Mandanten in einer LEI jeder Mandant nur seine eigene SMC-B für den Aufbau der VAU, die Erstellung der Befugnis-Signatur und das IDP-Token verwendet.**[<=]**

Die Verwendung der korrekten SMC-B wird über den Aufrufkontext gesteuert.

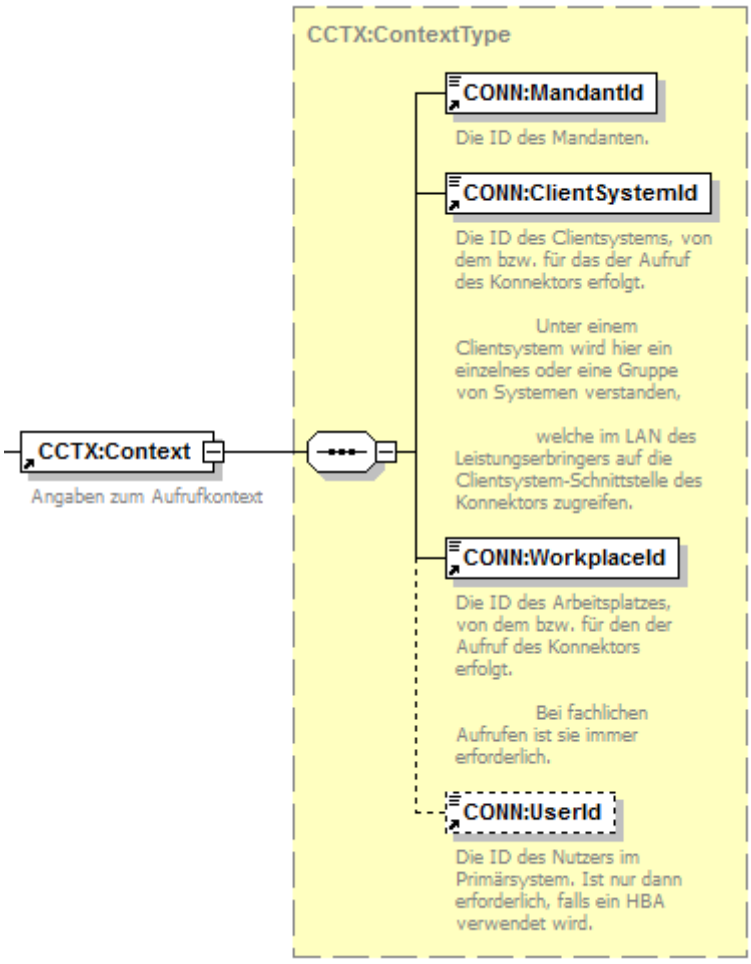

Abbildung 12: ILF_ePA_Element_Context

Beispiel 1: Bsp_ILF_ePA_Context

```
<m0:Context>
<m1:MandantId>m0001</m1:MandantId>
<m1:ClientSystemId>csid0001</m1:ClientSystemId>
<m1:WorkplaceId>wpid007</m1:WorkplaceId>
</m0:Context>
```

3.8 Funktionsmerkmale

Leistungserbringerinstitutionen haben zwei Möglichkeiten, vom Versicherten eine Befugnis zum Zugriff auf das Aktenkonto zu erhalten:

1. Der Versicherte erteilt eine Befugnis für die LE-Institution am ePA-Frontend des Versicherten.
2. Im Behandlungskontext wird vom PS, im Zusammenhang mit dem Einlesen der eGK, eine Befugnis eingestellt.

Die Befugnis kann sowohl vom Versicherten selbst stammen, als auch vom Vertreter des Versicherten. Sie ist auf Leistungserbringerinstitutionen (inkl. deren berufsmäßigen Gehilfen oder zur Vorbereitung auf den Beruf Tätige, jedoch nicht die Gehilfen der nichtärztlichen Psychotherapeuten) eingeschränkt.

Die Laufzeit von Befugnissen ist begrenzt. Falls eine Befugnis aufgrund einem in der Vergangenheit liegenden `validTO` oder Befugnisentzug am ePA-Frontend des Versicherten nicht mehr existiert, ist eine erneute Befugnisvergabe erforderlich.

A_15090 - Protokollierung Dokumententransfer im Übertragungsprotokoll
Jeder Dokumententransfer (Dokumente einstellen, laden, löschen) MUSS im Übertragungsprotokoll vermerkt werden.**[<=]**

3.9 Erstellen einer Befugnis

Die Leistungserbringerorganisation benötigt eine Befugnis (Entitlement), um auf die ePA eines Versicherten zugreifen zu können.

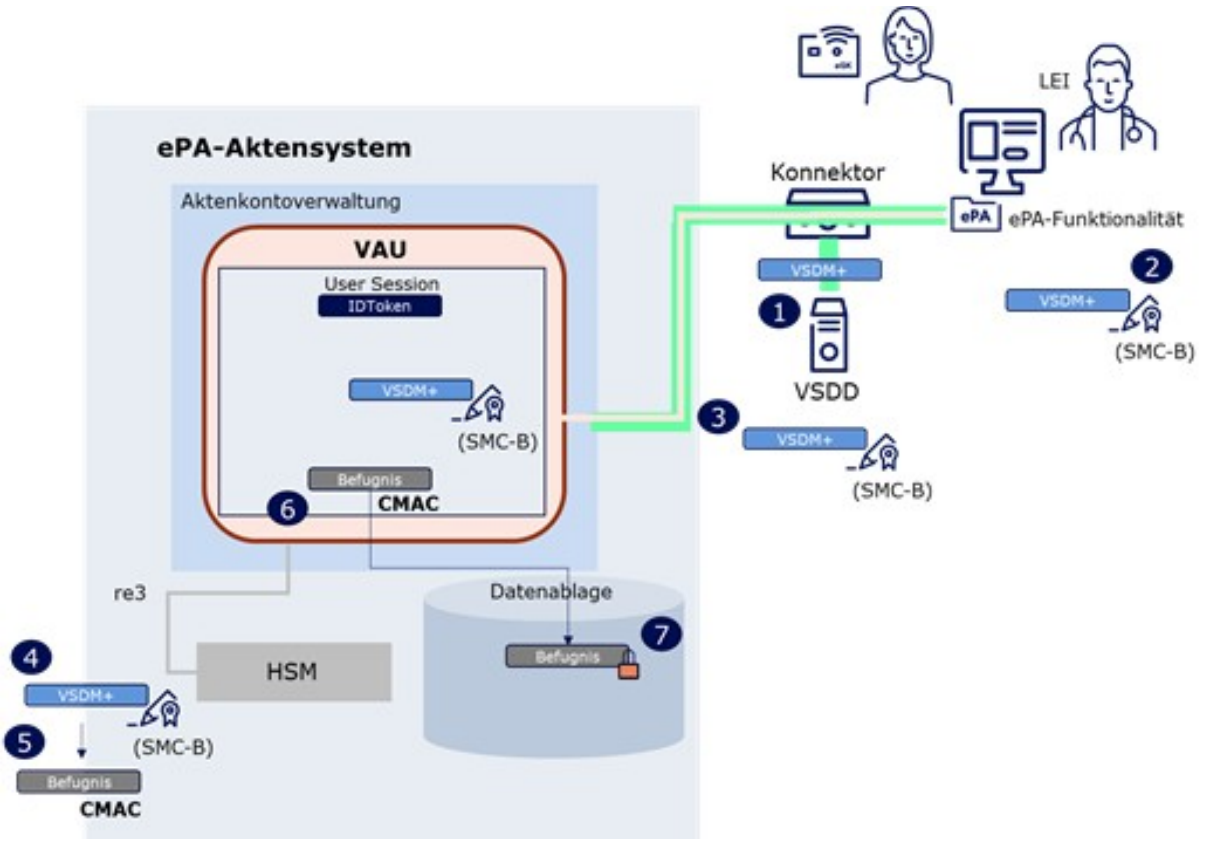

Abbildung 13: Ablauf Erstellung einer Befugnis

Der Auslöser zur Erstellung einer Befugnis ist das etablierte Lesen der eGK mit Onlineprüfung oder der Prozess der Befugniserstellung durch den Versicherten an dessen FdV. Ein ReadVSD auf die eGK wird beim ersten Praxisbesuch im Quartal, bei der Aufnahme im Krankenhaus oder bei der Einlösung eines eRezeptes mit eGK in der Apotheke durchgeführt.

Liegen in einer größeren Institution mehrere Mandanten vor, die auf die ePA eines Versicherten zugreifen wollen, so muss das ReadVSD für jeden dieser Mandanten mittels deren SM-B erfolgten.

Dabei wird vom Konnektor-Fachmodul VSDM ein Prüfungsnachweis erzeugt und in der ReadVSD-Response an das PS geliefert. Der Prüfungsnachweis enthält im Falle einer erfolgreichen Online-Prüfung (Ergebnis 1 oder 2) im Element Receipt die Prüfziffer des Fachdienstes als eine Base64Binary-kodierte Folge von bis zu 65 Bytes.

Damit die Prüfziffer in Verbindung zur Umgebung gesetzt werden kann, erfolgt die Erstellung eines signierten JSON-Web-Token (JWS). Dazu wird das JWS mit der AUT-Identität der SM-B signiert (2), bevor es im Entitlement Management des Aktensystems als Befugnis registriert (3) wird.

Die Befugnisdauer wird vom Aktensystem festgelegt. Die in der LEI erzeugte Befugnis muss innerhalb dieses Zeitraumes nicht erneuert werden. Im Falle eines späteren Hochladens eines neueren `Entitlements` im vorliegenden Quartal gilt der aktuellere bzw. aktualisierte Befugniszeitraum.

Die Befugnisdauer beträgt

- 3 Tage für Apotheken, ÖGD und Institutionen der Arbeits- und Betriebsmedizin und
- 90 Tage für alle anderen Arten von Leistungserbringer-Institutionen.

Eine erstellte Befugnis muss im Primärsystem nicht vorgehalten und damit in verteilten Systemen einem anderen System nicht bekannt gemacht werden. Die Befugnis liegt im ePA-Aktensystem vor und dieses prüft im Zuge des Aktenzugriffs aus einer LEI, ob diese zugriffsbefugt ist. Eine Befugnis kann auch vom Versicherten aus erstellt werden mithilfe des ePA FdV.

Das Einstellen einer Befugnis aus der LEI-Umgebung erfolgt über folgende Operation des **Entitlement Management** des Aktensystems:

Tabelle 7: I_Entitlement_Management::setEntitlementPs

REST-Schnittstelle des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)	
I_Entitlement_Management	
`setEntitlementPs`	Diese Operation registriert eine Befugnis im Entitlemanagent.

A_24388 - Einstellen der LEI-Befugnis in die ePA für alle
Das PS MUSS für das Einstellen einer Befugnis die Operation *setEntitlementPs* nutzen gemäß [I_Entitlement_Management].**[<=]**

3.9.1 Umsetzung

Die Aktivitäten des Anwendungsfalles *Erstellen einer Befugnis* sind:

Vorbedingung:

- Ermittelter `Service-Endpunkt` zum Aktenkonto
- erfolgreiches ReadVSD mit Online-Prüfung

Auslöser:

- Erhalt einer Prüfziffer durch Lesen der eGK mit erfolgreicher Online-Prüfung (Prüfnachweis 1 oder 2)
- manuelle Auslösung
- Nachfrage bei uploadpflichtigen PVS-Aktionen und fehlender Berechtigung

Aktivitäten:

- Auswahl KVNR
- Auswahl des `Service-Endpunkts` zum Aktenkonto
- Auswahl der Prüfziffer des Versicherten
- Bildung eines JWS mit Prüfziffer und Zertifikat
- JWS signieren mit SMC-B
- JWS als Entitlement einstellen
- Auswertung des Ergebnisses

Resultat:

- Die Antwort gibt Auskunft darüber, ob eine Befugnis im Aktensystem erzeugt werden konnte oder nicht.

- Das Einstellen scheitert z. B., wenn die SMC-B nicht zur Gruppe der erlaubten Berufsrollen (professionOID) gehört oder wenn die LEI selbst oder die ganze Nutzergruppe vom Versicherten geblockt wurde.
- Die Antwort enthält im Erfolgsfall mit dem *validTo* das Enddatum der Befugnisdauer. Das PS kann die Befugnisdauer persistieren.

3.9.2 Nutzung

A_24398 - Prüfung auf Durchführbarkeit der Befugnis-Erstellung
Das PS MUSS den Prüfungsnachweis daraufhin prüfen, ob ein Prüfergebnis 1 oder 2 vorliegt und anderenfalls den UseCase *Erstellen einer Befugnis* abbrechen.**[<=]**

A_24391 - Das Entitlement in zeitnahem Kontext der VSDM-Prüfung in die ePA hochladen
Nach Erzeugen eines VSDM-Prüfungsnachweises für einen bestimmten Versicherten MUSS das PS die signierte Prüfziffer innerhalb von 20 Minuten als `Entitlement` für einen Zugriff auf seine Akte über die Schnittstelle `I_Entitlement_Management` in die ePA einstellen.**[<=]**

A_24528 - Einstellen einer Befugnis ohne Nutzeraktion
Das PS MUSS das Einstellen der Befugnis so implementieren, dass dazu keine eigene Nutzeraktion notwendig ist.**[<=]**

A_24400 - Prüfziffer als JWS signieren mit ExternalAuthenticate
Das PS MUSS zum Signieren der Prüfziffer mit der SMC-B des ePA-Mandanten die Konnektorschnittstelle `AuthSignatureService::ExternalAuthenticate` nutzen gemäß [gemSpec_Kon].**[<=]**

A_24540 - Prüfziffer als JWS signieren als ECDSA-Signatur
Das PS MUSS beim Signieren des JWS mit Operation *ExternalAuthenticate* den Signatur-Typ ECDSA-Signatur verwenden. Dazu MUSS im Element `dss:SignatureType` die URI urn:bsi:tr:03111:ecdsa übergeben werden. Nur wenn der Signaturversuch scheitert, weil noch eine SMC-B G2 vorliegt, darf das PS auf eine PKCS#1-Signatur ausweichen.**[<=]**

A_24542 - Prüfziffer als JWS signieren als PKCS#1-Signatur
Das PS MUSS beim Signieren des JWS nach einem gescheiterten Versuch eine ECDSA-Signatur zu erzeugen, eine PKCS#1-Signatur erzeugen. Dazu MUSS im Element `dss:SignatureType` die URI urn:ietf:rfc:3447 übergeben werden. Als Signatur-Schema MUSS der Default-Wert für `SIG:SignatureSchemes` RSASSA-PSS genutzt werden.**[<=]**

Getrennte Mandanten im Primärsystem verfügen über SMC-Bs mit je verschiedenen Telematik-IDs. Wenn es SMC-Bs mit mehr als einer Telematik-ID gibt, muss dies in der Konfiguration von Konnektor und Primärsystem und im Aufrufkontextes der SMC-B berücksichtigt werden.

3.10 Versorgungsspezifische Services

Die ePA für alle unterstützt verschiedene Versorgungsprozesse mittels dedizierter Services. Initial unterstützt sie den digital gestützten **Medikationsprozess** (dgMP) durch die Bereitstellung einer Elektronischen Medikationsliste (eML) über einem FHIR Data Service.

3.10.1 Widersprüche zu Versorgungsprozessen abrufen

Versicherte können der Teilnahme an durch die ePA unterstützen Versorgungprozessen widersprechen. Das PS kann die Entscheidung zu Teilnahme (ConsentDecision) zur Behandlungsvorbereitung abfragen. Sie kann dabei den Zustand "kein Widerspruch erklärt" ("permit") oder "Widerspruch erklärt" ("deny") haben. Die Versorgungsprozesse werden über eine ID referenziert (z. B. die Teilnahme am Medikationsprozess "id":"medication").

Über diese Operation des **Information Service** kann das PS die Entscheidung zu den Versorgungsprozessen abfragen:

Tabelle 8: I_Information_Service::getConsentDecisionInformation

REST-Schnittstelle des Aktensystems (Nutzung ohne VAU-Kanal)	
I_Information_Service	
`getConsentDecisionInformation`	Diese Operation liest den aktuellen Zustand der Widersprüche gegen die Nutzung von widerspruchsfähigen Funktionen der Funktionsklasse "Versorgungsprozess" aus.

A_24493 - Nutzung der Schnittstelle I_Information_Service
Das PS MUSS es dem Nutzer ermöglichen, die Entscheidung zur Teilnahme an Versorgungsprozessen abzufragen unter der Verwendung der Operation *getConsentDecisionInformation* gemäß [I_Information_Service].**[<=]**

A_24368 - Persistieren der Information zur Teilnahme an Versorgungsprozessen
Das PS MUSS die erhaltenen Informationen zur Teilnahme an Versorgungsprozessen persistieren.**[<=]**

Wenn es bei Aufrufen im Rahmen des Versorgungsprozesses zu einem Fehler kommt, ist eine Wiederholung der Abfrage der Widersprüche sinnvoll.

3.10.2 Medikationsprozess

Der digital gestützte Medikationsprozess (dgMP) wird über eine elektronische Medikationsliste (eML) als auch einen elektronischen Medikationsplan (eMP) durch den Medication Service umgesetzt, welche vom Leistungserbringer über das Primärsystem abgerufen und angezeigt werden können. Die eML bzw. die Medikationshistorie hält sämtliche Medikationen des Versicherten vor. Durch optionale Eingabe eines Datumsbereichs kann über die entsprechende Schnittstelle eine verlaufsbasierte Einsicht auf diese Daten vorgenommen werden. Planungsmäßig erfasste Medikationen und Arzneimitteltherapiesicherheitsrelevante Zusatzinformationen (AMTS-rZI) können weiterhin durch die Erzeugung eines versionierten und optional verifizierten eMP mit aktuellen Medikationsinformationen eingesehen werden.

Basis für die eML sind primär Arzneimittelverordnungsdaten sowie Dispensierinformationen, welche ein Apothekenverwaltungssystem (AVS) dem E-Rezept-Fachdienst zur Verfügung stellt. Sofern der Versicherte dem Einstellen dieser Daten in den Medication Service nicht widersprochen hat, werden diese Daten bei Erzeugung durch Leistungserbringer über den E-Rezept-Fachdienst in den Medication Service automatisiert übertragen. Einträge der Medikationsplanung können von einem Primärsystem über dedizierte Management-Operationen gelesen oder auch manipuliert werden.

Der nachfolgend referenzierte FHIR-basierte Implementation Guide beschreibt Anforderungen an das Primärsystem zur Umsetzung der dgMP-Prozessabläufe.

A_26276 - Nutzung der Schnittstellen des FHIR IG Medication Service
Das PS MUSS die Schnittstellen des FHIR Implementation Guide für den Medication Service [IG_Medication_Service] bedienen.**[<=]**

3.11 Dokumentenmanagement

Für das Dokumentenmanagement in der ePA für alle nutzt das PS eine Profilierung der IHE-Spezifikationen rund um das Kernprofil `XDS.b` (Cross-Enterprise Document Sharing).

Tabelle 9: Tab_ILF_ePA_Profilierung

Profilierungen des Kernprofiles XDS.b	
Anwendungsfall	**IHE-Schnittstelle**
Dokumente einstellen	DocumentRepository_ProvideAndRegisterDocumentSet-b [ITI-41]
Dokumente suchen	Registry Stored Query [ITI-18]
Dokumente laden	Retrieve Document Set [ITI-43]
Dokument löschen	Remove Metadata [ITI-62]
Aktualisieren von Metadaten	Restricted Update Document Set [ITI-92]

A_24661-01 - Nutzung der Dokumentenmanagement-Schnittstelle I_Document_Management
Das PS MUSS die Aktensystemschnittstelle Schnittstelle I_Document_Management am Aktensystem der ePA für alle [gemSpec_Aktensystem_ePAfueralle#3.12.1.6.1] implementieren.**[<=]**

A_14418-01 - MTOM-Pflicht bei Verwendung von [ITI-41] und [ITI-43]
Das PS MUSS bei der Umsetzung der IHE XDS-Transaktionen [ITI-41] und [ITI-43] zur Übertragung von Dokumenten eine Kodierung mittels MTOM/XOP [MTOM] gemäß [IHE-ITI-TF-2b#3.39.5] mit Verweis auf [IHE-ITI-TF-2b#3.43.5] verwenden. **[<=]**

A_15084 - SOAP-Header nach [SOAP]
Das PS MUSS in der Kommunikation mit dem Aktensystem der ePA für alle die SOAP-Nachricht konform zu [SOAP] bilden. **[<=]**

Das Aktensystem setzt in `DocumentEntry.hash` eine Prüfsumme eines Dokumentes. Mithilfe dieser Prüfsumme kann ein PS eine Dublettenprüfung durchführen, um nicht unnötig Duplikate von Dokumenten in die ePA einzustellen oder Dokumente mehrfach herunterzuladen.

Das Aktensystem wirft einen Fehler mit dem Fehlercode `XDSDuplicateDocument`, wenn versucht wird, ein Dokument in die Akte eines Versicherten hochzuladen, das es dort schon gibt. Das Aktensystem führt die Dublettenprüfung mithilfe der Prüfsumme durch.

Ordner können durch die Option "Folder Management" (XDS.b Document Source) verwendet werden. Durch die Assoziation eines Dokumentes zu einem dieser Ordner wird

das Dokument dem Ordner der entsprechenden Dokumentenkategorie bzw. Dokumentensammlung zugeordnet. Nur für dynamische Dokumentensammlungen (pregnancy_childbirth) werden Ordner durch Primärsysteme erstellt, ansonsten werden Dokumente und Daten den Ordnern vom Aktensystem zugewiesen.

Die XDS-Option "Folder Management" ist nur für den geschilderten Verwendungszweck zugelassen; ein selbständiges Anlegen oder Bearbeiten von Ordnern und ihrer Metadaten ist nicht möglich. Das Entfernen von Dokumenten aus einem Ordner durch Löschen der entsprechenden Assoziation ist nicht vorgesehen, da dies die direkte Zuordnung gemäß einer Zugriffsunterbindungsregel verletzten könnte.

Wenn Dokumente verborgen eingestellt werden oder gelöscht werden, werden dadurch auch Dokumente verborgen bzw. gelöscht, die ihnen über Assoziationen verbunden sind.

Weitere übergreifenden Einschränkungen von IHE ITI-Transaktionen sowie Festlegungen spezieller Umsetzungsvorgaben bzgl. einzelner Transaktionen sind in [gemSpec_Aktensystem_ePAfueralle] beschrieben.

Wenn im Rahmen der IHE Interface-Beschreibung der Begriff "Patient" verwendet wird, ist im Rahmen der vorliegenden Spezifikation darunter der Aktenkontoinhaber zu verstehen.

3.11.1 Dokumente einstellen [ITI-41]

Ein eingestelltes Dokument kann auch ein existierendes Dokument ersetzen. Dies erfolgt durch Verwendung der „Document Replacement“-Option (XDS.b Document Source). Dazu wird das gleiche Dokument (mit geändertem Inhalt und nebst ggf. geänderten DocumentEntry-Metadaten) erneut hochgeladen. Das neue Dokument erhält den Status „Approved“. Das alte Dokument geht in den Status „Deprecated“. Beide Dokumente werden über eine „Replace“-Association miteinander verbunden, sodass nach dem Einstellen erkennbar ist, dass das neue Dokument das alte ersetzt. Lädt man erneut eine neue Fassung hoch, erhält man zwei Dokumente im Status "Deprecated" und das neueste im Status "Approved".

Alle alten Dokumente (Status "Deprecated") können nach wie vor gefunden und heruntergeladen werden. Einige Suchen erlauben das Filtern nach Status bzw. zeigen per Default auch nur Dokumente im Status „Approved“ an.
Eingestellt (im „Submission Set“) wird das neue Dokument inkl. DocumentEntry-Metadaten, ein Verweis auf das alte Dokument und die verbindende „Replace“-Association (urn:ihe:iti:2007:AssociationType:RPLC).

Das Ersetzen eines existierenden Dokuments mit der XDS-Option „Document Replacement“ eignet sich dafür, eine Änderung an einem bereits bestehenden Dokument abzubilden. Metadaten werden jedoch über Restricted Update Document Set geändert.

3.11.1.1 Umsetzung

Die Aktivitäten des Anwendungsfalles *Dokumente einstellen* sind:

Vorbedingungen:

- Dokumente sind einer KVNR zugeordnet
- Das einzustellende Dokument sollte mit dem Versicherten besprochen sein
- gültige Befugnis

Auslöser:

- Nutzerinteraktion
- Automatische Trigger

Aktivitäten:

- Auswahl der Dokumente
- Ermittlung der Metadaten zu den Dokumenten
- Generierung inklusive Metadaten
- Validierung der Nachricht
- Versand der Nachricht
- Auswertung des Ergebnisses

Resultat:

- Die Antwort gibt Auskunft darüber, ob die Dokumente eingestellt werden konnten oder nicht.

3.11.1.2 Nutzung

A_14253-01 - Metadaten-Pflicht für Dokumente
Das PS MUSS Metadaten ausschließlich aus der in [gemSpec_Aktensystem_ePAfueralle] aufgeführten Menge von Metadaten entnehmen. Das Primärsystem MUSS Dokumente, denen es keine passenden Metadaten zuweisen kann, von der Auswahl der einzustellenden Dokumente ausschließen. Das PS MUSS das Metadatenobjekt `XDSDocumentEntry` entsprechend den Vorgaben aus dem Datenmodell [gemSpec_Aktensystem_ePAfuerAlle#Tabelle Nutzungsvorgaben für Metadatenattribute XDS.b] befüllen. Das PS MUSS alle mit der Kardinalität [1..1] markierten Metadatenfelder setzen.**[<=]**

Die Auswahl der Metadaten soll möglichst weitgehend automatisiert werden.

A_16194 - Änderbarkeit der Metadaten - Auswahllisten
Bei der Auswahl der Metadaten zum Zwecke des Einstellens von Dokumenten SOLL das PS insbesondere im Falle erforderlicher Auswahldialoge beachten:

- die Bildung von Auswahllisten erfolgt gemäß Anhang B,
- Auswahllisten sind konfigurativ änderbar,
- Metadaten werden weitestgehend automatisch vorbefüllt,
- Nutzer können Metadaten editieren.

[<=]

A_20517-02 - Exklusivität der Dokumentenkategorien
Das PS MUSS beim Einstellen von Dokumenten die Kategorien beachten, zu denen Dokumente gehören. Dabei werden Kategorien durch zwei Arten von Foldern umgesetzt:

- Statische Folder. Die Zuordnung zu den Kategorien/Foldern erfolgt am Aktensystem aufgrund der vom PS gesetzten Metadaten. Die Angabe einer FolderUUID beim Hochladen von Dokumenten DARF NICHT erfolgen.
- Dynamische Folder. Dynamische Folder werden gemäß A_21610-* (`pregnancy_childbirth`) vom PS angelegt und die entsprechenden Dokumente dort eingestellt. Beim Hochladen von Dokumenten MUSS die FolderUUID angegeben werden.

[<=]

A_22515-02 - Pflicht zum Setzen von Dokumenten-Titeln
Das PS MUSS beim Einstellen von Dokumenten `documentEntry.title` belegen. Der Titel des Dokumentes MUSS eine fachliche Beschreibung des Dokumentes enthalten.**[<=]**

Dokumente werden statischen Ordnern automatisch am Aktensystem aufgrund der vergebenen Metadaten zugeordnet. Dokumente werden dynamischer Ordnern (`pregnancy_childbirth`) hingegen durch das PS zugeordnet.

Das Kinderuntersuchungsheft wird in die ePA des Kindes eingestellt.

A_22514-03 - Titel dynamischer Ordner für Schwangerschaften
Der Leistungserbringer legt bei Bedarf dynamische Ordner für `pregnancy_childbirth` an. Bei der Anlage dynamischer Ordner MUSS das PS das Metadatum `Folder.title` folgendermaßen setzen:

- Der dynamische Ordner der Kategorie `pregnancy_childbirth` identifiziert eine Schwangerschaft. Folder.title MUSS mit dem (ggf. prognostizierten) Entbindungstermin belegt werden.
- Bildungsregel: "Errechneter EBT: " + Datum im Format TT.MM.YYYY Beispiel: "Errechneter EBT: 03.03.2017"

[<=]

Der errechnete Entbindungstermin im dynamischen Ordner `pregnancy_childbirth` wird mit dem initial errechneten Wert befüllt. Eine spätere Änderung des Ordnernamens ist zur Identifizierung der Schwangerschaft nicht erforderlich, auch wenn zu einem späteren Zeitpunkt ein anderer Entbindungstermin errechnet werden sollte.

A_20180-04 - Für pregnancy_childbirth dynamischen Ordner auswählen
Falls das hochzuladende Dokument zur Kategorie `pregnancy_childbirth` gehört, MUSS das PS das hochzuladende Dokument genau einem der dynamischen Ordner `pregnancy_childbirth` zuweisen, indem es das Dokument in den entsprechenden Ordner hochlädt. Dazu MUSS das PS beim Einstellen im SubmissionSet mit dem `DocumentEntry` eine zusätzliche Association (FD-DE-HasMember) hinterlegen, die den `DocumentEntry` mit dem für die gewünschte Unterkategorie bereits existierenden Ordner über ihre jeweilige `entryUUID` verbindet, vgl. u.a. [IHE-ITI-TF3#4.2.1.3].**[<=]**

Die `entryUUID` des Ordners kann z. B. über die Suche `FindFolders` mit entsprechendem Filter auf `Folder.codeList` ermittelt werden.

A_25127 - Keine Verdoppelung dynamischer Ordner
Dynamische Ordner zu einem Anwendungsfall (z.B. zu einer Schwangerschaft) DÜRFEN NICHT doppelt angelegt werden.**[<=]**

A_14932 - Bildung und Verwendung einer UUID für Dokumente
Das PS MUSS eine `DocumentEntry.UniqueID` gemäß [ITI-TF-3#4.2.3.2.26] erstellen. Für den XDS Document Service im ePA-Aktensystem wird die `DocumentEntry.UniqueID` in die Metadaten der IHE-Nachrichten eingestellt:

- `DocumentEntry.@id`
- `ExternalIdentifier.@id`

[<=]

Wenn für das Feld `SubmissonSet.AuthorPerson` keine Person als Einsteller angegeben werden kann, ist das Feld mit Werten zu befüllen, mit denen die einstellende Softwarekomponente beschrieben wird. Laut [gemSpec_Aktensystem_ePAfueralle#A_14762*] wird die Softwarekomponente eines Geräts als Nachname und ggf. als Vorname(n) eingetragen.
Beispiel: `^PHR-Gerät-XY^PHR-Software-XY`

Ein Dokument kann verborgen eingestellt werden, wenn ein entsprechender Wunsch des Versicherten bekannt ist.

A_24672 - Verbergendes Einstellen von Dokumenten
Auf Wunsch des Versicherten MUSS das PS den `confidentialityCode` eines Dokumentes auf "CON" im Code System "ePA-Vertraulichkeit" mit der OID "`1.2.276.0.76.5.491`" setzen, um ein Dokument zu verbergen.**[<=]**

Der Wert "CON" wird vom Aktensystem nicht persistiert und ausschließlich für das Verbergen von Dokumenten mittels der General Deny Policy verwendet. Ein verborgen eingestelltes Dokument ist auch für den Einstellenden nicht ohne weiteres zu lesen und nicht durch Suchoperationen auffindbar.

Dokumente, die Bestandteile einer Sammlung sind (Ordner der Ausprägung "mixed" oder "uniform") können nicht verborgen eingestellt werden.

A_26165 - Verbot des verbergendes Einstellens für Dokumente einer Sammlung
Das PS MUSS verhindern, dass Dokumente eines Ordners der Ausprägung "mixed" oder "uniform" verborgen eingestellt werden.**[<=]**

Dokumente der Kategorie "emp" sind von der Möglichkeit des verbergenden Einstellens auszuschließen, weil für diese Dokumente das Consent Decision Management, bzw. der erteilte Widerspruch gegen die widerspruchsfähige Funktion "medication" der ePA den Zugriff regelt.

A_26150 - Verbot des verbergenden Einstellens für Dokumente der Kategorie "eMP"
Das PS MUSS verhindern, dass Dokumente der Kategorie "eMP" verborgen eingestellt werden.**[<=]**

Ein PS darf DocumentEntry.confidentialityCode = "CON" nicht aus den gespeicherten Daten zum Einstellen bzw. Replace verwenden. Der aktuelle Wille des Versicherten entscheidet über das Verbergen.

A_25142-01 - Ändern verborgener Dokumente
Das PS MUSS ein Dokument, das es selbst verborgen eingestellt hat, ändern können, obwohl es verborgen ist. Dazu muss das PS die DocumentEntry.entryUUID des vom PS verborgen in die ePA eingestellen Dokumentes persistieren. Da es die DocumentEntryUUID nicht mehr mittels Find ermitteln kann, muss es die DocumentEntry.entryUUID kennen. Dies wird dadurch möglich, dass das PS gemäß [IHE-ITI-TF-2b#3.42.4.1.3.7] beim Einstellen des Dokumentes die DocumentEntry.entryUUID als valide UUID selber setzt, anstatt eine symbolische ID zu verwenden. Beim nachfolgenden Ersetzen des Dokumentes mit der Option RPLC (replace) wird diese persistierte DocumentEntry.entryUUID verwendet.**[<=]**

Die Persistierung der DocumentEntry.entryUUID im PS zeigt an, dass ein Dokument bereits eingestellt wurde und ermöglicht ein Replace eines geänderten Dokumentes, so dass ein Dokument nicht unnötig in einer Akte dupliziert wird. Eine solche standardmäßige Dublettenprüfung führt dazu, dass veralte Dokumente, die inzwischen überholt sind, als solche erkennbar sind. Sie sind mittels RPLC in den Versionsbaum einzufügen.

Versicherte können am FdV einzelne Dokumente und Dokumentenkategorien verbergen. Beide Arten des Verbergens können dazu führen, dass Dokumente, die ein Leistungserbringer erstellt hat, für ihn selbst nicht mehr sichtbar sind. Das Persistieren des selbst eingestellten Dokumentes und der dabei erzeugten DocumentEntry.entryUUID macht es überflüssig, ein Dokument erneut einzustellen, nur weil es nicht sichtbar ist. Falls der Versicherte das Dokument selbst gelöscht hat, soll der Leistungserbringer das Dokument nur auf explizite Aufforderung des Versicherten erneut einstellen. Das kann erforderlich sein, wenn der Versicherte es aus Versehen gelöscht hat.

Das PS sollte ggf. den Nutzer in einem Warnhinweis darauf aufmerksam machen, dass es nicht ohne weiteres (bzw. nicht ohne zusätzlichen Aufwand, wie in A_25142-*

beschrieben) möglich ist, das verborgen eingestellte Dokument anzuzeigen, zu ändern oder zu löschen.

A_23329-02 - Einschränkung der Änderbarkeit von Metadaten beim Hochladen eines Dokumentes unter Verwendung der RPLC-Option
Das Primärsystem DARF beim Hochladen eines Dokumentes mittels DocumentRepository_ProvideAndRegisterDocumentSet-b bei Nutzung der RPLC-Option an Metadaten des Dokumentes KEINE Veränderung vornehmen, es sei denn, das Ändern spezieller Metadaten ist gemäß [gemSpec_Aktensystem_ePAfueralle#A_24797-*] erlaubt. **[<=]**

Dokumente, die Leistungserbringer einstellen, werden unabhängig vom Inhalt des Dokumentes als LE-Dokumente (Kennzeichnung über entsprechende Auswahl aus `SubmissionSet.AuthorRole`, und dem konfigurierten `XDSDocumentEntry.healthcareFacilityTypeCode`) kategorisiert, um sie von Dokumenten zu unterscheiden, die vom Versicherten selbst (`SubmissionSet.AuthorRole="102"`) oder von Kostenträgern (`SubmissionSet.AuthorRole="105"`) eingestellt wurden. Das heißt u. a., dass die Codes für Versicherte und Kostenträger ("102" und "105") dabei explizit nicht verwendet werden dürfen.

A_15621-02 - Kategorisierung der vom LE eingestellten Dokumente
Das PS MUSS die von der LEI eingestellten Dokumente kategorisieren:

- `documentEntry.author` oder `submissionset.author` sind gemäß den Vorgaben von [gemSpec_Aktensystem_ePAfueralle#Tabelle Nutzungsvorgaben für Metadatenattribute XDS.b] zu befüllen;
- `XDSDocumentEntry.author.authorSpecialty` wird mit einem die Fachrichtung der LEI beschreibenden Wert der Selbstauskunft der LEI befüllt, es sei denn, der Autor des Dokumentes entstammt nicht der das Dokument einstellenden Institution;
- `XDSDocumentEntry.healthcareFacilityTypeCode` wird mit einem den Typ der LEI beschreibenden Wert der Selbstauskunft der LEI (A_15086-*) befüllt, es sei denn, der Autor des Dokumentes entstammt nicht der das Dokument einstellenden Institution;
- Das PS MUSS sicherstellen, dass der `XDSDocumentEntry.healthcareFacilityTypeCode` nicht mit den Werten "KTR" oder "EGA" belegt wird.

DocumentEntry und SubmissionSet enthalten übereinstimmende Werte, wenn der Autor des Dokumentes aus der das Dokument einstellenden Institution stammt. Falls eine LEI ein Dokument hochlädt, das einer Quelle außerhalb der hochladenden LEI entstammt, können diese Wert voneinander abweichen. **[<=]**

A_24967-01 - Konvertieren von PDF in PDF/A
Das PS MUSS Dokumente im PDF-Format, die in das Aktenkonto eingestellt werden sollen, automatisch in ein erlaubtes PDF/A-Format konvertieren und ausschließlich das konvertierte Dokument im PDF/A-Format in das Aktenkonto übermitteln.**[<=]**

Die im ePA-Aktensystem erlaubten Formate sind durch A_25233 definiert.

Die Unterstützung für RPLC (replace) durch das Aktensystem ermöglicht, dass Dokumente durch eine neue Version des gleichen Dokuments ersetzt werden können. Das alte Dokument wechselt in den Status (DocumentEntry.availabilityStatus) "Deprecated" und wird mit dem neuen Dokument (Status "Approved") über eine "RPLC"-Association verbunden. Der AvailabilityStatus wird beim Dokumente einstellen ausschließlich vom Aktensystem automatisiert gesetzt bzw. geändert.

A_16187 - Maximalgröße des Dokumentes

Das PS MUSS sicherstellen, dass jedes einzelne einzustellende Dokument nicht größer als 25 MB ist, und dass ein Satz der in einem einzelnen Request einzustellenden Dokumente insgesamt nicht größer als 250 MB ist.**[<=]**

3.11.2 Dokumente suchen [ITI-18]

Das Suchen nach Dokumenten erfolgt auf den Metadaten des Dokumentes, nicht auf den Inhalten des Dokumentes selbst. Die Suche kann zur Anzeige der Metadaten eines Dokumentes verwendet werden.

Die Suche erfolgt ausschließlich auf Dokumenten, die für den Leistungserbringer sichtbar sind.

Zur Suche nach Dokumenten sind u. a. folgende Filterfunktionen möglich:

- kein Filter
- Zeitintervall
- Dokumentenkategorie, darunter auch Dokumentenkategorie 1a (Suche über Ordner)
- Dokumentenquelle (z. B. eine bestimmte Facharztgruppe)
- SubmissionSet-Identifier
- Submission-Zeit.

Für die Suche über Parameter:

- $XDSDocumentEntryTitle und
- $XDSDocumentEntryAuthorInstitution
- XDSDocumentEntry.comment

ist eine Ähnlichkeitssuche möglich, wie auch beim Parameter $XDSDocumentEntryAuthorPerson. Diese Ähnlichkeitssuche beruht auf dem SQL-Suchmuster LIKE, in dem mit einer Kombination aus dem SQL-Wildcard-Zeichen "%" und dem SQL-Platzhalterzeichen "_" Suchanfragen zusammengestellt werden, in denen nach einer Kombination aus bestimmten und beliebigen Zeichen gesucht wird.

Zudem können bei Verwendung der folgenden Suchparameter auch auf diese Suchparameter bezogen unscharfe, d. h. leicht abweichende, Suchergebnisse zurückgegeben werden:

- $XDSDocumentEntryTitle
- $XDSDocumentEntryAuthorInstitution
- $XDSDocumentEntryAuthorPerson
- $XDSSubmissionSetAuthorPerson
- XDSDocumentEntry.comment.

Die Umsetzung der Suche von Dokumenten über Metadaten ist in vielfältiger Form möglich, insbesondere als

1. Suchen mittels einer Suchmaske;
2. anlassbezogene Suche ohne Suchmaske, z. B. aus dem UseCase "Benachrichtigung verwalten" heraus.

Je nachdem, ob `returnType` auf `LeafClass` oder `ObjectRef` gesetzt wird, enthält die Response der Suche eine Objektliste im Result (`LeafClass`) oder eine Liste von Objektidentifiern (`ObjectRef`), s. [ITI-18#3.18.4.1.2.6].

3.11.2.1 Umsetzung

Die Aktivitäten des Anwendungsfalles *Dokumente suchen* sind:

Vorbedingungen:

- Ausgewählte KVNR
- gültige Befugnis

Auslöser:

- Nutzerinteraktion
- anlassbezogene Suche

Aktivitäten:

- Auswahl der Suchkriterien
- Generierung und Versand der Nachricht
- (optional) Filterung der Ergebnisse
- (optional) Sortierung des Ergebnisses

Resultat:

- Ergebnismeldung
- Dokumenten-UUID-Liste (XDSDocumentEntry_uniqueId)

3.11.2.2 Nutzung

A_16336-01 - Eingrenzung von Suchergebnissen
Das PS SOLL verschiedene Strategien nutzen können, um die Menge der ePA-Dokumente einer Akte auf die für den LE relevanten Dokumente zu reduzieren:

- Die Auswahl der Metadaten-Suchstrategie (Wahl eines geeigneten `StoredQuery`)
- Je nach Wahl des Suchtyps und der Ergebnistypen `LeafClass` oder `ObjectRef` werden die Dokumente direkt oder nach einem zusätzlichen Auswahlschritt angezeigt:
  - `Leafclass`: Auswahl anhand der Metadaten-Suchergebnisse
  - `ObjectRef`: Direkte Auswahl der anzuzeigenden Dokumente ohne zusätzlich verfügbare Metadaten
- Die Suche kann in einigen `StoredQueries` bezüglich des Dokumentenstatus (`DocumentEntry.availabilityStatus`) eingeschränkt werden auf `"Deprecated"` oder `"Approved"`.

[<=]

Das Ergebnis der Suche in der Dokumenten-Registry sind Mengen eindeutiger Dokumenten-Identifier als UUID.

A_17198-02 - Nutzung des um XDSDocumentEntryTitle erweiterten Registry Stored Query FindDocuments
Das PS MUSS den in [ITI-18] nicht enthaltenen zusätzlichen Anfragetyp `FindDocumentsByTitle` mit der Query-ID "urn:uuid:ab474085-82b5-402d-8115-3f37cb1e2405" und denselben Parameternutzungsvorgaben der Registry Stored

QueryFindDocuments gemäß [IHE-ITI-TF-2b#3.38] in Verbindung mit dem zusätzlich zu [ITI-38] eingeführten Suchparameter $XDSDocumentEntryTitle nutzen können. Der zusätzliche Parameter $XDSDocumentEntryTitle ist verpflichtend und filtert die Suchergebnismenge über das Attribut XDSDocumentEntry.title . **[<=]**

A_25187 - Nutzung des um XDSDocumentEntryComment erweiterten Registry Stored Query FindDocuments
Das PS MUSS den in [ITI-18] nicht enthaltenen zusätzlichen Anfragetyp FindDocumentsByComment mit der Query-ID "urn:uuid:2609dda5-2b97-44d5-a795-3e999c24ca99" und denselben Parameternutzungsvorgaben der Registry Stored QueryFindDocuments gemäß [IHE-ITI-TF-2b#3.38] in Verbindung mit dem zusätzlich zu [ITI-38] eingeführten Suchparameter $XDSDocumentEntryComment nutzen können. Der zusätzliche Parameter $XDSDocumentEntryComment ist verpflichtend und filtert die Suchergebnismenge über das Attribut XDSDocumentEntry.comment **[<=]**

Tabelle 10: Tab_ILF_ePA_Fehlerbehandlung_Dokumente_Suchen

Fehlercode	Beschreibung	Handlungsanweisung
XDSTooManyResults	Die Ergebnismenge der Suche ist zu groß.	Die Suche verfeinern und neu durchführen bis das Aktensystem den Fehler nicht mehr wirft. Die Reduktion von Metadaten-Suchergebnissen erfolgt gemäß A_16336.

Durch die Einführung der Folder für jede Kategorie, also auch für solche der Kategorie patient, kann eine Suche mittels FindFolders auf Dokumentenkategorie erfolgen, die in Folder.Codelist angegeben sind.

A_24457-01 - Unveränderbarkeit des eindeutigen DokumentenIdentifiers in der referenceIdList
Das Aktensystem hinterlegt beim initialen Einstellen eines Dokumentes in der referenceIdList die DocumentEntry.uniqueId des initial eingestellten Dokumentes als rootDocumentUniqueId im Format: <DocumentEntry.uniqueId>^^^^urn:gematik:iti:xds:2023:rootDocumentUniqueId . Über alle Versionen des Dokumentes bleibt diese rootDocumentUniqueId erhalten. Das PS DARF die rootDocumentUniqueId NICHT durch ein RestrictedUpdateDocumentSetRequest ändern, damit mittels einem Find auf der referenceIdList ein Dokument in allen Versionen gefunden werden kann. **[<=]**

Die Metadaten der StoredQuery-Response sind geeignet, dem Nutzer weitere Filtermöglichkeiten zu geben, um die Ergebnismenge der Dokumenten-Anzeige einzuschränken.

A_15030 - Filteroptionen für den Nutzer
Das PS MUSS mittels der Metadaten aus der StoredQuery-Response Filteroptionen anbieten, mit denen Leistungserbringer die Ergebnismenge für die Anzeige von Dokumenten einschränken können.**[<=]**

3.11.3 Dokumente laden [ITI-43]

Falls das anzuzeigende Dokument nicht schon mit seiner Dokumenten-ID bekannt ist, und eine Liste vorliegt, SOLL das PS die Auswahl des anzuzeigenden Dokumentes unter Auswertung von Metadaten ermöglichen.

3.11.3.1 Umsetzung

Die Aktivitäten des Anwendungsfalles Dokumente laden sind:

Vorbedingungen:

- Auswahl KVNR
- gültige Befugnis
- `XDSDocumentEntry_uniqueId` (`DocumentEntry.uniqueId`) bekannt

Auslöser:

- Fachliches Erfordernis
- Nutzerinteraktion

Aktivitäten:

- Auswahl `XDSDocumentEntry_uniqueId`
- Generierung und Versand der Nachricht
- Dekodierung des empfangenen Dokumentes (Base64 oder XOP)
- Anzeige des angefragten Dokumentes oder der Dokumentenmenge
- Auswertung des Ergebnisses

Resultat:

- Das angefragte Dokument oder die Dokumentenmenge liegt vor und kann in das PS übernommen werden

3.11.3.2 Nutzung

Die RetrieveDocumentSet Request Message muss mindestens eine `DocumentUniqueID` enthalten.

Das PS soll die `DocumentEntry.UniqueID` gemäß [ITI-TF-3#4.2.3.2.26] nicht nur für das Laden von Dokumenten, sondern auch in der Primärakte verwenden. Eine aktenweit eindeutige `DocumentEntry.UniqueID` ermöglicht dem PS eine zuverlässige Benachrichtigungsverwaltung (s. Kap. 5.3.1 und Kap. 5.2.3).

Ein http-Request im MTOM/XOP - Format (type="application/xop+xml") führt zu einer MTOM-Response.

Im Primärsystem sollte eine Absicherung gegen mögliche Schadsoftware in heruntergeladenen Dokumenten erfolgen.

Die RetrieveDocumentSet Request Message enthält je Dokument, welches geladen werden soll, die DocumentUniqueID und die RepositoryUniqueID (Metadaten des DocumentEntry). Zu beachten ist, dass sich die Semantik von RepositoryUniqueID im Vergleich zu epa 2.x geändert hat. In epa3.x wird das Repository, in welches das Dokument ursprünglich eingestellt wurde und nicht mehr das Repository, aus dem das Dokument abgerufen wird, adressiert. Das heißt, Dokumente einer Akte eines Versicherten können in Folge von Aktenumzügen in den Metadaten unterschiedliche RepositoryUniqueID haben. Der Wert kann deshalb nicht je Versicherten persistiert, sondern muss vor dem Herunterladen ermittelt werden.

A_17769 - Schutzmaßnahmen nach Plausibilitätsprüfungen an heruntergeladenen Dokumenten
Das PS SOLL Maßnahmen zur Absicherung gegen mögliche Schadsoftware in heruntergeladenen Dokumenten ergreifen, falls:

- das Format oder der Inhalt des heruntergeladenen Dokumentes nicht mit dem angegebenen Dokumententyp in den Metadaten übereinstimmen;
- das Format oder der Inhalt des heruntergeladenen Dokumentes nicht den zulässigen Dokumententypen im Metadatum `mimeType` gemäß [gemSpec_Aktensystem_ePAfueralle#Tabelle Nutzungsvorgaben für Metadatenattribute XDS.b] entspricht.

[<=]

A_17770 - Maßnahmen zum Schutz vor heruntergeladenen Dokumenten
Das PS MUSS bei Anzeige oder persistenter Speicherung eines heruntergeladenen Dokumentes sicherstellen, dass geeignete Maßnahmen zum Schutz von PS und LE-Umgebung durchgeführt werden. **[<=]**

Geeignet wären insbesondere folgende Maßnahmen:

- Anzeigesoftware in einer Sandbox oder einem Modus betreiben, das die Umgebung der LEI vor einer potentiellen Gefährdung durch das Dokument schützt;
- vor der Anzeige eines Dokumentes Sonder-und Meta-Zeichen im Dokument für die jeweilige Anzeigesoftware mit einer geeigneten Escape-Syntax entschärfen (als Schutz z. B. gegen Injection-Angriffe aus [OWASP Top 10#A1]).
- den Nutzer darüber informieren, dass Dokumente Schadsoftware enthalten können und welche Maßnahmen der Nutzer zum Selbstschutz vornehmen kann.

Eine Beispielimplementierung eines Antiviren-Gateways findet sich im Fachportal der gematik.

A_23621-02 - Den LE informieren über fehlerhafte medizinische Dokumente
Das PS MUSS den Nutzer mit einer Fehlermeldung informieren, wenn nach dem Download aus dem Aktensystem fehlerhafte medizinische Dokumente bzw. Teildokumente einer Sammlung erkannt werden. Sofern es sich um eine fehlerhaftes Teildokument einer Sammlung handelt, MÜSSEN die korrekten Teildokumente der Sammlung trotzdem angezeigt werden, soweit dies möglich ist.
[<=]

A_15089 - Protokollierung einer Dokumentenanzeige im Übertragungsprotokoll
Das Anzeigen von Dokumenten MUSS als Übertragung eines Dokumentes aus der ePA in das PS im Übertragungsprotokoll vermerkt werden.**[<=]**

A_16198 - Prüfung der Zuordnung von Dokument zu Akte
Die `PatientId` enthält die Versicherten-ID und SOLL vom PS zur Überprüfung verwendet werden, ob das angezeigte Dokument vor einem möglichen Abspeichern dem richtigen Versicherten bzw. der richtigen lokalen Patientenakte zugeordnet ist. **[<=]**

A_16196 - Verarbeitung strukturierter Inhalte
Das PS SOLL in der Lage sein, aus ePA-Dokumenten, deren Inhalte strukturiert vorliegen, die strukturierten Inhalte in die Primärdokumentation des Versicherten zu übernehmen. **[<=]**

A_21503-01 - Daten digitaler Gesundheitsanwendungen auslesen
Das Primärsystem MUSS DiGA-Daten, deren Formatvorgabe als Medizinisches Informationsobjekt gemäß [gemSpec_IG_ePA] definiert sind, bei vorliegender Berechtigung aus dem ePA-Aktensystem des Versicherten auslesen können.**[<=]**

Wenn DiGA-Daten als PDF bereit gestellt werden, ist eine Anzeige der DiGA-Daten mittels eines PDF-Viewers möglich.

3.11.4 Dokumente löschen [ITI-62]

Der Leistungserbringer löscht Dokumente und dynamische Ordner in Absprache mit dem Versicherten.

3.11.4.1 Umsetzung

Die Aktivitäten des Anwendungsfalles Dokumente löschen sind:

Vorbedingung:

- Auswahl KVNR
- gültige Befugnis
- Absprache zwischen LE und Versicherten zur Löschung liegt vor
- Die zu löschenden Dokumente innerhalb einer Document-Request-Liste anhand ihrer `XDSDocumentEntry.entryUUID`

Auslöser:

- Nutzerinteraktion

Aktivitäten:

- Auswahl des Dokumentes bzw. der Dokumente unter Verwendung der `XDSDocumentEntry.entryUUID`
- `Sicherheitsabfrage`
- Generierung und Versand der Nachricht
- Auswertung des Ergebnisses

Resultat:

- Im Erfolgsfall sollte im PS die UUID gelöscht werden, falls sie zuvor persistent gespeichert wurde.

3.11.4.2 Nutzung

Das Löschen von Ordnern ist nur in einem eingeschränkten Umfang möglich. Das Aktensystem akzeptiert den Lösch-Request nur dann, wenn er auf einen dynamischen Folder abzielt, und wenn dieser Request nicht die im Folder enthaltenen Dokumente, SubmissionSets und Assoziationen enthält. Diese werden vielmehr vom Aktensystem selbst zusammen mit dem Folder Object gelöscht. Falls im dynamischen Ordner, der gelöscht werden soll, Dokumente vorliegen, muss daher zuvor eine Absprache mit dem Versicherten stattgefunden haben, da eine Löschung von Dokumenten immer in Absprache mit dem Versicherten stattfinden soll.

3.11.5 Aktualisieren von Metadaten [ITI-92]

Bei Dokumenten, bei denen Metadaten fehlen oder falsch sind, sollte das Primärsystem die korrekten Metadaten ändern bzw. korrigieren können. Dazu dient die Schnittstelle `updateDocumentSet`. In der Operation können sowohl eigene, als auch durch Dritte eingestellte Dokument-Metadaten bearbeitet werden, soweit es die Berechtigung des Nutzers erlaubt. Ein Herunterladen des Dokumentes, auf die sich die Metadaten beziehen, ist zum Editieren der Metadaten nicht erforderlich.

3.11.5.1 Umsetzung

Die Aktivitäten des Anwendungsfalles Aktualisieren von Metadaten sind:

Vorbedingungen:

- Auswahl KVNR
- gültige Befugnis
- Notwendigkeit, die Metadaten zu aktualisieren, liegt vor
- Die zu aktualisierenden Dokumente innerhalb einer Document-Request-Liste liegen vor anhand ihrer `XDSDocumentEntry.entryUUID`

Auslöser:

- Nutzerinteraktion

Aktivitäten:

- Auswahl des Dokumentes bzw. der Dokumente unter Verwendung der `XDSDocumentEntry.entryUUID`
- Generierung und Versand der Nachricht

Resultat:

- Im Erfolgsfall sollten auch im PS die Metadaten in der aktuellen Form gespeichert sein, falls sie zuvor persistent gespeichert wurden.

3.11.5.2 Nutzung

A_24386 - Aktualisierbare Metadaten

Das PS MUSS sich beim Anwendungsfall Aktualisieren von Metadaten des DocumentEntry mittels RestrictedUpdateDocumentSet beschränken auf das Ändern der Dokumentmetadaten

- author
- classCode
- comments
- confidentialityCode (Der UseCase "Metadaten Aktualisieren" kann jedoch nicht für das Verbergen von Dokumenten verwendet werden, sondern nur für Nutzung des Codes außerhalb der ePA)
- eventCodeList
- formatCode
- healthcareFacilityTypeCode
- languageCode
- legalAuthenticator
- practiceSettingCode
- referenceIdList
- serviceStartTime
- serviceStopTime
- title
- typeCode

- URI

[<=]

A_25166 - Keine Änderung von Metadaten von Dokumenten einer mixed- oder uniform-Sammlung
Das PS MUSS unterbinden, dass Metadaten von Dokumenten einer mixed- oder uniform-Sammlung geändert werden.**[<=]**

Das Ändern von Metadaten von Dokumenten, die ein PS selbst eingestellt hat, jedoch verborgen, ist in A_25142 beschrieben.

3.11.6 Artefakte

3.11.6.1 Namensräume

Tabelle 11: Tab_ILF_ePA_Namensräume

Präfix	Namensraum
ds	http://www.w3.org/2000/09/xmldsig
ec	http://www.w3.org/2001/10/xml-exc-c14n#
wst	http://docs.oasis-open.org/ws-sx/ws-trust/200512
wsu	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd
xsi	http://www.w3.org/2001/XMLSchema-instance
fed	http://docs.oasis-open.org/wsfed/federation/200706
wsp	http://schemas.xmlsoap.org/ws/2004/09/policy
wsa	http://www.w3.org/2005/08/addressing
xds	urn:ihe:iti:xds-b:2007
rmd	urn:ihe:iti:rmd:2017
rim	urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0
lcm	urn:oasis:names:tc:ebxml-regrep:xsd:lcm:3.0
query	urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0
soap12	http://www.w3.org/2003/05/soap-envelope

3.11.6.2 WSDLs und Schemata

Die normativen WSDLs und Schemata der ePA werden von der gematik zur Verfügung gestellt.

Für den Fall, dass es sich dabei um IHE-Artefakte handelt, gilt, dass diese Artefakte denjenigen entsprechen, die von IHE im entsprechenden Zeitraum bereitstellt.

3.11.7 Testunterstützung

Zur Unterstützung von Tests im Zusammenhang mit den oben geschilderten Funktionsmerkmalen dürfen keine Echtdaten verwendet werden.

3.12 Informationsmodell

A_21651-02 - Verarbeitung von Dokumenten der gesetzlich vorgegebenen Kategorien
Das Primärsystem MUSS Dokumente der in [gemSpec_Aktensystem_ePAfueralle#A_19303-*] aufgeführten Kategorien im Rahmen der dort aufgeführten berufsgruppenspezifischen Zugriffsregeln verarbeiten können.**[<=]**

A_14246 - Verarbeitbarkeit ausgelesener Dokumente und Formate
Das Primärsystem MUSS anhand der Metadaten eines durch *Dokumente Suchen* aufgefundenen Dokumentes erkennen, ob es in der Lage ist, diese zu verarbeiten, insbesondere anhand von `mimeType`, `formatCode`, `classCode` und `typeCode` des `DocumentEntry` in [gemSpec_IG_ePA].**[<=]**

3.12.1 Metadaten

A_24505 - Automatisiertes Setzen von Metadaten
Das PS SOLL Metadaten automatisiert aus den Primärdaten der Versicherten übernehmen und erzeugen, ohne dass eine händische Eingabe von Metadaten zwingend erforderlich ist. Die manuelle Belegung der Werte von Metadaten soll auf ein Minimum begrenzt werden. Wertebereiche (Value Sets) für ePA-Dokumente sind je nach Festlegung von [gemSpec_Voc_ePA] zu benutzen. **[<=]**

A_23556-02 - Einheitliche Metadaten-Vorgaben für unstrukturierte Dokumente ohne ImplementationGuide
Das PS MUSS für die in Tabelle *Tab_ILF_ePA_KDL-Mapping* aufgeführten Dokumententypen die dort aufgeführten Metadatenbelegungen auf Basis von [IHE-ITI-VS] anwenden, falls es für die Dokumententypen keinen IG gibt. Für Dokumententypen aus der Klinische Dokumentenklassen-Liste (KDL), für die es kein IG gibt und die nicht in *Tab_ILF_ePA_KDL-Mapping* enthalten sind, wird für die Metadatenbelegung die Verwendung der aktuellsten Version von [KDL-ILF] empfohlen. Ältere Mapping-Tabellen wie [DKG_Übermittlung_MD] dürfen verwendet werden.

Tabelle 12: Tab_ILF_ePA_KDL-Mapping

Dokumententyp	class Code	type Code	eventCodeList (KDL)	OID Code System	Anzeigename
Arztbrief (nicht IG eArztbrief)	BRI	BERI	-	-	Arztbericht /Arztbrief
Krankenhausentlassungsbericht	BRI	BERI	AD010104	1.2.276.0.76.5.552	Krankenhausentlassungsbericht
Befund/Vorbefund/ Altbefund	BEF	BEFU	-	-	Ergebnisse Diagnostik

Röntgenbefund	BEF	BILD	DG020110	1.2.276.0.76.5.552	Ergebnisse bildgebender Diagnostik (Radiologie)
Sonographiebefund	BEF	BILD	DG020111	1.2.276.0.76.5.552	Ergebnisse bildgebender Diagnostik (Sonographie)
EKG-Auswertung	BEF	FUNK	DG060111	1.2.276.0.76.5.552	Ergebnisse Funktionsdiagnostik (EKG)
Histologiebefund	BEF	PATH	PT080102	1.2.276.0.76.5.552	Pathologiebefundberichte
Lungenfunktionstest	BEF	FUNK	DG060108	1.2.276.0.76.5.552	Ergebnisse Funktionsdiagnostik (Lunge)
Bild	BIL	BILD	-	-	Ergebnisse bildgebender Diagnostik
Foto	BIL	FOTO	-	-	Fotodokumentation
OP-Bericht	DUR	OPDK	OP150103	1.2.276.0.76.5.552	OP-Dokumente (OP-Bericht)
OP-Plan/OP-Vorbereitung	DUR	OPDK	-	-	OP-Dokumente (OP-Vorbereitung)
Dialyseprotokoll	DUR	FPRO	VL040202	1.2.276.0.76.5.552	Therapiedokumentation (Dialyse)
Überweisung	VER	AUFN	AU050102	1.2.276.0.76.5.552	Überweisung (Überweisunsgschein)
Krankenhauseinweisung	VER	AUFN	AU050101	1.2.276.0.76.5.552	Verordnung von Krankenhausbehandlung
Anamnese	DUR	AUFN	-	-	Anamnese
Anamnesebogen	DUR	AUFN	AU010101	1.2.276.0.76.5.552	Anamnesebogen
Therapievorschlag/ Therapiebedarf	ANF	FPRO	-	-	Therapiedokumentation

Histologieanforderung	ANF	PATH	PT080101	1.2.276.0.76.5.552	Histologieanforderung
Kontaktdaten Angehörige	ADM	PATD	-	-	Kontaktdaten Angehörige
Neugeborenensceening	BEF	GEBU	SD070104	1.2.276.0.76.5.552	Neugeborenenscreening

[<=]

Einstellen von Dokumenten

Auf die Auszeichnung von in die ePA einzustellenden Dokumenten durch Metadaten kann das PS spezifische Einschränkungen und Vorbelegungen umsetzen:

- abhängig vom Nutzungskontext bzw. Anwendungsfall;
- gemäß sektorspezifischen Besonderheiten;
- je nach LE-spezifischen Besonderheiten und Konfigurationen, etwa in Zusammenhang mit der Selbstauskunft der Leistungserbringer.

Wenn Leistungserbringer Dokumente einstellen, bei denen sie nicht selbst der Autor sind, kann es passieren, dass die Telematik-ID des ursprünglichen Dokumenten-Autors nicht in DocumentEntry.author.authorInstitution angegeben wurde. Ein Herunterladen und eine Weiterverarbeitung solcher Dokumente soll möglich sein, auch wenn eine strenge Validierung des Metadatums aufgrund der fehlenden Telematik-ID nicht erfolgreich sein sollte.

A_15748-03 - Metadaten-Vorbelegungen bei Dokumenten, die nicht aus der eigenen LEI stammen
Für den Fall, dass LE der eigenen LE-Institution nicht die Autoren der einzustellenden Dokumente sind, KANN das PS in seinen Dialogen zur Beschreibung des Dokumenten-Autors und seiner Institution Auswahllisten von Wertebereiche der Metadaten `author`, `authorSpecialty`, `healthcareFacilityTypeCode` und `practiceSettingCode` in einer verkürzten Form zur Auswahl bringen.**[<=]**

A_16206-02 - Empfehlungen zur sektorspezifischen Reduktion von Auswahllisten
Beim Einstellen von Dokumenten SOLLEN die in Anhang B aufgeführten sektorspezifische Empfehlungen zur Reduktion von Auswahllisten mögliche Werte für die Metadaten `authorRole` und `typeCode` beim Einstellen von Dokumenten beachtet werden. **[<=]**

Auslesen von Dokumenten

Insoweit Metadaten zur Anzeige gebracht werden, muss das PS die Anzeigenamen der Metadaten in eine lesbare Form bringen. Die Anzeige von Metadaten ist insbesondere zu dem Zwecke des Filterns großer Ergebnismengen erforderlich sowie zur Auswahl der gegebenenfalls herunterzuladenden Dokumente. Zum Filtern über Dokumentenmengen kann es nützlich sein, nicht nur Metadaten der `DocumentEntries`, sondern auch Metadaten der `SubmissionSets` anzuzeigen, um ein Ausblenden bestimmter Suchergebnisse zu ermöglichen.

3.12.2 Strukturierte Dokumente

In der ePA können strukturierte Dokumente verarbeitet werden. Strukturierte Dokumente und deren Zuordnung zu Sammlung und Sammlungstypen sind in [gemSpec_IG_ePA] und in [gemSpec_Aktensystem_ePAfueralle] beschrieben.

3.12.2.1 Medizinische Informationsobjekte

Für strukturierte Dokumente gelten die Anwendungsfälle zum Laden, Suchen, Einstellen und Löschen von Dokumenten. Besteht der Bedarf nach mehreren Sammlungen des gleichen Typs in den dynamischen Ordnern `pregnancy_childbirth`, so wird jeweils ein dynamischer Ordner (je Schwangerschaft) angelegt. Beim erstmaligen Erstellen einer dynamischen Sammlung muss vom Primärsystem für diese Sammlung ein Ordner angelegt werden.

Mit der ePA für alle wird das Kinderuntersuchungsheft ausschließlich in die ePA des Kindes in den XDSFolder.codeList="child" eingestellt. Falls schon ein Kindersuchungsheft in der 2.6-Akte vorlag, wird die überholte Aktenzuordnung XDSFolder.codeList="childsrecord" nicht durch die Aktenmigration alleine korrigiert, sondern verlangt Aktivitäten des PS.

- Falls das Kinderuntersuchungsheft in der Akte eines Elternteils vorliegt, ist es von dort in die Kinderakte zu überführen;
- Falls das Kinderuntersuchungsheft schon in der Akte des Kindes vorliegt, aber in der falschen Kategorie (XDSFolder.codeList="childsrecord") ist es herunterzuladen, in der Akte zu löschen und erneut hochzuladen. Dabei wird es automatisch in die richtige Kategorie (XDSFolder.codeList="child") eingeordnet.

A_25008 - Nutzung des childrecord in der Akte des Kindes
Das PS MUSS für die Nutzung von Dokumenten der Kategorie `child` die Akte des Kindes verwenden. Ebenso müssen Zugriffe auf andere Dokumente mit medizinischen Daten von Kindern in deren ePAs durchgeführt werden.**[<=]**

3.12.2.2 NFD, DPE und eMP

Ein Notfalldatensatz (NFD) oder ein Datensatz persönliche Erklärungen (DPE), der in die ePA eingestellt werden soll, wird vom PS entweder zuvor gemäß [gemILF_PS_NFDM] von der eGK gelesen, vgl. auch [gemSpec_InfoNFDM], oder er liegt bereits im PS vor. Analog wird der elektronischen Medikationsplan (eMP) gemäß [gemILF_PS_AMTS] und [gemSpec_Info_AMTS] von der eGK gelesen, falls er nicht schon im PS vorliegt, in der ePA verarbeitet. Die Einwilligung in die Nutzung des eMP wird nicht in der ePA gespeichert.

NFD, DPE und eMP werden im Base64-Format gespeichert. Die Datensätze werden so, wie sie aus der eGK ausgelesen werden, in das Element <xds:Document> eingefügt, welches ein Attribut @id enthält das mit dem rim:ExtrinsicObject/@id übereinstimmt.

3.12.2.3 Elektronischer Arztbrief im DischargeLetterContainer-Format

Falls ein eArztbrief im Format als HL7 CDA R2-Dokument vorliegt, ohne dass der eArztbrief eine PDF-Darstellung hat, soll er direkt im Format `mimeType = application/xml` im XDS Document Service der ePA verwaltet werden. Ein eArztbrief, der als reines PDF-Dokument in die ePA eingestellt werden soll, soll direkt im Format `mimeType = application/pdf` in den XDS Document Service der ePA verwaltet werden.

Der eArztbrief DischargeLetterContainer-Format hat gemäß [Richtlinie eArztbrief] die verpflichtenden Teile PDF-Dokument und CDA-XML (nur der CDA-Header ist verpflichtend). Um diesen eArztbrief in die ePA einzustellen und wieder auszulesen, wird auf das XML-Containerformat `DischargeLetterContainer` (s. Abb_ILF_ePA_eAB-XML-Containerformat) nach [PHR_Common.xsd] zurückgegriffen.

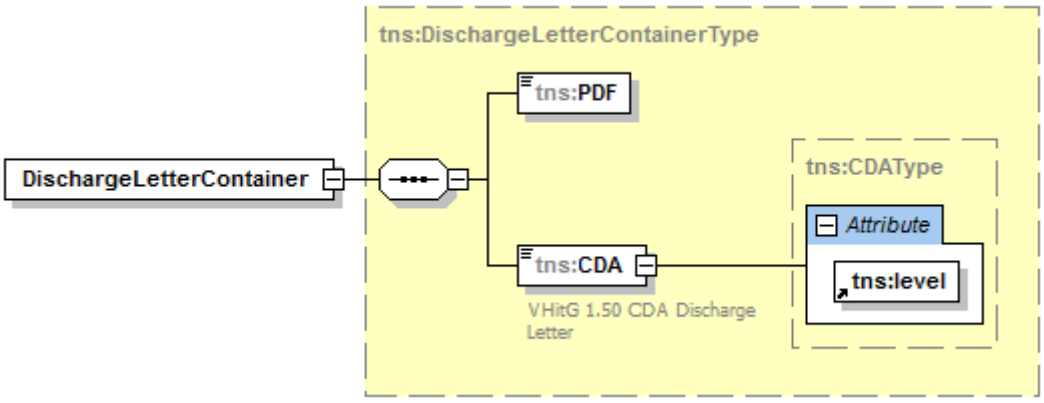

Abbildung 14: Abb_ILF_ePA_eAB-XML-Containerformat

A_14244-02 - Verarbeitungsvorschrift für eAB im DischargeLetterContainer-Format
Falls der eArztbrief im DischargeLetterContainer-Format gemäß [Richtlinie eArztbrief] in zwei Anteilen vorliegt (einem CDA-Anteil und einem PDF-Anteil), MUSS das PS beide Teile gemeinsam in eine XML-Container-Struktur nach [PHR_Common.xsd] einstellen und diese gemeinsam in einem SubmissionSet in den XDS Document Service der ePA einstellen. In diesem SubmissionSet MÜSSEN die Metadaten konform zu den Vorgaben des Implementation Guides des eArztbriefes ig-eab* in [gemSpec_IG_ePA] gesetzt werden. **[<=]**

Die folgende XML-Struktur für einen Container mit eArztbrief im DischargeLetterContainer-Format wird festgelegt:

Tabelle 13: XML-Struktur für Arztbrief im DischargeLetterContainer-Format

Element-, Attribut- oder Textknoten	Opt.	Nutzungsvorgabe
DischargeLetterContainer	R	
PDF	R	Base64-kodierter Arztbrief in PDF-Repräsentation gemäß [Richtlinie eArztbrief]
CDA	R	
@level	O	Der Wert "1", "2" oder "3" MUSS gesetzt werden, um den CDA-Level des Dokuments zu

			kennzeichnen. Der CDA-Level DARF weiterhin NICHT gesetzt werden, sofern der CDA Body gemäß [Richtlinie eArztbrief] leer ist.
	text()	R	Base64-kodierter Arztbrief in CDA-Repräsentation gemäß [VHITG_AB]

A_16246-02 - Auslesen des eArztbriefes im DischargeLetterContainer-Format
Beim Auslesen eines eArztbriefes mit `formatCode`="Code=urn:gematik:ig:Arztbrief:r3.1" MUSS das PS die zwei Anteile (den CDA-Anteil und den PDF-Anteil) aus der XML-Container-Struktur `DischargeLetterContainer` nach [PHR_Common.xsd] aus dem XDS Document Service herauslesen und als eArztbrief im DischargeLetterContainer-Format gemäß [Richtlinie eArztbrief] weiterverarbeiten und den PDF-Anteil zur Anzeige bringen können. **[<=]**

3.12.3 Selbstauskunft

A_15086-08 - Selbstauskunft der LE-Institution mit Belegung von Default-Werten
Das PS MUSS dem LE die Möglichkeit zur Hinterlegung einer Default-Konfiguration von Metadaten geben. Die Selbstauskunft der LE-Institution MUSS zur Befüllung der Metadaten in Tab_ILF_ePA_Datenfelder_Selbstauskunft automatisiert herangezogen werden können.

Tabelle 14: Tab_ILF_ePA_Datenfelder_Selbstauskunft

Vorkonfigurierbare Werte für DocumentEntry und SubmissionSet	Default-Konfiguration unter Beachtung von [gemSpec_Aktensystem_ePAfuerAlle] und [IHE-ITI-VS]
authorPerson	Person, die im Default-Fall als Autor von Dokumenten innerhalb der LEI fungiert
authorInstitution	Im Normalfall die Institution, welche die SMC-B beantragt hat
authorRole	Übliche Prozessrolle des Autors der LEI, in der das PS installiert ist
authorSpecialty	Fachrichtung des Default-Autors
authorTelecommunication	Telekommunikationsdaten der LEI, in der das PS installiert ist
healthcareFacilityTypeCode	Art der Einrichtung, in der das PS installiert ist
practiceSettingCode	Fachrichtung der Einrichtung, in der das PS installiert ist

languageCode	Sprache, in welcher üblicherweise der menschenlesbare Teil des Dokuments abgefasst ist

[<=]

Die Telematik-ID der Leistungserbringerinstitution muss in vielen Nachrichten angegeben werden. Sie sollte aus der SMC-B ausgelesen werden und im PS persistent gespeichert werden.

Die Telematik-ID ist von den Kartenherausgebern der SM-B festgelegt und immer im Attribut `registrationNumber` im Admission-Element der Extension der SMC-B-Zertifikate (`C.HCI.AUT, C.HCI.ENC,C.HCI.OSIG`) eingetragen. Wenn nicht explizit vom Antragsteller eine neue Telematik-ID angefordert wird, wird bei Ausgabe von Folge- und Ersatzkarten die bisherige Telematik-ID wiederverwendet. Eine generelle Vorgehensweise kann die gematik hierfür nicht geben, da die Personalisierung der SMC-B sektoral unterschiedlich ist (siehe [gemSpec_PKI#Anhang A]). Zum Auslesen der Zertifikate kann die Operation `ReadCardCertificate` gemäß [gemSpec_Kon#4.1.9.5.2] verwendet werden (oder aber im Falle des CS des KTR `ReadCertificate`). Die Telematik-ID ist in allen Zertifikaten in der Admissionstruktur als `registrationNumber` im ASN.1-Format gespeichert.

3.12.4 Signieren von Dokumenten

Ob eine Signatur und welche Art der Signatur (QES oder nonQES) erforderlich ist, wird durch den Anwendungsfall für das jeweilige Dokumentenformat festgelegt und außerhalb dieser Spezifikation veröffentlicht.

Im Folgenden wird das Vorgehen für den Fall, dass ein Medizinisches Informationsobjekt signiert wird, beschrieben.

Im Primärsystem liegt ein strukturiertes Dokumentenformat der ePA als FHIR-XML-Darstellung oder FHIR-JSON-Darstellung vor. Im Sinne der Signaturerstellung wird dies als Data to be Signed (DTBS) bezeichnet.

Vor dem Einstellen des Dokuments wird dieses elektronisch signiert (QES oder nonQES). Das Primärsystem nutzt dafür die Schnittstelle des Konnektors und dieser den HBA für QES bzw. SM-B für nonQES des einstellenden LE.

Bei der Signaturerstellung ist folgender Ablauf im Primärsystem erforderlich:

1. Das Primärsystem stellt fachliche DTBS zusammen.
2. Das Primärsystem serialisiert die Daten zu einer Data to be Signed Representation (DTBSR).
3. Das Primärsystem übermittelt DTBSR an den Konnektor zur Signaturerstellung (Aufruf der Operation `SignDocument` gemäß [gemILF_PS]).
4. Der Konnektor erzeugt eine `CADES Enveloping Signatur`.
5. Das signierte Objekt enthält sowohl die Signatur als auch die ursprünglichen DTBSR bitgenau und in einem binären ASN.1 Format (PKCS#7).
6. Der Konnektor übermittelt das signierte Objekt an das Primärsystem.
7. Das Primärsystem stellt über das Funktionsmerkmal "Dokumente einstellen" das signierte Objekt als`DocumentEntry` im ePA-Aktensystem im PKCS#7-Format ein.

A_19742 - strukturiertes Dokument - QES signieren
Falls eine QES-Signatur für ein strukturiertes Dokument gefordert wird, MUSS das PS vor dem Einstellen eines strukturierten Dokumentes in die Akte des Versicherten eine QES-

Signatur als `CADES Enveloping Signatur` für das strukturierte Dokument durch Aufruf der Operation `SignDocument` erstellen.**[<=]**

A_19957 - strukturiertes Dokument - nonQES signieren
Falls eine nonQES-Signatur für ein strukturiertes Dokument gefordert wird, MUSS das PS vor dem Einstellen eines strukturierten Dokumentes in die Akte des Versicherten eine nonQES Signatur als `CADES Enveloping Signatur` für das strukturierte Dokument durch Aufruf der Operation `SignDocument` erstellen.**[<=]**

Bei der Signaturprüfung ist folgender Ablauf im Primärsystem erforderlich:

1. Das Primärsystem lädt Dokument aus dem ePA-Aktensystem.
2. Das Primärsystem erkennt, dass es sich dabei um ein medizinisches Objekt im Format im PKCS#7 handelt (`DocumentEntry. mimetype = application/pkcs7-mime`).
3. Das Primärsystem übermittelt das signierte Objekt an den Konnektor zur Signaturprüfung (Aufruf der Operation VerifyDocument [gemILF_PS]).
4. Der Konnektor prüft die Signatur.
5. Der Konnektor übermittelt das Prüfergebnis an das Primärsystem.
6. Bei erfolgreicher Signaturprüfung verarbeitet das Primärsystem die fachlichen Daten entsprechend dem `formatCode` weiter. Hierzu parst das Primärsystem die binäre ASN.1-Struktur der Daten im PKCS#7-Format und trennt die Fachdaten von den restlichen Daten ab.

A_19743 - strukturiertes Dokument - QES-Signatur prüfen
Falls eine QES-Signatur für ein strukturiertes Dokument gefordert wird MUSS das PS nach dem Laden eines strukturierten Dokumentes aus der Akte des Versicherten die QES des Dokumentes durch Aufruf der Operation `VerifyDocument` prüfen und das Prüfergebnis zur Anzeige bringen.**[<=]**

A_19958 - strukturiertes Dokument - nonQES Signatur prüfen
Falls eine nonQES-Signatur für ein strukturiertes Dokument gefordert wird, MUSS das PS nach dem Laden eines strukturierten Dokumentes aus der Akte des Versicherten die nonQES des Dokumentes durch Aufruf der Operation `VerifyDocument` prüfen und das Prüfergebnis zur Anzeige bringen.**[<=]**

4 Spezielle Nutzungsumgebungen

Nutzerumgebungen werden grundlegend durch [gemSpec_Aktensystem_ePAfueralle#A_19303-*] in ihren Zugriffsrechten auf Dokumente des Versicherten in der ePA für alle eingeschränkt.

4.1 Funktionsumfang Clientsystem des Kostenträgers

Der Kostenträger stellt für Versicherte Dokumente in ihr Aktenkonto ein. Das können sein:

- Abrechnungsdaten,
- digitalisierte Papierdokumente von Versicherten ohne FdV.

Somit muss das Clientsystem des Kostenträgers das Einstellen von Dokumente des XDS Document Service umsetzen.

Des Weiteren übernimmt das Clientsystem des Kostenträgers Aufgaben im Rahmen eines betreiberübergreifenden Aktenumzugs. Damit unterscheidet sich der Funktionsumfang des Clientsystems des Kostenträgers wesentlich vom Funktionsumfang des Primärsystems einer Leistungserbringerinstitution. Der Kostenträger wird dabei durch die SMC-B des Kostenträgers repräsentiert. Der Kostenträger ist grundsätzlich befugt, schreibend auf die Akten der Versicherten zuzugreifen, das individuelle Befugen durch Lesen der Versichertenkarte entfällt. Ein lesender Zugriff ist nicht möglich.

Im Folgenden wird der spezifische Funktionsumfang beschrieben und die Anforderungen genannt, die sich nur auf das Primärsystem des Kostenträgers beziehen.

4.1.1 Einstellen von Daten durch Kostenträger

A_19394-04 - Kennzeichnung eines Dokumentes als Kostenträgerinformation
Das Clientsystem des Kostenträgers MUSS zur Kennzeichnung der Dokumente, die für die ePA des Versicherten eingestellt werden, die in Tab_ILF_ePA_KTR_Metadatenkennzeichnungen für den Dokumententyp aufgeführten Metadaten für DocumentEntry setzen.

Tabelle 15: Tab_ILF_ePA_KTR_Metadatenkennzeichnungen

Dokumententyp	Metadaten
Dokumente der bei den Krankenkassen gespeicherten Daten über die in Anspruch genommenen Leistungen der Versicherten	DocumentEntry.healthcareFacilityTypeCode=VER und DocumentEntry.typeCode=ABRE DocumentEntry.authorRole=105 Submissionset.authorRole = 105
Eingescannte Dokumente	Submissionset.authorRole = 105

[<=]

Aufgrund der Einordnungsregeln in A_19388-* werden eingescannte Dokumente der Kategorie bzw. dem Ordner `patient`(Versichertendokumente) zugeordnet.

A_26275 - Nutzung der Schnittstelle des FHIR IG Patient Information Service
Das Clientsystem des Kostenträgers MUSS die Schnittstellen des FHIR Implementation Guide für den Patient Information Service [IG_Patient_Information_Service] bedienen.
[<=]

4.1.2 Ablauf eines betreiberübergreifenden Aktenumzugs (informativ)

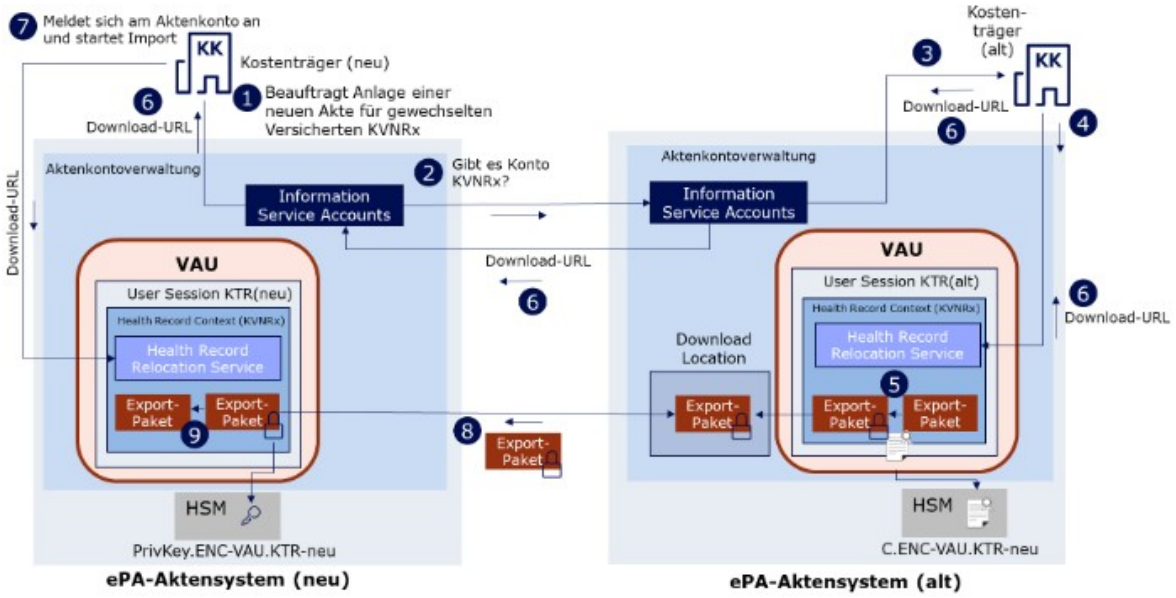

Abbildung 15: Ablauf eines betreiberübergreifenden Aktenumzugs

Anstoßen eines Aktentransfers
Der Kostenträger (neu) lässt im Aktensystem eine neue Akte anlegen (1). Das Aktensystem fragt am **Information Service** der anderen Aktensysteme ab, ob für diese KVNR schon eine Akte existiert (2). Sollte dies der Fall sein, wird der Anbieterwechsel angestossen.

Dafür informiert der **Information Service** des alten Aktensystems den Kostenträger (alt) über den Wechsel (3). Der Kostenträger (alt) meldet sich an der ePA an, startet die Erstellung eines Export-Pakets im **Health Record Relocation Service** (4). Der Service ändert den Status der Akte auf SUSPENDED und baut das Export-Paket. Das Export-Paket wird mit dem Verschlüsselungszertifikat für die VAU des neuen Betreibers verschlüsselt (5).

Das verschlüsselte Export-Paket wird nun auf dem Download-Punkt des alten Aktensystems abgelegt und die entsprechende Download-URL dem Kostenträger (alt) bekannt gemacht. Dieser übermittelt die Download-URL an den **Information Service** seines Aktensystems, welches diese an den **Information Service** des neuen Aktensystems übergibt. Dieses leitet die URL mit der Information, dass ein Anbieterwechsel ansteht, an den Kostenträger (neu) weiter (6).

Import einer Akte
Der Kostenträger (neu) meldet sich an der ePA an und startet am **Health Record Relocation Service** den Import der Akte (7). Nachdem der **Health Record Relocation Service** das Export-Paket abgerufen (8) und entschlüsselt hat, werden die Daten in die entsprechenden Services importiert und die Akte ist beim neuen Anbieter nutzbar und deren Status wechselt auf ACTIVATED (9).

4.1.3 Erstellung des Exportpakets auf Seiten des alten Kostenträgers

Der **Information Service** des Aktensystems informiert das Clientsystem des Kostenträgers über den anstehenden Aktenumzug und gibt dabei die KVNR des umzuziehenden Aktenkontos und eine RequestID mit. Das Format dieser Information wird nicht von der gematik vorgegeben und ist betreiberspezifisch. Die RequestID wird durch das alte Aktensystem bei der Anlage eines Exportpakets erzeugt und identifiziert die Abfolge der Aufrufe und Antworten im Rahmen eines Aktenumzugs als zusammengehörig.

Getriggert durch diese Information loggt sich das Clientsystem des Kostenträges in das Aktenkonto ein und startet die Herstellung des Exportspakets unter Verwendung des Verschlüsselungszertifikats.

Dazu nutzt es diese Operation des **Health Record Relocation Service** des Aktensystems:

Tabelle 16: I_Health_Record_Relocation_Service::startPackageCreation

REST-Schnittstelle des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)	
I_Health_Record_Relocation_Service	
`startPackageCreation`	Diese Operation startet die Anlage eines Exportpakets der Inhalte eines Aktenkontos zum Download.

A_24683 - Anlage eines Exportpakets
Das Clientsystem des Kostenträgers MUSS die Anlage eines Exportpakets der Inhalte eines Aktenkontos zum Download starten unter Verwendung der Operation *startPackageCreation* gemäß [I_Health_Record_Relocation_Service].**[<=]**

Die startPackageCreation-Response enthält die Download-URL des Export-Pakets. Diese Download-URL muss das Clientsystem an den Information Service des Aktensystems senden. Das Format dieser Nachricht wird nicht von der gematik vorgegeben und ist betreiberspezifisch.

4.1.4 Einspielen des Exportpakets auf Seiten des neuen Kostenträgers

Der **Information Service** des neuen Aktensystems informiert das Clientystem des neuen Kostenträgers, dass der Import des Exportpakets beginnen kann und gibt dabei die Download-URL mit. Das Format dieser Information wird nicht von der gematik vorgegeben und ist betreiberspezifisch.

Getriggert durch diese Information loggt sich das Clientsystem des Kostenträges in das Aktenkonto ein und startet den Import des Exportpakets.

Dazu nutzt es diese Operation des **Health Record Relocation Service** des Aktensystems:

Tabelle 17: I_Health_Record_Relocation_Service::startPackageImport

REST-Schnittstelle des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)	
I_Health_Record_Relocation_Service	
`startPackageImport`	Diese Operation startet den Import des Exportpakets der Inhalte in das neue Aktensystem.

A_24692 - Import des Exportpakets
Das Clientsystem des Kostenträgers MUSS den Import eines Exportpakets starten unter Verwendung der Operation *startPackageImport* gemäß [I_Health_Record_Relocation_Service].**[<=]**

4.1.5 Verhalten bei Scheitern des Imports

Falls der Import des Exportpakets im neuen Aktensystem scheitert, erhält das Clientsystem des alten Kostenträgers diese Information vom **Information Service** des alten Aktensystems.

Das Clientsystem muss daraufhin den **Health Record Relocation Service** auffordern, den Status des Aktenkontos von SUSPENDED zurück auf ACTIVATED zu setzen.

Das Format dieser Aktionen wird nicht von der gematik vorgegeben und ist betreiberspezifisch.

4.1.6 Verwaltung von E-Mail-Adressen

Ein Kostenträger kann die E-Mail-Adressen der Versicherten, die bei diesem Kostenträger versichert sind, bei Bedarf anpassen. Im ePA-Aktensystem wird die Verwaltung der E-Mail-Adressen im Email Management Service realisiert. Ist nur eine E-Mail-Adresse für den Nutzer hinterlegt, kann diese nicht gelöscht werden. Das Ändern einer E-Mail-Adresse wird realisiert durch das Einstellen einer neuen und Löschen der alten E-Mail-Adresse. Der Kostenträger stellt sicher, dass eine neu hinterlegte E-Mail-Adresse zuvor validiert wurde.

Folgende Anwendungsfälle werden ermöglicht:

- alle für den beim Kostenträger Versicherten hinterlegten E-Mail-Adressen abrufen
- neue E-Mail-Adresse für den beim Kostenträger Versicherten hinterlegen
- E-Mail-Adresse für den beim Kostenträger Versicherten löschen

A_25446 - Verwaltung von email-Adressen
Das Clientsystem des Kostenträgers MUSS für die Verwaltung der E-Mail-Adressen der Versicherten, die bei diesem Kostenträger versichert sind, die Operationen getEmails, setEmail, deleteEmail der Schnittstelle `I_Email_Management` gemäß [I_Email_Management] verwenden.**[<=]**

4.2 Funktionsumfang Clientsystem der Ombudsstelle

Die vom Kostenträger eingerichtete Ombudsstelle ermöglicht es Versicherten, die über kein FdV verfügen, sonst nur über das FdV nutzbare Funktionalitäten ihres Aktenkontos zu nutzen. Das sind:

- für spezifische LEI das Erstellen einer Befugnis ausschließen und dieses wieder rückgängig machen,
- im Rahmen des Medikationsprozesses:
  - Widerspruch einlegen gegen die Teilnahme am digitalen Medikationsprozess (medication) und die Rücknahme dieses Widerspruchs,
  - Widerspruch einlegen gegen das Einstellen der Medikationsdaten durch den E-Rezept-Fachdienst und die Rücknahme dieses Widerspruchs,
- Protokolldaten aus dem Aktenkonto herunterladen.

Diese Funktionen werden aus dem Clientsystem der Ombudsstelle heraus getriggert, dessen Funktionsumfang sich damit wesentlich vom Funktionsumfang des Primärsystems einer Leistungserbringerinstitution unterscheidet. Die Ombudsstelle wird dabei duch die SMC-B der Ombudsstelle repräsentiert. Die Ombudsstelle ist grundsätzlich befugt, auf die Akten der Versicherten zuzugreifen, das individuelle Befugen durch Lesen der Versichertenkarte entfällt.

Im Folgenden wird der spezifische Funktionsumfang beschrieben und die Anforderungen genannt, die sich nur auf das Clientsystem der Ombudsstelle beziehen.

Zum Funktionsumfang des Clientsystems der Ombudsstelle gehört die Verarbeitung von Dokumenten nicht. Somit muss der XDS Document Service nicht umgesetzt werden.

4.2.1 Spezifische LEI für die Nutzung eines Aktenkontos sperren

Um für einen Versicherten eine bestimmte LEI für den Zugriff auf das Aktenkonto zu sperren, muss das Clientsystem der Ombudsstelle zunächst die Telematik-ID, den Displaynamen und die ProfessionID der zu sperrenden LEI ermitteln. Dazu sind die Suchmöglichkeiten des VZD-FHIR-Directory der TI zu nutzen.

Zur Authentisierung am VZD-FHIR-Directory nutzt ein Clientsystem der Ombudstelle ein search-access_token, welches das Clientsystem der Ombudstelle am ePA-Aktensystem anfragt. Dies erfolgt durch Aufruf der Operation getFHIRVZDtoken gemäß [I_Authorization_Service.yaml].

Informationen zu Leistungserbringerinstitutionen sind im Verzeichnisdienst FHIR-Directory (VZD-FHIR-Directory) der TI-Plattform hinterlegt. Der Nutzer kann mit verschiedenen Kriterien nach Leistungserbringerinstitutionen im VZD-FHIR-Directory suchen und Informationen abrufen. Das Informationsmodell des Verzeichnisdienstes ist in [gemSpec_VZD_FHIR_Directory#4.1.1 Datenmodell] beschrieben.

Die Suche nach LEI erfolgt primär über den Namen oder Institutionsnamen, aber auch über zusätzliche Informationen wie Adressen, Fachgebiet oder Institutionstyp.

Für die Umsetzung der Suche siehe [gemSpec_ePA_FdV#6.2.3.2].

A_24668 - Suche nach LEI im Verzeichnisdienst durch Ombudsstelle
Das Clientsystem der Ombudsstelle MUSS es dem Nutzer ermöglichen, eine oder mehrere LEI im VZD-FHIR-Directory zu suchen und für die weitere Verarbeitung auszuwählen.**[<=]**

Für die Sperrung nutzt das Clientsystem der Ombudsstelle folgende Operation:

Tabelle 18: I_Entitlement_Management::setBlockedUserPolicyAssignment

REST-Schnittstelle des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)	
I_Entitlement_Management	
`setBlockedUserPolicyAssignment`	Diese Operation erstellt den Befugnisausschluss für eine LEI (Telematik-ID).

A_24657 - Sperren einer spezifischen LEI durch Ombudsstelle
Das Clientsystem der Ombudsstelle MUSS es dem Nutzer ermöglichen, einen Widerspruch gegen die Nutzung der ePA durch eine spezifische LEI zu erteilen unter Verwendung der Operation *setBlockedUserPolicyAssignment* gemäß [I_Entitlement_Management].**[<=]**

Um eine Sperrung aufzuheben, benutzt das Clientsystem der Ombudsstelle folgende Operation:

Tabelle 19: I_Entitlement_Management::deleteBlockedUserPolicyAssignment

REST-Schnittstelle des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)	
I_Entitlement_Management	
`deleteBlockedUserPolicyAssignment`	Diese Operation hebt einen Befugnisausschluß einer LEI (Telematik-ID) auf.

A_24666 - Löschen einer Sperrung einer spezifische LEI durch Ombudsstelle
Das Clientsystem der Ombudsstelle MUSS es dem Nutzer ermöglichen, einen Widerspruch gegen die Nutzung der ePA durch eine spezifische LEI zurückzunehmen unter Verwendung der Operation *deleteBlockedUserPolicyAssignment* gemäß [I_Entitlement_Management].**[<=]**

Um alle gesperrten LEI zu ermitteln, nutzt das Clientsystem folgende Operation:

Tabelle 20: I_Entitlement_Management::getBlockedUserPolicyAssignment

REST-Schnittstelle des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)	
I_Entitlement_Management	
`getBlockedUserPolicyAssignment`	Diese Operation ruft die aktuell vorhandenen Befugnisausschlüsse ab.

A_24931 - Einsehbarkeit von Befugnisausschlüssen
Das Clientsystem der Ombudsstelle MUSS es dem Nutzer ermöglichen, alle aktuell vorhandenen Befugnisausschlüsse abzurufen unter Verwendung der Operation *getBlockedUserPolicyAssignment* gemäß [I_Entitlement_Management].**[<=]**

4.2.2 Widersprüche zum Medikationsprozess einstellen oder widerrufen

Das Clientsystem der Ombudsstelle nutzt das **Consent Decision Management** des Aktensystems, um für einen Versicherten Einsprüche gegen im Rahmen des Medikationsprozesses einzustellen oder diese zu widerrufen.

Es gibt zwei verschiedene Widersprüche:

Tabelle 21: Widersprüche im Rahmen des Medikationsprozesses

Art des Widerspruchs	Folgen des Widerspruchs	Rücknahme des Widerspruchs
Medication	Das Lesen und Schreiben in Medical Services "emp" (XDS) und Medical Services "medication" (fhir) wird für alle LEI und FdV unterbunden. Daten der ePA werden nicht gelöscht.	Kann nur zusammen mit dem Erp-submission-Widerspruch zurückgenommen werden.
Erp-submission	Die Daten in Medical Services "emp" (XDS) und Medical Services "medication" (fhir) werden gelöscht. Das Einstellen von Verordnungen und Dispensierdaten durch den Fachdienst wird abgelehnt. Der Medication-Widerspruch wird automatisch (durch das AS) mit gesetzt.	Rücknahme muss explizit erfolgen. Der Medication-Widerspruch bleibt erhalten.

Es wird folgende Operation genutzt:

Tabelle 22: I_Consent_Decision_Management::updateConsentDecision

REST-Schnittstelle des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)	
I_Consent_Decision_Management	
`updateConsentDecision`	Diese Operation setzt für den digitalen Medikationsprozess (functionid "medication") und für die Einstellung von Medikationsdaten durch den Fachdienst (functionid "erp-submission") eine Zustimmung ("permit") oder eine Ablehnung ("deny").

A_24659 - Entscheidung zum Medikationsprozess setzen durch Ombudsstelle
Das Clientsystem der Ombudsstelle MUSS es dem Nutzer ermöglichen, Widersprüche im Rahmen des Medikationsprozesses zu erteilen bzw. zurückzunehmen unter Verwendung der Operation `updateConsentDecision` gemäß [I_Consent_Decision_Management].**[<=]**

Um den Zustand eines Widerspruchs festzustellen, benutzt das Clientsystem folgende Operation:

Tabelle 23: I_Consent_Decision_Management::getConsentDecision

REST-Schnittstelle des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)	
I_Consent_Decision_Management	
`getConsentDecision`	Diese Operation liest den aktuellen Zustand des Widerspruchs gegen die Nutzung von widerspruchsfähigen Funktionen aus.

A_24927 - Entscheidungen zu widerspruchsfähigen Funktionen abfragen
Das Clientsystem der Ombudsstelle MUSS es dem Nutzer ermöglichen, den aktuellen Zustand des Widerspruchs gegen die Nutzung von widerspruchsfähigen Funktionen

abzufragen unter Verwendung der Operation `getConsentDecision` gemäß [I_Consent_Decision_Management].**[<=]**

4.2.3 Protokolldaten dem Versicherten zur Verfügung stellen

Versicherte ohne ePA-FdV können bei ihrer zuständigen Ombudsstelle beantragen, die Protokolldaten zur Verfügung gestellt zu bekommen. Für den Abruf der Protokolldaten aus dem Aktenkonto des Versicherten nutzt das Clientsystem der Ombudsstelle die Schnittstelle **Audit Event Service** des Aktensystems. Bei den Audit Events handelt es sich um eine FHIR-Ressource gemäß der FHIR-Profilierung [gemSpec_EPAAuditEvent].

Die Anfrage des Client-Systems enthält eine FHIR-Suche, bei der über verschiedene Suchparameter das Suchergebnis eingeschränkt wird. Die Response enthält ein Bundle mit den Suchergebnissen der passenden Audit Events. Alternativ können die Protokolldaten in gerenderter Form als PDF/A Dokument abgerufen werden.

Es werden folgende Operationen genutzt:

Tabelle 24: I_Audit_Event_Service

REST-Schnittstelle des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)	
I_Audit_Event	
`GET/audit/v1/fhir/AuditEvent`	Mit dieser Operation kann die Ombudsstelle über eine FHIR-basierte Abfrage unter Nutzung der entsprechenden Suchparameter die Protokolldaten eines Aktenkontos abrufen.
I_Audit_Event_Render	
GET//audit/render/v1/pdf (renderAuditEventsToPDF)	Mit dieser Operation kann die Ombudsstelle die Protokolldaten eines Aktenkontos als PDF/A Dokument abrufen.

A_24660 - Abruf der Protokolldaten durch Ombudsstelle
Das Clientsystem der Ombudsstelle MUSS es dem Nutzer ermöglichen, Protokolldaten aus einem Aktenkonto herunterzuladen gemäß [I_Audit_Event].**[<=]**

A_25350 - Abruf der Protokolldaten im Format PDF/A durch Ombudsstelle
Das Clientsystem der Ombudsstelle KANN es dem Nutzer alternativ auch ermöglichen, gerenderte Protokolldaten aus einem Aktenkonto herunterzuladen gemäß [I_Audit_Event_Render].**[<=]**

A_24711-01 - Aufbereitung der Protokolldaten für den Versicherten
Das Clientsystem der Ombudsstelle MUSS die Protokolldaten in für den Versicherten lesbarer Form bereitstellen.**[<=]**

4.3 Funktionsumfang Clientsystem DiGA

Das Clientsystem eines DiGA-Herstellers kann DiGA-Daten in die ePA einstellen und aktualisieren. Jede mit einer individuellen Telematik-ID ausgestatteten DiGA legt dazu einen DiGA-individuellen dynamischen Ordner an. Die Telematik-ID im Folder-Title

identifiziert die DiGA, deren Daten in einem MIO im Folder des Versicherten abgelegt sind.

4.3.1 Einstellen von DiGA-Daten

A_23131-01 - DiGA-CS: Persistierung der DocumentEntry.entryUUID
Das DiGA-CS MUSS die DocumentEntry.entryUUID des von ihm in die ePA eingestellen Dokumentes persistieren, falls er die Möglichkeit nutzen möchte, für dieses Dokument Updates durchzuführen. Hierzu ist es gemäß [IHE-ITI-TF-2b#3.42.4.1.3.7] erforderlich, dass ein DiGA-Client beim Einstellen des Dokumentes die DocumentEntry.entryUUID als valide UUID setzt und keine symbolische ID verwendet. Beim nachfolgenden Einstellen von Dokumenten mit der Option RPLC (replace) MUSS die persistierte DocumentEntry.entryUUID verwendet werden.**[<=]**

5 Ergänzende Funktionalitäten

5.1 Betriebs- und Performancedaten

Das PS versendet Messdaten zur Userexperience (UX-Messdaten) der in Tab_UX_KPI_Messung_ePA_PS aufgeführten erfolgreich abgeschlossenen Anwendungsfälle an das Aktensystem, bei dem ein Aktenzugriff erfolgte.

Tabelle 25: I_Information_Service::setUserExperienceResult

REST-Schnittstelle des Aktensystems (Nutzung ohne VAU-Kanal)	
I_Information_Service	
	Diese Operation versendet Messdaten von Verarbeitungszeiten.

A_24685 - Messung von Verarbeitungszeiten
Das PS MUSS bei Durchführung der Anwendungsfälle aus Tab_UX_KPI_Messung_ePA_PS die in der Spalte "Beschreibung" beschriebene Messung von Verarbeitungszeiten durchführen und das Ergebnis in Millisekunden speichern.

Tabelle 26: Tab_UX_KPI_Messung_ePA_PS

UX-Anwendungsfälle	Beschreibung
UX_Login_PS	Es wird der Zeitraum gemessen, den ein Nutzer eines Primärsystems nach der Auswahl einer ePA warten muss, bis die angeforderte Akte geöffnet ist. Dabei beginnt die Messung mit der letzten Nutzer-Interaktion (z. B. Anklicken eines Feldes "Patient A12345680") bevor die Akte geöffnet wird und endet mit der Anzeige von Inhalten der Akte (z. B. Dokumentenübersicht oder einer Fehlermeldung bei fehlender Befugnis).
UX_Doc_Upload_PS	Es wird der Zeitraum gemessen, den ein Nutzer eines Primärsystems nach dem Befehl zum Hochladen eines Dokumentes warten muss, bis dieses Dokument im PS angezeigt wird oder die Information über den Erfolg der Operation erfolgt.
UX_Doc_Download_PS	Es wird der Zeitraum gemessen, den ein Nutzer eines Primärsystems nach dem Befehl zum Herunterladen eines Dokumentes warten muss, bis dieses Dokument vollständig heruntergeladen wurde.

[<=]

A_24686 - Übertragung von Verarbeitungszeiten

Das PS MUSS unmittelbar nach erfolgreicher Durchführung der Messung von Verarbeitungszeiten der Anwendungsfälle aus [gemILF_PS_ePA::Tab_UX_KPI_Messung_ePA_PS] das Messergebnis ohne Nutzerinteraktion im Hintergrund an das gleiche Aktensystem (unter Verwendung der Schnittstelle `InformationService.setUserExperienceResult`) übermitteln, bei dem der Aktenzugriff erfolgte. Im Anschluss MÜSSEN die gespeicherten Werte gelöscht werden, sofern die Übermittlung erfolgreich war.**[<=]**

Hinweis: "Im Hintergrund" bedeutet, dass die Übermittlung einerseits automatisch (ohne Nutzerinteraktion) geschieht und andererseits für den Nutzer auch keine "Wartezeit" entsteht.

5.2 Übertragungsprotokolle speichern

Das PS benutzt "Übertragungsprotokolle", um insbesondere die vorgeschriebenen Nachweispflichten von Leistungserbringern bei der Übertragung von Dokumenten zwischen PS und Aktensystem zu erfüllen, bei denen Patientendaten betroffen sind. Das Erstellen, Speichern, durchsuchbar Machen und Anzeigen der Übertragungsprotokolle zwischen PS und Aktensystem ist eine Aufgabe des PS, die nicht durch Komponenten der TI abgedeckt wird. Die Übertragungsprotokolle geben Auskunft über die Aktivität des PS bei der Nutzung der Akte, nicht aber über die Datenverarbeitung im Aktensystem des Versicherten.

A_16434 - Übertragungsprotokolle durchsuchbar und einsehbar speichern
Das PS MUSS Übertragungsprotokolle der Kommunikation mit dem ePA-Aktensystem speichern, durchsuchbar und einsehbar machen.**[<=]**

Das Format der Speicherung und die Schnittstellen zu den Übertragungsprotokollen können herstellerspezifisch sein. Das PS kann zum Speichern Record Audit Event [ITI-20] verwenden, und darauf aufbauende Filtermechanismen zur Anzeige der Übertragungsprotokolle verwenden.

Durch das Loggen der SOAP-Parameter aus Tab_ILF_ePA_ClientInformationen bei Dokumentenmanagementzugriffen werden für das Einsehen von Übertragungsprotokollen erforderliche Zugriffsinformationen bereit gestellt.

Details zur Nutzung der Übertragungsprotokolle obliegen dem PS.

5.3 Empfehlung zur Archivierung

Auf der Grundlage gesetzlicher Regelungen besteht eine Archivierungspflicht für die medizinischen Dokumente und für die Übertragungsprotokolle des Versicherten. Die Archivierung ist korrekt, verständlich, vollständig, nachvollziehbar und zeitnah durchzuführen. Je nach gesetzlicher Regelung sind damit dokumentierte Inhalte mit Aufbewahrungszeiträumen verbunden.

Zur Aufbewahrungsfrist wird auf die jeweils aktuelle Fassung der „Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“ der BÄK und KBV, siehe [BÄK_KBV], und auf die einschlägigen gesetzlichen Normen verwiesen.
Im Umfang der Archivierung sollen zusätzlich zu den aus der ePA heruntergeladenen und persistent im PS gespeicherten ePA-Dokumenten des Versicherten auch die zu diesen Dokumenten gehörigen Metadaten enthalten sein, die in [gemSpec_Aktensystem_ePAfuerAlle#Tabelle Nutzungsvorgaben für Metadatenattribute XDS.b] aufgelistet sind, soweit sie für den Verarbeitungskontext relevant sind.

6 UX Best practice für Primärsysteme

Dieses Kapitel gibt einen Einblick in die Möglichkeit, die ePA in Versorgungsprozesse nutzerfreundlich und möglichst aufwandsarm einzubinden. Ein Anspruch auf Vollständigkeit bei der Abdeckung möglicher Anwendungsfälle und Versorgungsprozesse besteht nicht.

6.1 Standardeinstellungen und Konfigurationsmöglichkeiten des Systems

Die Abbildungen und Beschreibungen in diesem Kapitel beschreiben Standardeinstellungen und stellen Varianten dar, wie die Anforderungen zur Bedienung der ePA umgesetzt werden können. Die hier beschriebenen Inhalte sind als Interpretationshilfe zu verstehen. Der Lösungsraum geht hierüber hinaus. Das Nähere zum Anforderungskatalog regeln die Leistungserbringerinstitution und der Primärsystemhersteller miteinander, bspw. in Form von Richtlinien in einem Krankenhaus.

6.1.1 Befugniserzeugung aus der Leistungserbringerumgebung

Das Primärsystem stellt eine User Session für die Leistungserbringerinstitution zum ePA-Aktensystem her. Innerhalb der User Session kann der Endanwender jederzeit im Laufe des Tages bei Bedarf auf jedes ePA-Aktenkonto zugreifen, für das er befugt ist. Um eine User Session aufzubauen, muss zunächst eine Verbindung zum VAU-Kanal aufgebaut werden und dann eine Nutzerauthentifizierung am IDP-Dienst erfolgen. Die User Session ermöglicht den Zugriff alle Aktenkonten des Aktensystems, in denen eine Befugnis für die LEI hinterlegt ist. (siehe Abbildung 15).

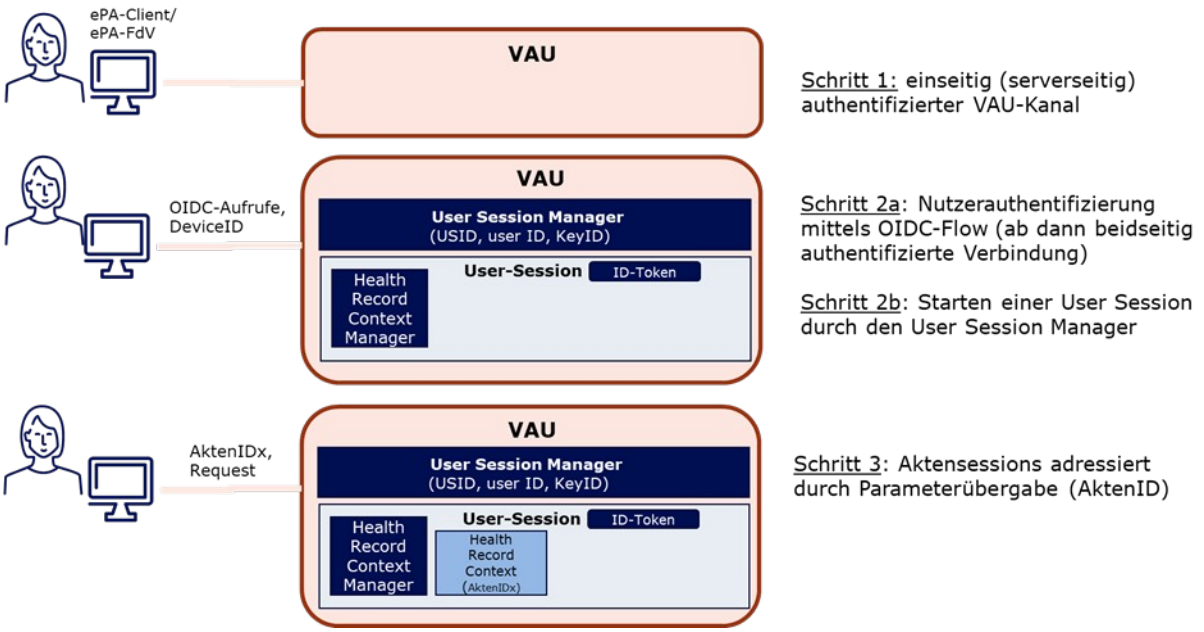

Abbildung 16: Voraussetzung für eine Befugniserzeugung

In allen Sektoren setzt die Benutzung der ePA voraus, dass ein technisch nachgewiesener Behandlungskontext vorliegt und eine Berechtigung erzeugt wird. Dies geschieht, indem die eGK eingelesen, eine Prüfziffer vom VSDM erzeugt und dieser HMAC signiert in das ePA-Aktensystem eingestellt wird. Das Einstellen des VSDM-Prüfnachweises muss innerhalb von 20 Minuten nach Erzeugung geschehen. Die Erstellung einer Befugnis kann automatisch im Hintergrund als implizite Operation durchgeführt werden. Um eine sofortige Benutzung der ePA in der Leistungserbringerinstitution zu gewährleisten, wird empfohlen, dass die Befugniserzeugung ohne Zeitverzug durchgeführt wird.

Zusätzlich soll die Befugniserzeugung als eine aktive, explizit ansteuerbare Operation für den Nutzer des Primärsystems angeboten werden, bspw.:

- wenn das Einlesen der eGK zu einem nachträglichen Zeitpunkt geschieht.,
- wenn eine Befugnis in einer Einrichtung eines öffentliche Gesundheitsdienstes bezogen wird (Opt-in) oder
- wenn eine Befugnis in einer Einrichtung der Arbeits- oder Betriebsmedizin bezogen wird (Opt-in).

Das ePA-Aktensystem liefert eine Antwortnachricht validTo zurück, womit das zeitliche Ende der Befugnis bekannt gemacht wird. Das Primärsysteme kann diese Information lokal vorhalten, um dem Nutzer zu einem späteren Zeitpunkt eine Auskunft darüber zu geben, für wie lang eine errechnete Zugriffsbefugnis noch Gültigkeit haben sollte.

Dem Nutzer soll das Weiterarbeiten im Primärsystem ermöglicht werden. Erfolgsmeldungen können so in die Benutzeroberfläche integriert werden, dass sie keine Interaktion des Nutzers verlangen und den Nutzer nicht im weiteren Arbeitsprozess stören. Dem Nutzer werden nur bei Fehlermeldungen verständliche Hinweise angezeigt. Das Primärsystem soll dem Nutzer Konfigurationsmöglichkeiten zur Anzeige und zum Umgang mit Fehlermeldungen anbieten.

Zu den möglichen Fehlerkonstellationen gehören:

- Es ist kein Zugriff auf das ePA-Aktenkonto möglich, weil das ePA-Aktenkonto nicht (mehr) existiert.
  - *Hinweis:* Dies entspricht der REST-Fehlermeldung Health record does not exist – 404 – noHealthRecord.
- Es ist kein Zugriff auf das ePA-Aktenkonto möglich, weil sich das ePA-Aktenkonto im Umzug befindet. Bitte versuchen Sie es in 24h erneut.
  - *Hinweis:* Dies entspricht der REST-Fehlermeldung Health record is not in state ACTIVATED – 409 – statusMismatch.
- Es ist kein Zugriff auf das ePA-Aktenkonto möglich, weil keine Berechtigung vorliegt (die Einrichtung wurde vom Versicherten für den Zugriff ausgeschlossen).
  - *Hinweis:* Dies entspricht der REST-Fehlermeldung request claims actorId and actorIdis referenced by a Blocked User Policy assignment – 409 – requestMismatch.

Hinweis: Das Primärsystem muss alle Zertifikate, die es aktiv verwendet, auf Integrität und Authentizität prüfen. Wenn die Serverzertifikate gewechselt werden, muss der Client die neue Zertifikatskette kennen, gegen die er prüft. Das Primärsystem kann zyklisch die TSL der TI herunterladen, auswerten und in seinem Zertifikatspeicher die neuen, relevanten Zertifikatsketten für die Zertifikatsprüfung verfügbar machen. Die Komponenten-CA-Zertifikate findet man in der TSL und auf https://download.tsl.ti-dienste.de/.

6.1.2 Anzeige und Suche von Dokumenten eines ePA-Aktenkontos

Für den Nutzer des Primärsystems soll es möglich sein, das ePA-Aktenkonto eines Versicherten zur Anzeige zu bringen. Das bedeutet, dass mit einer Art ePA-Browser-Ansicht die Ergebnisse einer Such-Operation auf das ePA-Aktenkonto angezeigt werden. Diese Ansicht soll bspw. aus der Patientenkartei heraus aufgerufen werden können.

Beim Aufruf sollte ein Standard-Suchfilter angewendet werden. Das Suchen nach Dokumenten erfolgt auf den Metadaten des Dokumentes und erfolgt im ePA-Aktenkonto ausschließlich auf Dokumente, die für den Leistungserbringer sichtbar sind. Der Filter soll nach Dokumenten suchen, die ein Einstelldatum größer Datum des letzten Kontakts der Leistungserbringerinstitution mit dem Patienten tragen (laut Karteikarte oder lokaler Dokumentation im Primärsystem).

Dafür können bei einer RegistryStoredQuery (z.B. FindDocuments) die Parameter $XDSDocumentEntryCreationTimeFrom und $XDSDocumentEntryCreationTimeTo verwendet werden. Es sollte möglich sein die Suchkriterien des Filters entsprechend den Bedürfnissen der Leistungserbringerinstitution anzupassen. Die Filterauswahl sollte vom Nutzer gespeichert und als Standard gesetzt werden können.

Für den Nutzer des Primärsystems soll konfigurierbar sein, dass bestimmte MIOs einer Patient:in in einer separaten Ansicht aufgerufen werden. Zu diesen MIOs zählen der Impfpass, das Kinderuntersuchungsheft, der Mutterpass und das Zahnbonusheft. Der Nutzer soll konfigurieren können, für welche MIOs eine separate Ansicht im Primärsystem benutzt werden soll. Diese MIOs sind pass- oder eintragsbasiert und unterscheiden sich vom herkömmlichen Dokumenten-Handling.

Dafür können mittels einer RegistryStoredQuery per GetFolders sowie der bekannten Folder.entryUUID für das MIO die Folder-Metadaten abgerufen werden. Das Attribut $XDSFolder.lastUpdateTime zeigt, ob es ein Update gab.

Künftige MIOs werden sich technisch wie ein herkömmliches Dokument verhalten, sind inhaltlich vollstrukturiert.

Eine Übersicht über (noch) nicht in die ePA gestellte MIOs oder fehlende Dokumente in der ePA, die bspw. aufgrund einer ausstehenden Laboruntersuchung noch nicht verfügbar sind, werden vom ePA-Aktensystem nicht unterstützt. Eine logische Auswertungs- und Darstellungsmöglichkeit für den Nutzer kann vom Primärsystem implementiert werden.

6.1.3 Hochladen in ein ePA-Aktenkonto im Kontext der lokalen Dokumentenverwaltung

Für Nutzer eines Primärsystems soll es einfach sein, Dokumente in die ePA einzustellen. Damit soll erreicht werden, dass behandlungsrelevante Dokumente Einzug in die ePA erhalten und somit für den Versicherten und andere Leistungserbringerinstitutionen einsehbar sind. Der Upload von Dokumenten über den XDS Document Service setzt voraus, dass das ePA-Aktenkonto des Versicherten lokalisiert wurde und damit der Service-Endpunkt des ePA-Aktenkontos bekannt ist.

Der Nutzer des Primärsystems soll auf Basis einer bestehenden User Session, des lokalisierten Service-Endpunkts und des lokalisierten ePA-Aktenkontos daher die ePA immer nutzen können, wenn er sich in einem Dokumentenmanagementkontext befindet. Das kann der Fall sein, wenn bspw.:

- ein Dokument vor Ort eingescannt und in die Primärdokumentation übernommen wird (und in die ePA hochgeladen werden soll),
- ein Dokument im Zug einer Dokumentenbearbeitung verändert und aktualisiert wird (und in die ePA hochgeladen werden soll),

- ein Dokument im Zuge einer Dokumentenbearbeitung an einem bestimmten Zeitpunkt vidiert oder archiviert wird (und in die ePA hochgeladen werden soll).

Das Hochladen in die ePA soll aus diesen Sichten und Prozessen heraus angestoßen werden können. Ob das Dokument durch das Primärsystem- oder ein Archivsystem in die ePA hochgeladen wird, legt die Leistungserbringerinstitution fest. Die technische Integrationsebene der ePA im Primärsystem legt jeder Hersteller für sich selber fest.

6.1.4 Hochladen in ein ePA-Aktenkonto als Standard für bestimmte Dokumententypen

In den Einstellungen des Primärsystems soll festgelegt sein, dass bestimmte Dokumente standardmäßig in das dazugehörige ePA-Aktenkonto der Patient:in hochgeladen werden. Das Nähere zum Anforderungskatalog regeln die Leistungserbringerinstitution und der Primärsystemhersteller miteinander, bspw. in Form von Richtlinien in einem Krankenhaus.

Zu diesen Dokumenten gehören:

- eArztbrief (PDF/A)
- Krankenhaus-Entlassbrief (PDF/A)
- Laborbefund (PDF/A)
- Bildbefund (PDF/A)
- Befundberichte aus invasiven oder chirurgischen sowie aus nicht-invasiven oder konservativen Maßnahmen (PDF/A)

Die Option zum Hochladen des in Erstellung befindlichen Dokuments in die ePA ist dann in diesen Fällen voreingestellt. Das Hochladen des Dokuments wird vom Primärsystem durchgeführt und kann nach der Erstellung, Freigabe, Finalisierung oder Archivierung durchgeführt werden. Die Festlegung zur Standardeinstellung trifft die Leistungserbringerinstitution für sich selber.

Das ePA-Aktensystem unterscheidet nicht auf Metadatenebene, ob ein Dokument vorläufig oder endgültig ist. Für den Fall, dass ein vorläufiges Dokument in die ePA hochgeladen wird, sollte diese Dokumenteneigenschaft innerhalb des Dokuments für den Leser ersichtlich sein.

Beim Hochladen eines Dokuments in das ePA-Aktensystem wird eine unique ID vergeben. Das ePA-Aktsystem erzeugt dabei einen Hashwert und nimmt bei jedem Hochladen eine Dublettenprüfung vor. Um ein Dokument zu überschreiben und dessen Status von „approved“ auf „deprecated“ zu verändern, muss es mit der replace-Operation hochgeladen werden.

Für den Fall, dass dem Hochladen eines Krankenhaus-Entlassbriefs, eines Laborbefundes oder eines Bildbefundes widersprochen wurde, erzeugt das Primärsystem standardmäßig einen Protokolleintrag in der Patientenübersicht oder eine Hinweisnotiz in der Karteikarte der Patient:in.

6.1.5 Hochladen in ein ePA-Aktenkonto als Standard für ausgewählte Dokumententypen in der Benutzung von KIM

In den Einstellungen des Primärsystems soll festgelegt sein, dass beim Versenden eines eArztbriefs oder einer elektronischen Arbeitsunfähigkeitsbescheinigung (eAU) über KIM das Dokument standardmäßig in das dazugehörige ePA-Aktenkonto der Patient:in hochgeladen wird. Die Option zum Hochladen des ausgewählten Dokuments in die ePA ist

dann in diesen Fällen voreingestellt und kann in der Form umgesetzt werden, wenn die gleiche Telematik-ID für beide Vorgänge verwendet wird.

Der Nutzer klickt nur dann in der Eingabemaske oder bedient eine Tastenkombination, um das voreingestellte Hochladen in das ePA-Aktenkonto abzuwählen, wenn der Versicherte dem widerspricht.

Für den Fall, dass das Hochladen im Kontext eArztbrief abgewählt wurde, erzeugt das Primärsystem standardmäßig einen Protokolleintrag in der Patientenübersicht oder eine Notiz in der Karteikarte der Patient:in, dass diese:r dem Hochladen des eArztbriefs widersprochen hat. Der eArztbrief wird per KIM verschickt, jedoch nicht gleichzeitig in das ePA-Aktenkonto hochgeladen. Da Leistungserbringer nach §§ 347 und 348 SGB V zum Hochladen eines eArztbriefs in die ePA gesetzlich verpflichtet sind, muss der Widerspruch protokolliert werden.

Für den Fall, dass das Hochladen im Kontext eAU abgewählt wurde, erzeugt das Primärsystem keinen Protokolleintrag in der Patientenübersicht bzw. keine Notiz in der Karteikarte der Patient:in. Die eAU wird per KIM verschickt, jedoch nicht gleichzeitig in das ePA-Aktenkonto hochgeladen. Da Leistungserbringer zum Hochladen einer eAU in die ePA gesetzlich nicht verpflichtet sind, muss der Widerspruch nicht protokolliert werden.

Der Leistungserbringer soll die Möglichkeit haben die Voreinstellung zum standardmäßigen Hochladen anzupassen. Die Voreinstellung soll differenziert für eArzbriefe einerseits und für eAU andererseits gesetzt werden können.

6.1.6 Hochladen in ein ePA-Aktenkonto als Standard für NFDM und eMP (eGK)

Das Primärsystem sollte die Möglichkeit bieten, dass in den Einstellungen des Primärsystems festgelegt werden kann, dass beim Erstellen eines Notfalldatensatzes für die eGK (NFDM) oder eines elektronischen Medikationsplans auf der eGK (eMP) diese standardmäßig in das dazugehörige ePA-Aktenkonto der Patient:in hochgeladen werden. Das Nähere zum Anforderungskatalog regeln die Leistungserbringerinstitution und der Primärsystemhersteller miteinander, bspw. in Form von Richtlinien in einem Krankenhaus.

Die Option zum Hochladen des ausgewählten Dokuments in die ePA ist dann in diesen Fällen voreingestellt. Der Nutzer klickt nur dann in der Eingabemaske oder bedient eine Tastenkombination, um das voreingestellte Hochladen in die ePA abzuwählen, wenn der Versicherte dem widerspricht.

Für den Fall, dass dem Hochladen im Kontext NFDM widersprochen wurde, erzeugt das Primärsystem keinen Protokolleintrag in der Patientenübersicht bzw. keine Notiz in der Karteikarte der Patient:in.

Für den Fall, dass dem Hochladen im Kontext eMP (eGK) widersprochen wurde, erzeugt das Primärsystem keinen Protokolleintrag in der Patientenübersicht bzw. keine Notiz in der Karteikarte der Patient:in und es wird der eMP als Ausdruck in Form des BMP angeboten.

Der Master-Datenträger für NFDM und eMP (eGK) ist die eGK.

6.1.7 Standardmäßige Vorbelegung von Werten beim Hochladen eines Dokuments in ein ePA-Aktenkonto

Um Dokumente aufwandsarm hochladen zu können, soll es möglich sein, in den Einstellungen des Primärsystems bestimmte Parameter zu setzen. Es sollen die Stammdaten des behandelnden Leistungserbringers und der Leistungserbringerinstitution in ein Dokument standardmäßig übernommen oder editiert werden können, um ohne eine

nachträgliche Metadateneingabe hochladen zu können. Das Primärsystem kann dem Nutzer auch die Möglichkeit zur Anlage von Metadatentemplates für gängige Dokumente aus dem Versorgungsalltag der Leistungserbringerinstitution bereitstellen, um beim Hochladen eine Auswahl treffen zu können ohne durch die unterschiedlichen Metadatenfelder gehen zu müssen.

6.1.8 Nachträgliches Hochladen eines Dokuments in ein ePA-Aktenkonto

Leistungserbringer sind nach §§ 347 und 348 SGB V dazu verpflichtet bestimmte Dokumente aus dem aktuellen Behandlungskontext in das ePA-Aktenkonto der Patient:in hochzuladen. In gewissen Konstellationen ist es möglich, dass ein Hochladen zum gewünschten Zeitpunkt nicht möglich ist, bspw. durch eine technische Störung oder weil die Zugriffsbefugnis noch nicht oder nicht mehr vorliegt.

Das Primärsystem kann dem Nutzer die Möglichkeit geben Dokumente zu merken, auf eine Aufgabenliste zu setzen oder einen Bereich zur ePA-Dokumentenverwaltung einer Patient:in bereitstellen, um ein Hochladen an einem späteren Werktag ausführen zu können.

6.1.9 Widerspruch gegen das Hochladen eines Dokuments in ein ePA-Aktenkonto

Der Versicherte hat das Recht dem Hochladen eines Dokuments in sein ePA-Aktenkonto zu widersprechen. In der lokalen Behandlungsdokumentation im Primärsystem sollte eine Gesprächsnotiz zu dieser Entscheidung protokolliert und das betroffene Dokument entsprechend gekennzeichnet werden.

Die Kennzeichnung soll im Primärsystem einfach und unmittelbar „mit einem Klick“ zu jedem Dokument zu hinterlegen sein. Das Entfernen der Kennzeichnung muss nach Anzeige einer Warnung ebenfalls ermöglicht werden. Der Versuch des Einstellens eines gekennzeichneten Dokumentes in das ePA-Aktenkonto der Patient:in soll durch das Primärsystem unterbunden werden. Hierbei ist eine verständliche Rückmeldung auszugeben.

6.2 XDS Document Service: Dokumentenverwaltung in der elektronischen Patientenakte

Das Primärsystem soll zum XDS Document Service in der elektronischen Patientenakte folgende funktionale Anwendungsfälle und die dazugehörigen Klickpfade umsetzen:

1. Dokumentenübersicht anzeigen
2. Dokumente suchen, filtern und sortieren
3. Dokumente herunterladen, aktualisieren und löschen
4. Dokumente hochladen aus Karteikarte oder Dokumentenmanagementkontext
5. Dokumente hochladen aus KIM-Workflow
    a. eArztbrief
    b. eAU

6.2.1 Dokumentenübersicht anzeigen

Für den Nutzer des Primärsystem muss es möglich sein, eine Übersicht über die im ePA-Aktenkonto sichtbaren Dokumente abzurufen.

Eine Möglichkeit ist, dass die Dokumente des ePA-Aktenkontos über eine separate Ansicht angezeigt werden (siehe Abbildung 16). Eine weitere Möglichkeit ist, dass die Dokumente des ePA-Aktenkontos in der Dokumentenverwaltung integriert und dort zur Anzeige gebracht werden (siehe Abbildung 17).

Die Ärzt:in oder Psychotherapeut:in soll anhand der Dokumentenübersicht erkennen können, ob die in der ePA sichtbaren Dokumente bereits in seiner lokalen Behandlungsdokumentation im Primärsystem enthalten sind, also schon heruntergeladen wurden. Die Dokumentenübersicht soll standardmäßig nach dem Erstellungsdatum der Dokumente sortiert sein.

Eine Dokumentenübersicht ist das Ergebnis einer Dokumentensuche in der ePA. Die Suche bezieht sich auf die aktuellen Metadaten der Dokumente im XDS Document Service. Im Primärsystem können für den Nutzer die Suchparameter dokumentiert werden, mit der nach Dokumenten in der ePA gesucht wurde. Damit kann ein Nutzer zu einem späteren Zeitpunkt nachvollziehen, wonach zum vorherigen Zeitpunkt gesucht wurde.

Tabelle 27: Dokumentenübersicht anzeigen - UX Optimaler Klickpfad

Titel	**ePA_DMS_1 – Dokumentenübersicht anzeigen**
Zielstellung	Der Nutzer öffnet die ePA der Patient:in, kann die Dokumente in der ePA sehen und Folgeschritte innerhalb der ePA unternehmen.
Vorbedingung	• Der Nutzer befindet sich im Primärsystem in der Karteikarte einer konkreten Patient:in. • Das Primärsystem muss einen VAU-Kanal zum ePA-Aktensystem und eine User Session aufgebaut haben. • Zum Suchen muss ein gültiges Entitlement für die Leistungserbringerinstitution im ePA-Aktensystem für das angefragte ePA-Aktenkonto vorliegen.
Nachbedingung	• Der Nutzer sieht die ihm sichtbaren Dokumente in der ePA der Patient:in.
Klickpfad	1a. Die Ärzt:in oder MFA klickt einen Menüpunkt zur ePA an oder bedient eine Tastenkombination. 1b. Die Ärzt:in oder MFA klickt einen Menüpunkt zur Dokumentenverwaltung an oder bedient eine Tastenkombination 2. Eine Übersicht von sichtbaren Dokumente in einem ePA-Aktenkonto wird angezeigt, für welche die Einrichtung eine Zugriffsbefugnis hat.
Alternative	N/A

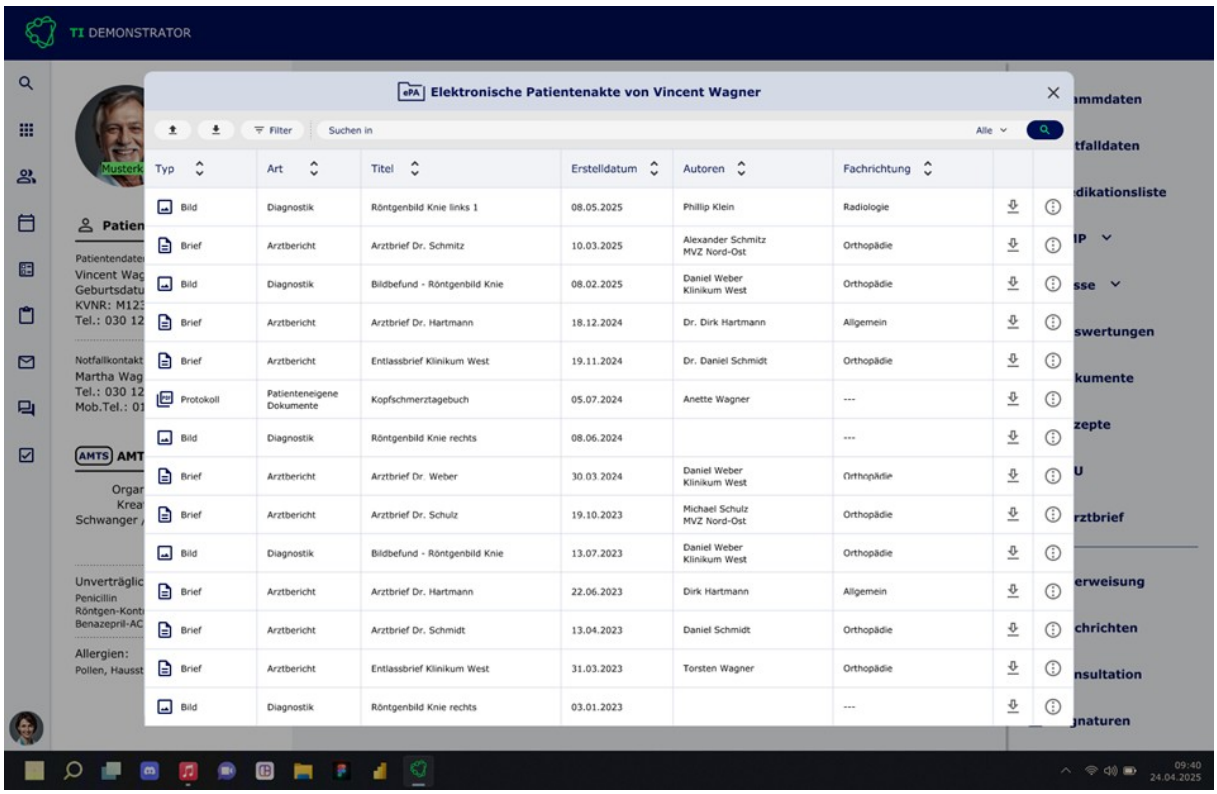

Abbildung 17: Anzeige der ePA-Dokumentenübersicht als separate Ansicht aus einer Karteikarte heraus

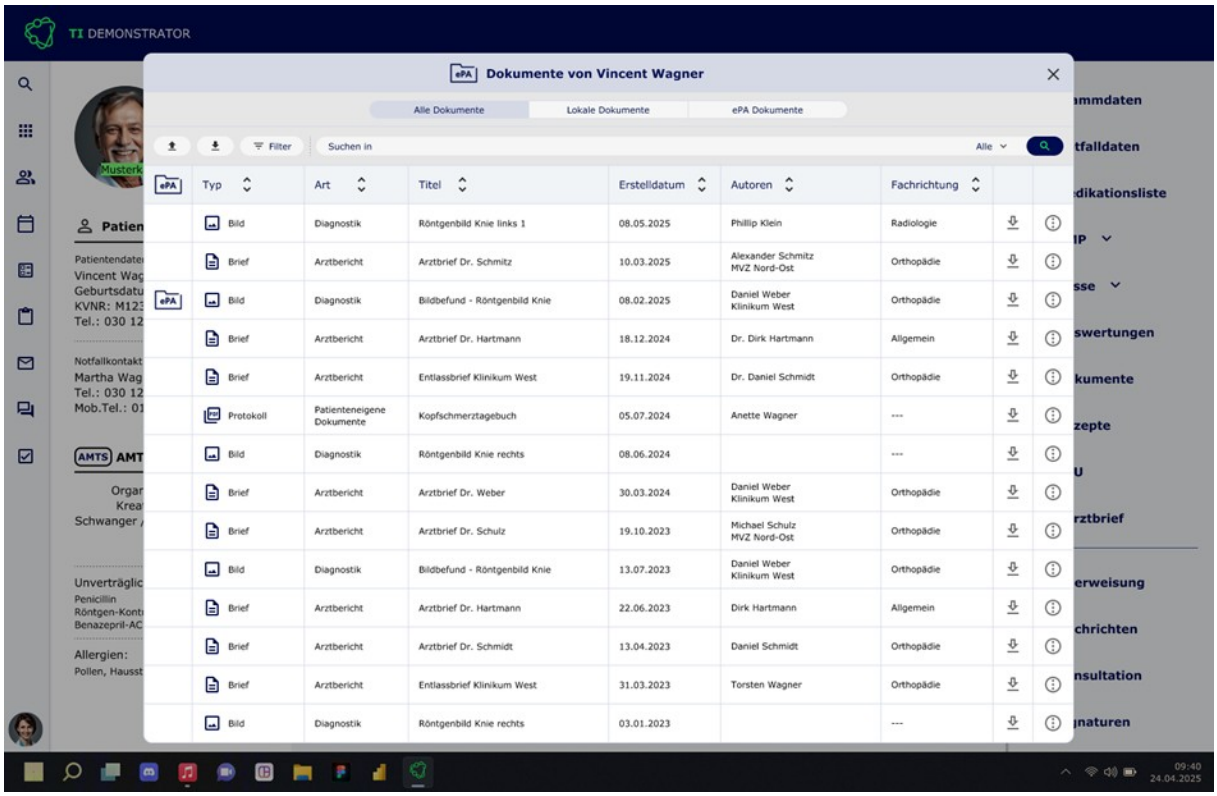

Abbildung 18: Anzeige von ePA-Dokumenten als Teil einer integrierten Dokumentenübersicht in der lokalen Dokumentenverwaltung

6.2.2 Dokumente suchen, filtern und sortieren

Um Dokumente im ePA-Aktenkonto der Patient:in finden zu können, soll das Primärsystem die Möglichkeit nutzen, auf Metadatenebene in der ePA zu suchen, filtern und sortieren. Die Suchoperation bezieht sich standardmäßig auf die aktuellen Metadaten und auf „approved“ Dokumente im ePA-Aktenkonto.

Die Dokumente in der Trefferliste sollen auf Ebene ihrer Metadaten sortiert und gefiltert werden können. Der Nutzer des Primärsystems kann damit je Metadatum die Reihenfolge der Dokumente in der Trefferliste ändern lassen (z.B. das neueste Einstelldatum zuerst) oder je Metadatum die Anzahl der Suchergebnisse in der Trefferliste reduzieren (z.B. nur Dokumente der Dokumentenart „Befundbericht“ oder des Dokumententyps „Ergebnisse Funktionsdiagnostik“). Der Nutzer des Primärsystems soll auch anhand mehrerer Kriterien gleichzeitig suchen und filtern können (z.B. Dokumente des Dokumententyps „Arztberichte“ mit dem Datum „letztes Jahr“ (tt.mm.yyyy-tt.mm.yyyy)).

Der Nutzer des Primärsystems soll nach den eineindeutigen IHE Metadaten suchen, filtern und sortieren können. Das Primärsystem soll dem Nutzer auch eine Möglichkeit bieten über ähnliche Metadaten ein Dokument finden zu können. Dazu können im Primärsystem die alternativen Begriffe verwendet werden, die IHE in ihrer Beschreibung jeweils einem Wert eindeutig zuordnet. Ein Beispiel ist der IHE typeCode BERI mit der Bezeichnung „Arztberichte“. Eine Ähnlichkeitssuche entlang der Begriffe „Arztbrief“, „Entlassungsbericht“, „Rehabericht“, etc., die in der Beschreibung zu finden sind, soll dem Nutzer des Primärsystems angeboten werden. Das Primärsystem leitet vom ausgewählten Begriff den eineindeutigen und auffindbaren Wert nach IHE ab und sucht anhand dieses Werts im ePA-Aktenkonto nach den dazugehörigen Dokumenten. Eine Suche mit der Methode "FindDocuments" ist ebenfalls möglich, mit der nach der eventCodeListe gefiltert werden kann.

Für den Nutzer des Primärsystems sollen neue Dokumente im ePA-Aktenkonto kenntlich gemacht werden, die seit der letzten Suche im ePA-Aktenkonto dazugekommen sind. Dazu kann nach Dokumenten gesucht werden, für die das Einstelldatum nach dem Datum des letzten Kontakts mit der Patient:in liegt (bspw. mithilfe einer RegistryStoredQuery und den Parametern $XDSDocumentEntryCreationTimeFrom und $XDSDocumentEntryCreationTimeTo).

Im Primärsystem können für den Nutzer die Suchparameter dokumentiert werden, mit der nach Dokumenten in der ePA gesucht wurde. Damit wird es für den Nutzer möglich eine Folgesuche zu einem späteren Zeitpunkt gezielt anzupassen.

Eine Darstellung, wie eine Such-, Filter- und Sortiermaske gestaltet sein kann, kann Abbildung 18 und Abbildung 19 entnommen werden.

Tabelle 28: Dokumente suchen, filtern und sortieren - UX Optimaler Klickpfad

Titel	**ePA_DMS_2 - Dokumente suchen, filtern und sortieren**
Zielstellung	Der Nutzer kann mithilfe der Metadaten der Dokumente im ePA-Aktenkonto nach einem oder mehreren Dokumenten suchen, filtern und sortieren.

Vorbedingung	• Der Nutzer befindet sich im Primärsystem in der Karteikarte einer konkreten Patient:in. • Das Primärsystem muss einen VAU-Kanal zum ePA-Aktensystem und eine User Session aufgebaut haben. • Zum Suchen muss ein gültiges Entitlement für die Leistungserbringerinstitution im ePA-Aktenkonto vorliegen.
Nachbedingung	• Der Nutzer sieht die ihm sichtbaren Dokumente in der ePA der Patient:in. • Die angezeigte Trefferliste der Dokumente im ePA-Aktenkonto entspricht den ausgewählten Kriterien.
Klickpfad	1a. Die Ärzt:in oder MFA klickt einen Menüpunkt zur ePA an oder bedient eine Tastenkombination. 1b. Die Ärzt:in oder MFA klickt einen Menüpunkt zur Dokumentenverwaltung an oder bedient eine Tastenkombination 2. Eine Übersicht von sichtbaren Dokumente in einem ePA-Aktenkonto wird angezeigt, für welche die Einrichtung eine Zugriffsbefugnis hat. 3. Die Funktion im Primärsystem bietet mit einem Klick oder einer bestimmten Tastenkombination die Möglichkeit: a) zu suchen b) zu filtern c) zu sortieren.
Alternative	N/A

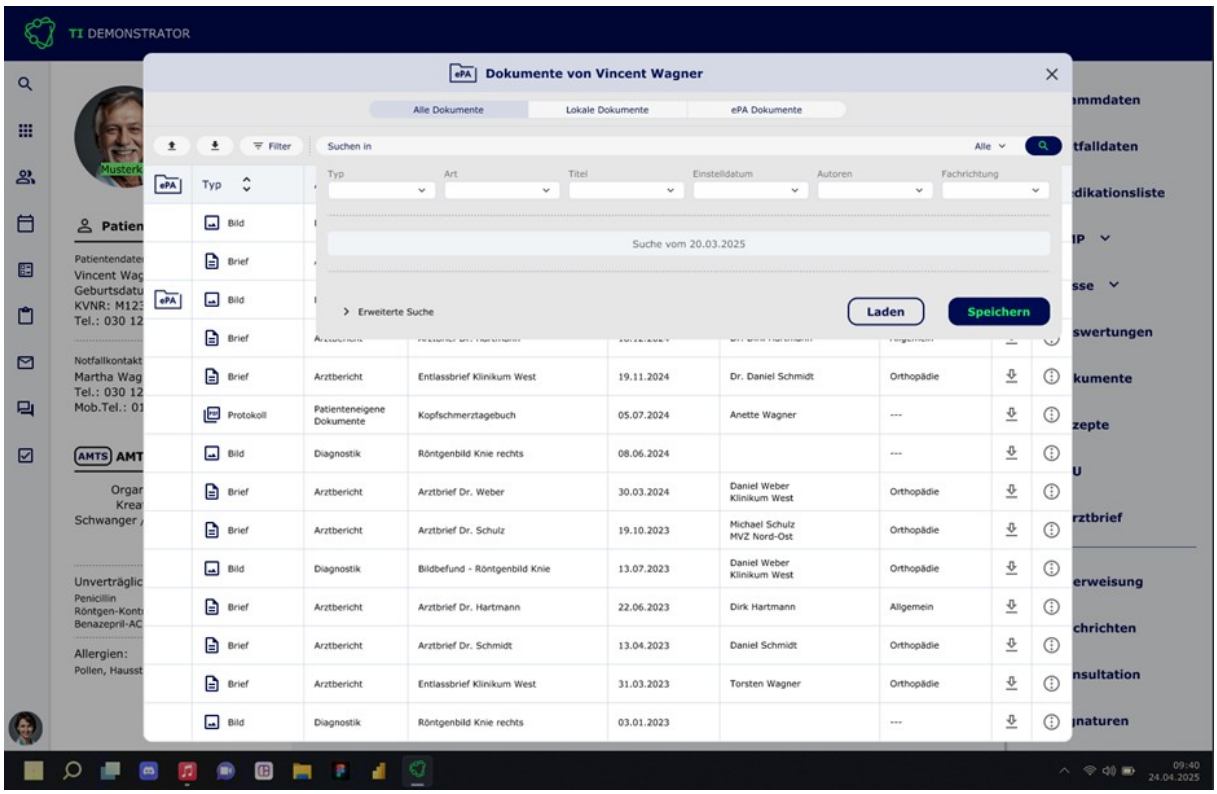

Abbildung 19: Funktion im Primärsystem, um zu suchen, filtern und sortieren von Dokumenten in einem ePA-Aktenkonto

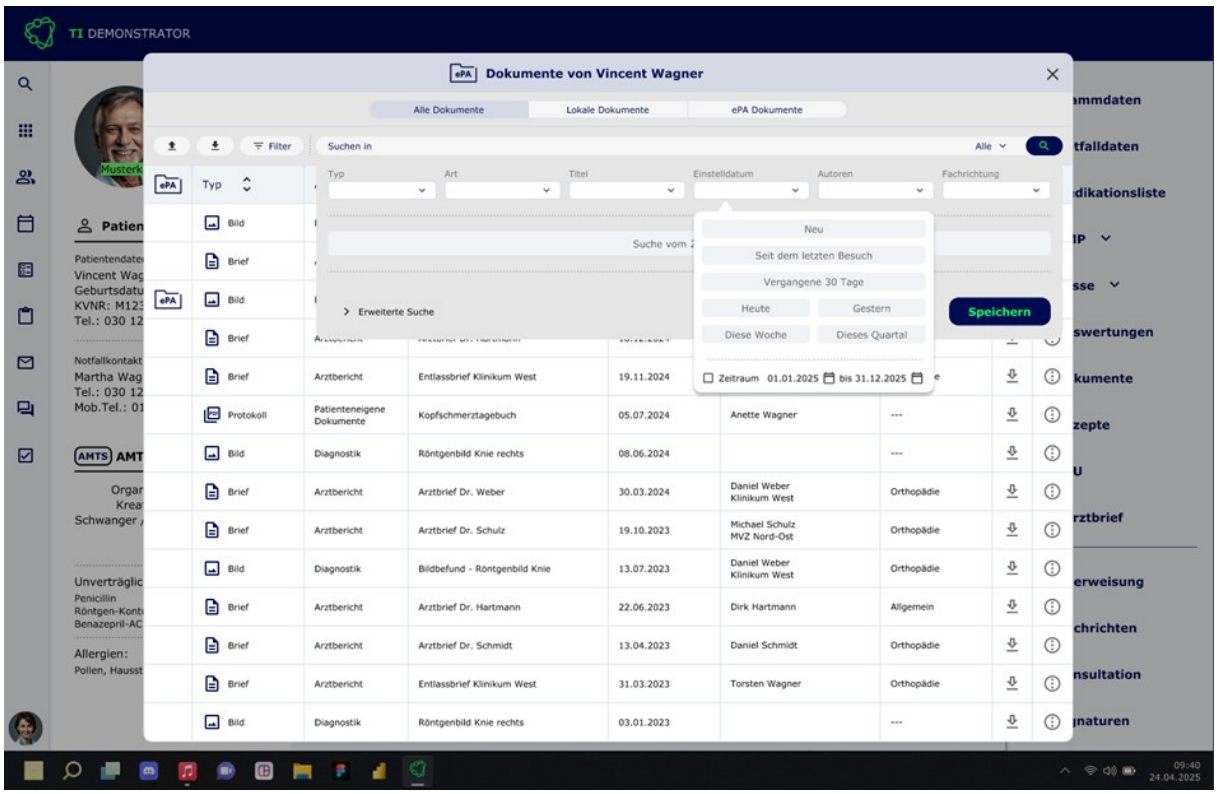

Abbildung 20: Funktion im Primärsystem, um zu suchen, filtern und sortieren von Dokumenten in einem ePA-Aktenkonto

6.2.3 Dokumente herunterladen, aktualisieren oder löschen

Um ein oder mehrere Dokumente aus dem ePA-Aktenkonto der Patient:in anzuzeigen und in die Primärdokumentation zu übernehmen, dessen Metadaten zu bearbeiten oder diese im ePA-Aktenkonto löschen zu können, kann das Primärsystem dem Nutzer für die diese Operationen ein Kontextmenü anbieten.

Damit ein Dokument aus einer Dokumentenübersicht oder aus der Trefferliste einer Dokumentensuche vom Nutzer des Primärsystems angezeigt und gelesen werden kann, muss es heruntergeladen werden. Das Herunterladen eines Dokuments soll für den Nutzer maximal wenige Sekunden Zeit in Anspruch nehmen. Das Primärsystem soll das Herunterladen eines einzelnen Dokuments und von mehreren Dokumenten im Stapel ermöglichen.

Das Primärsystem soll dem Nutzer eine "Vorschau" eines Dokuments aus dem ePA-Aktenkonto ermöglichen. In diesem Fall wird ein Dokument technisch bereits heruntergeladen, ein Protokolleintrag im ePA-Aktenkonto hinterlegt und das Dokument nach dem Beenden der Vorschau wieder verworfen. Der Nutzer soll die Möglichkeit haben aus einer Vorschau in eine (Voll-)Ansicht des Dokuments wechseln zu können. In den Einstellungen des Primärsystems soll der Nutzer einstellen können, ob immer mit Ansicht eines Dokuments eine standardmäßige Übernahme erfolgt oder erst nach Lesen eines Dokuments vom Nutzer eine aktive Übernahme in die lokale Behandlungsdokumentation erfolgen soll.

Beim Herunterladen von Dokumenten aus dem ePA-Aktenkonto soll das Primärsystem den Nutzer dabei unterstützen zu prüfen, ob das ausgewählte Dokument bereits in der lokalen Behandlungsdokumentation vorhanden ist. So kann eine Doppelablage von Dokumenten vermieden werden.

Der Nutzer soll in den Einstellungen des Primärsystems einstellen können, ob immer mit Ansicht eines Dokuments eine standardmäßige Übernahme erfolgt oder erst nach Lesen eines Dokuments vom Nutzer eine aktive Übernahme in die lokale Behandlungsdokumentation erfolgt.

In der Dokumentenübersicht bzw. der Trefferliste der Dokumentensuche soll eine Auswahl mehrerer Dokumente möglich sein, um diese direkt und ohne ein vorheriges Lesen in die lokale Behandlungsdokumentation zu übernehmen.

Eine Aktualisierung von Dokumenten oder von deren Metadaten erfordert immer eine gültige Zugriffsbefugnis. Eine Änderung von Metadaten eines Dokuments im ePA-Aktenkonto kann durchgeführt werden, ohne dass das Dokument heruntergeladen werden muss. Eine Aktualisierung von Dokumenten im ePA-Aktensystem kann jederzeit durchgeführt werden. Das ePA-Aktensystem erzeugt für jedes Dokument eine unique ID und versioniert die verschiedenen Dokumentenversionen. Jedes Dokument hat dementsprechend einen Status. Ein neues Dokument wird mit einer replace Operation hochgeladen und ersetzt damit das vorliegende, nunmehr alte Dokument. Gültige Dokumente tragen den Status „approved“ und ungültige Dokumente den Status „deprecated“. Die Sichtbarkeit eines Dokuments kann sich aufgrund einer Aktualisierung der Metadaten nicht verändern.

Eine Darstellung, wie die Dokumentenbearbeitung eines Dokuments aus der ePA der Patient:in angesteuert werden kann, kann Abbildung 20 entnommen werden.

Hinweis:

1. *Das Löschen von Dokumenten kann zu ungewollten Lücken in der medizinischen Dokumentation der Patientenakte führen. Bevor ein Dokument in einem ePA-Aktenkonto gelöscht wird, soll der Nutzer des Primärsystems darüber informiert werden, dass das Dokument im Anschluss unwiderruflich für den Versicherten in dessen ePA gelöscht sein wird. Ebenso soll ein Hinweis erscheinen, dass das Dokument auch (erneut) verborgen eingestellt werden kann und damit nur für die Patient:in einsehbar ist.*
2. *Eine Änderung von Metadaten kann von jedem Leistungserbringer durchgeführt werden, d.h. vom Ersteller, vom Einsteller und von Dritten. Die Annahme ist, dass eine Änderung fachlich motiviert ist und zur Korrektur der dann gültigen Metadaten führt. Eine Versionierung der vorher vergebenen Metadaten findet nicht statt im ePA-Aktensystem.*
3. *Beim Ändern von Metadaten ist darauf zu achten, dass das Dokument nicht erneut abgelegt wird. Die Sichtbarkeit über den CON-Code als ConfidentialityCode ist vom Metadata Update ausgeschlossen.*
4. *Eine Dublettenablage in der ePA, d.h. die Ablage eines identischen Dokuments im ePA-Aktenkonto, wird durch den Vergleich eines Hash-Werts vom ePA-Aktensystem vermieden. Eine Dublettenablage im Primärsystem, d.h. die Ablage eines identischen Dokuments in der lokalen Patientendokumentation, soll durch den Vergleich der UUID des Dokuments vom Primärsystem vermieden werden.*

Tabelle 29: Dokumente herunterladen, aktualisieren oder löschen - UX Optimaler Klickpfad

Titel	**ePA_DMS_3 – Dokumente herunterladen, aktualisieren oder löschen**
Zielstellung	Der Nutzer kann Dokumente aus einem ePA-Aktenkonto a) herunterzuladen, um sich diese anzeigen zu lassen, sie zu lesen und sie in der lokalen Behandlungsdokumentation zu speichern, oder

	b) aktualisieren, indem die Metadaten eines vorhandenen Dokuments korrigiert werden oder ein Dokument komplett ersetzt wird, oder c) löschen.
Vorbedingung	• Der Nutzer befindet sich im Primärsystem in der Karteikarte des Primärsystems einer konkreten Patient:in. • Das Primärsystem muss einen VAU-Kanal zum ePA-Aktensystem und eine User Session aufgebaut haben. • Zum Herunterladen, Aktualisieren und Löschen muss ein gültiges Entitlement für die Leistungserbringerinstitution im ePA-Aktenkonto vorliegen. • Der Nutzer hat ein oder mehrere für die Leistungserbringerinstitution sichtbare Dokumente ausgewählt, die verwaltet werden sollen.
Nachbedingung	a) Für den Nutzer wird erkenntlich, dass das Dokument erfolgreich aus dem ePA-Aktenkonto heruntergeladen wurde. b) Für den Nutzer wird erkenntlich, dass die Metadaten eines Dokuments im ePA-Aktenkonto erfolgreich aktualisiert wurden. c) Für den Nutzer wird erkenntlich, dass ein Dokument im ePA-Aktenkonto erfolgreich gelöscht wurde.
Klickpfad	1a. Die Ärzt:in oder MFA klickt einen Menüpunkt zur ePA an oder bedient eine Tastenkombination. 1b. Die Ärzt:in oder MFA klickt einen Menüpunkt zur Dokumentenverwaltung an oder bedient eine Tastenkombination 2. Eine Übersicht von sichtbaren Dokumente in einem ePA-Aktenkonto wird angezeigt, für welche die Einrichtung eine Zugriffsbefugnis hat. 3. Die Funktion im Primärsystem bietet mit einem Klick oder einer bestimmten Tastenkombination die Möglichkeit: a) Zum Herunterladen: i) ein Herunterladen und damit eine direkte Übernahme des Dokuments in die lokale Behandlungsdokumentation; ii) ein Herunterladen und damit Anzeigen des Dokuments ii-1) mit der anschließenden Option das Dokument in die lokalen Behandlungsdokumentation zu übernehmen; ii-2) mit der anschließenden Option das Dokument zu verwerfen und nicht in die lokale Behandlungsdokumentation zu übernehmen; b) Zum Aktualisieren i) der Metadaten eines bestehenden Dokuments; ii) eines bestehenden Dokuments, indem dieses ersetzt wird; c) Zum Löschen eines Dokuments im ePA-Aktenkonto.
Alternative	N/A

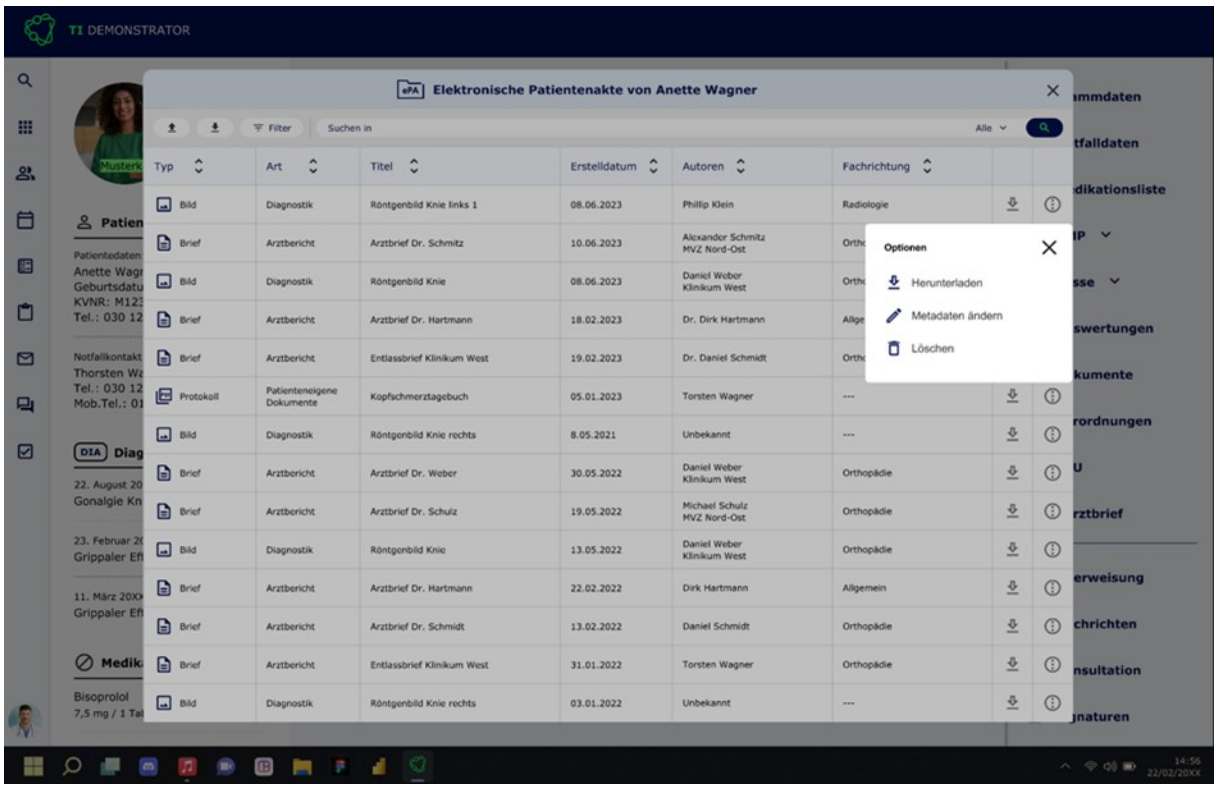

Abbildung 21: Anzeige eines Kontextmenüs für ein ausgewähltes Dokument, um dieses zu bearbeiten (am rechten Bildrand ist der Menüpunkt zu finden)

6.2.4 Dokument hochladen aus Karteikarte oder Dokumentenmanagementkontext

Um ein oder mehrere Dokumente in das ePA-Aktenkonto der Patient:in aufwandsarm hochzuladen, soll die Funktion zum Hochladen aus der Karteikarte der Patient:in angeboten werden und an jeder Stelle, an dem ein Dokument im Rahmen eines Dokumentenmanagementkontexts verwaltet wird (bspw. Dokument wird vor Ort eingescannt, im Zuge einer Dokumentenbearbeitung im Primärsystem verändert oder in einem Archivsystem abgelegt). Das Primärsystem soll das Hochladen eines einzelnen Dokuments und von mehreren Dokumenten im Stapel ermöglichen.

Das Hochladen eines Dokuments soll im Hintergrund laufen. Der Nutzer soll seine Arbeit mit dem Primärsystem nicht unterbrechen müssen, während ein Dokument hochgeladen wird. Das ePA-Aktensystem übernimmt automatisch eine Versionierung von Dokumenten, wenn diese mit der replace Operation hochgeladen werden. Ob ein Dokument ersetzt werden soll, entscheidet der Nutzer des Primärsystems aus fachlichen Erwägungsgründen.

Die Metadaten des Dokuments sollen mit den im Primärsystem hinterlegten Stammdaten des Leistungserbringenden und der Leistungserbringerinstitution vorbefüllt sein. Die Datenfelder sollen vor dem Versand und Hochladen durch den Nutzer änderbar sein. Aus der Eingabemaske heraus oder mithilfe einer Dialogstrecke sollen fehlende Metadatenfelder manuell belegt werden können. Das Primärsystem kann dem Nutzer auch die Möglichkeit zur Anlage von Metadatentemplates für gängige Dokumente aus dem Versorgungsalltag der Leistungserbringerinstitution bereitstellen, um beim

Hochladen eine Auswahl treffen zu können ohne durch die unterschiedlichen Metadatenfelder gehen zu müssen.

Eine Darstellung, wie die Option zum Hochladen eines Dokuments in das ePA-Aktenkonto standardmäßig als ausgewählt angezeigt werden kann, kann Abbildung 21 entnommen werden.

Hinweise:

1. *Das Hochladen mehrerer Dokumente kann in einem einzelnen SubmissionSet erfolgen.*
2. *Es ist erlaubt, dass Dokumente von berufsmäßigen Gehilfen in ein ePA-Aktenkonto hochgeladen werden dürfen. Da die Zugriffsbefugnis für die Leistungserbringerinstitution gilt und sich diese mittels SMC-B dem ePA-Aktensystem gegenüber kenntlich macht, kann die Aufgabe zum Hochladen von Inhalten einrichtungsintern geregelt werden.*
3. *Es ist vorgesehen, dass das ePA-Aktensystem und das Primärsystem Dokumente auf Dubletten prüfen. Hierzu werden Hash-Werte gebildet, die miteinander verglichen werden. Der Einstellversuch scheitert mit dem Fehlercode XDSDuplicateDocument. Das ePA-Aktensystem gibt im codeContext-Attribut des zurückgegebenen rs:RegistryError-Elements die Liste der UUIDs (DocumentEntry.entryUUID) der identifizierten Dokumente an. Das Primärsystem soll dem Nutzer eine verständliche Fehlermeldung anzeigen.*

Tabelle 30: Dokument hochladen aus Karteikarte - UX Optimaler Klickpfad

Titel	**ePA_DMS_4 – Dokument hochladen aus Karteikarte**
Zielstellung	Der Nutzer öffnet Karteikarte der Patient:in im Primärsystem, scannt, verändert oder archiviert ein Dokument und lässt dieses im gleichen Prozessschritt in ein ePA-Aktenkonto hochladen, insofern dem nicht widersprochen wurde.
Vorbedingung	• Der Nutzer befindet sich in der Karteikarte oder im Dokumentenmanagementkontext zu einer bestimmten Patient:in innerhalb des Primärsystems. • Alle (Pflicht-)Metadatenfelder für ein Hochladen des Dokuments in ein ePA-Aktenkonto sind belegt.
Nachbedingung	Für den Nutzer ist erkenntlich, dass das Dokument erfolgreich in das ePA-Aktenkonto hochgeladen wurde.
Klickpfad	1. Die Ärzt:in oder MFA fügt ein Dokument in die Patientenakte der Patient:in innerhalb des Primärsystem ein. 2. Es wird eine Maske oder Dialogstrecke angezeigt, mit welchen Metadaten das Dokument für die Verschlagwortung im Primärsystem und für das ePA-Aktenkonto vorbefüllt wurde. Der Nutzer hat an dieser Stelle die Möglichkeit diese zu ergänzen und bei Bedarf zu korrigieren. 3. Die Option zum Speichern in ein ePA-Aktenkonto ist standardmäßig bereits ausgewählt (und kann bei Widerspruch durch die Patient:in vom Nutzer abgewählt

	werden).
Alternative	Die Nutzerführung zum Hochladen eines Dokuments in das ePA-Aktenkonto einer Patient:in kann zusätzlich auch aus einem anderen Kontextmenü heraus gestartet werden.

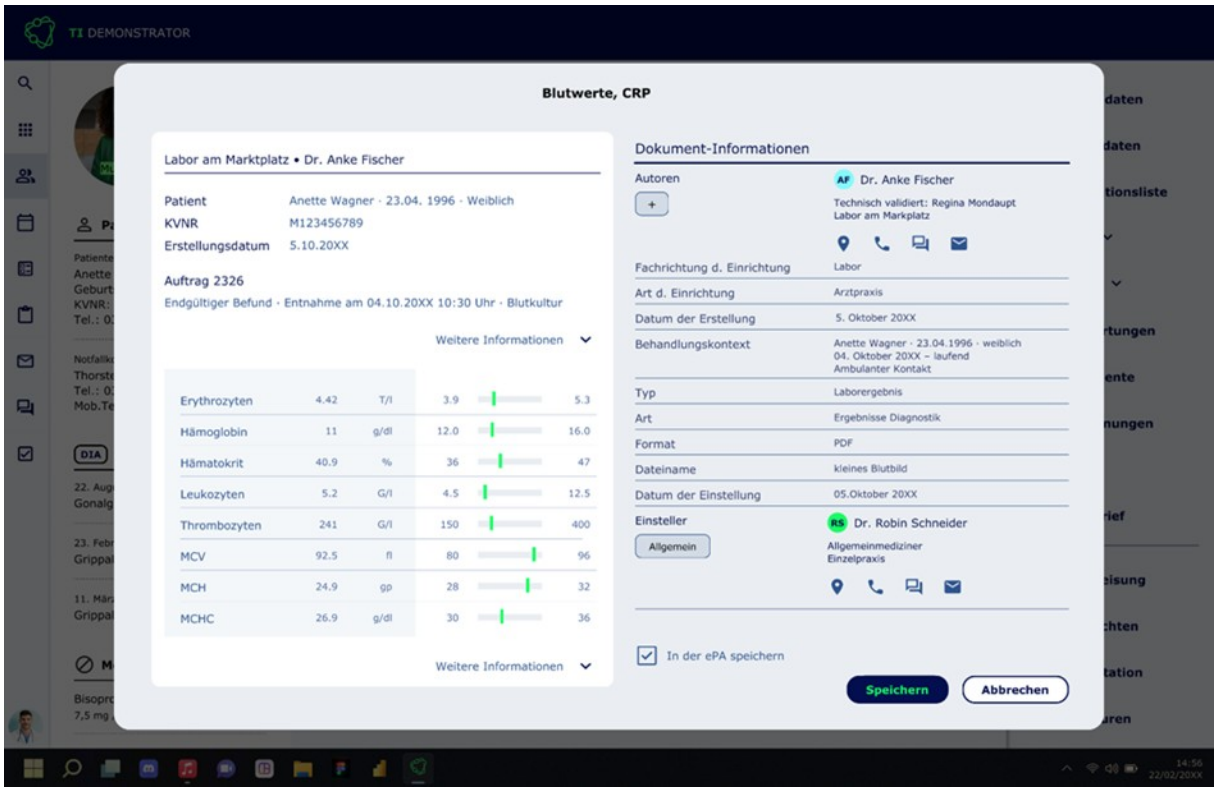

Abbildung 22: Eingabemaske mit der vorausgefüllten Einstellung, dass ein Dokument (am unteren Bildrand ist der Menüpunkt zu finden)

6.2.5 Dokument hochladen aus KIM-Workflow

Um ein oder mehrere Dokumente in das ePA-Aktenkonto der Patient:in aufwandsarm hochzuladen, soll die Funktion zum Hochladen für bestimmte Dokumente aus dem KIM-Workflow angeboten werden. In der Eingabemaske zum Versand eines eArztbriefs und einer eAU mithilfe von KIM soll die Option für das Hochladen des Dokuments in die ePA standardmäßig ausgewählt sein. Der Leistungserbringer soll die Möglichkeit haben diese Voreinstellung anzupassen. Die Voreinstellung soll differenziert für eArzbriefe einerseits und für eAU andererseits gesetzt werden können.

Die Metadaten des Dokuments sollen mit den im Primärsystem hinterlegten Stammdaten des Leistungserbringenden und der Leistungserbringerinstitution vorbefüllt sein. Die Datenfelder sollen vor dem Versand und Hochladen durch den Nutzer änderbar sein. Aus der Eingabemaske heraus oder mithilfe einer Dialogstrecke sollen fehlende Metadatenfelder manuell belegt werden können.

Bei der Erstellung einer eAU soll dem Nutzer das Datum der zuletzt ausgestellten eAU angezeigt werden, um den aktuellen Krankschreibungszeitraum erkennen zu können. Der Nutzer des Primärsystems kann dann festlegen, ab wann die neue eAU gelten soll.

Eine Darstellung, wie die Option zum Hochladen eines Dokuments in ein ePA-Aktenkonto im KIM-Workflow standardmäßig als ausgewählt angezeigt werden kann, kann Abbildung 22 entnommen werden.

Tabelle 31: Dokument hochladen aus KIM-Workflow - UX Optimaler Klickpfad

Titel	**ePA_DMS_5 - Dokument hochladen aus KIM-Workflow**
Zielstellung	Der Nutzer verschickt einen eArztbrief oder eine eAU per KIM und soll das Dokument standardmäßig in das ePA-Aktenkonto der Patient:in hochladen können, insofern dem nicht widersprochen wurde.
Vorbedingung	• Der Nutzer hat einen eArztbrief erstellt oder erstellt eine eAU per KIM. • Alle (Pflicht-)Metadatenfelder für ein Hochladen des Dokuments in ein ePA-Aktenkonto sind belegt.
Nachbedingung	• Für den Nutzer wird erkenntlich, dass das Dokument erfolgreich in das ePA-Aktenkonto hochgeladen wurde.
Klickpfad	1. Die Ärzt:in oder MFA erstellt einen eArtzbrief oder eine eAU. 2. Es wird eine KIM-Nachricht erstellt mit dem eArztbrief oder der eAU im Anhang. 2. Es wird eine Maske angezeigt, mit welchen Metadaten das Dokument für die Verschlagwortung im Primärsystem und in der ePA vorbefüllt wurde. Der Nutzer hat an dieser Stelle die Möglichkeit diese bei Bedarf zu korrigieren. 3. Die Option zum Speichern in der ePA ist standardmäßig ausgewählt (und kann bei Widerspruch durch die Patient:in abgewählt werden).
Alternative	Die Nutzerführung zum Hochladen eines Dokuments in die ePA einer Patient:in kann zusätzlich auch aus einem anderen Kontextmenü heraus gestartet werden.

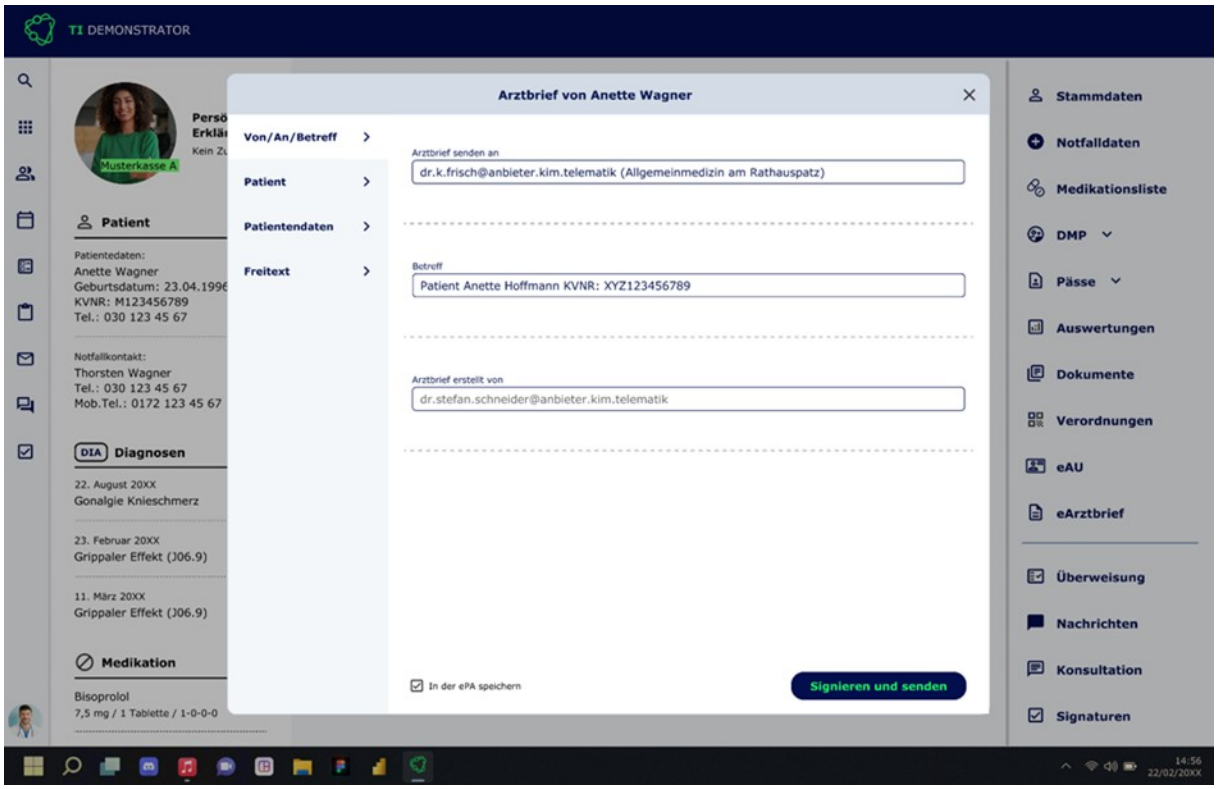

Abbildung 23: Option zum Hochladen eines Dokuments im Falle des Versands eines eArztbriefs oder einer eAU im Rahmen des KIM-Workflows ist standardmäßig ausgewählt

6.3 FHIR Medication Service: Digital gestützter Medikationsprozess in der elektronischen Patientenakte

Das Primärsystem soll über den Information Service prüfen, ob der Versicherte am digital gestützten Medikationsprozess (dgMP) teilnimmt. Das Ergebnis soll im Primärsystem persistiert werden. Wenn der Versicherte am dgMP teilnimmt, kann der FHIR Medication Service auf verschiedene Arten angesprochen werden.

Das ePA-Aktensystem bietet dem Primärsystem die Möglichkeit die elektronische Medikationsliste (eML) als PDF oder xHTML anzuzeigen (siehe Tabelle 9). Wenn die eML als PDF angezeigt wird (siehe Abbildung 23), dann übernimmt das ePA-Aktensystem die Erstellung der Liste. Die Nutzer des Primärsystems ist mithilfe der eML als PDF in der Lage die Informationen der Liste zur Kenntnis zu nehmen und bspw. dargestellte Informationen wie eine PZN für die Ausstellung eines E-Rezepts im Verordnungsmodul zu übernehmen.

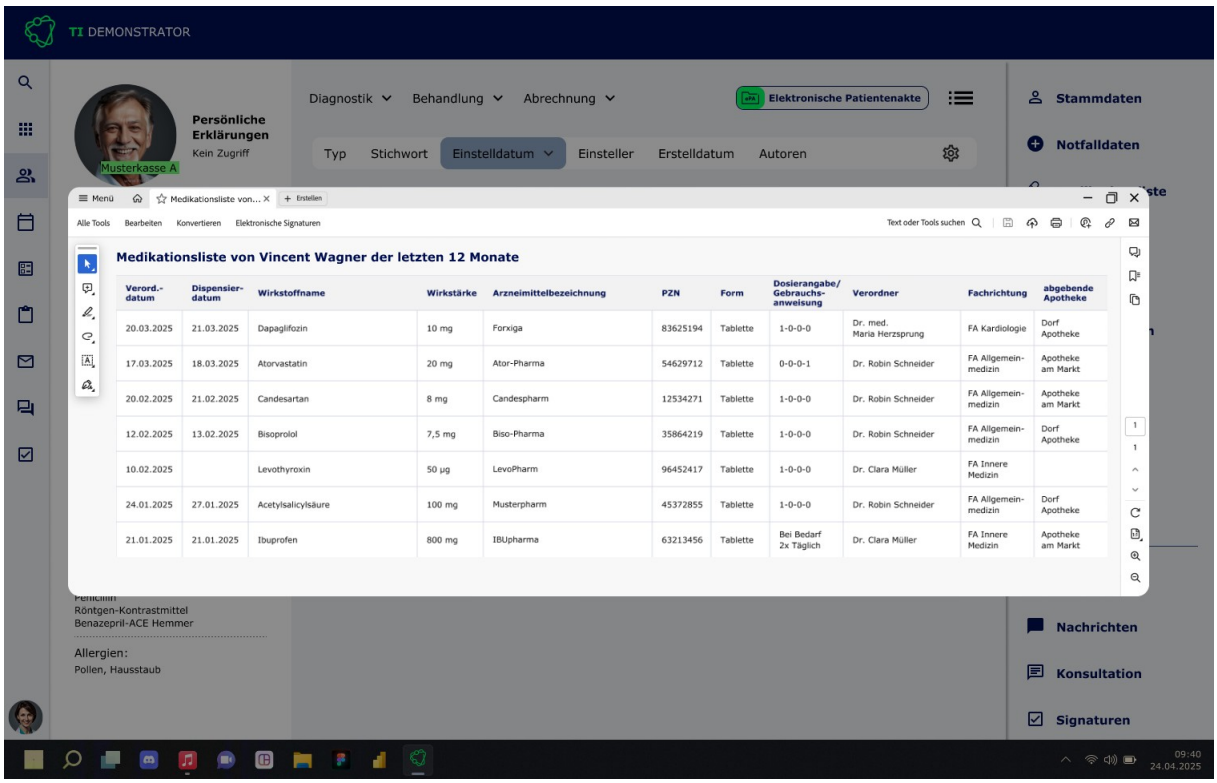

Abbildung 24 : Medikationsliste als PDF

Das ePA-Aktensystem bietet dem Primärsystem auch die Möglichkeit die Verordnungs- und Dispensierdaten im nativen FHIR-Format zu übernehmen (siehe Tabelle 10). Wenn die eML basierend auf nativen FHIR Resourcen angezeigt wird (siehe Abbildung 24), dann übernimmt das Primärsystem die Erstellung der Liste.

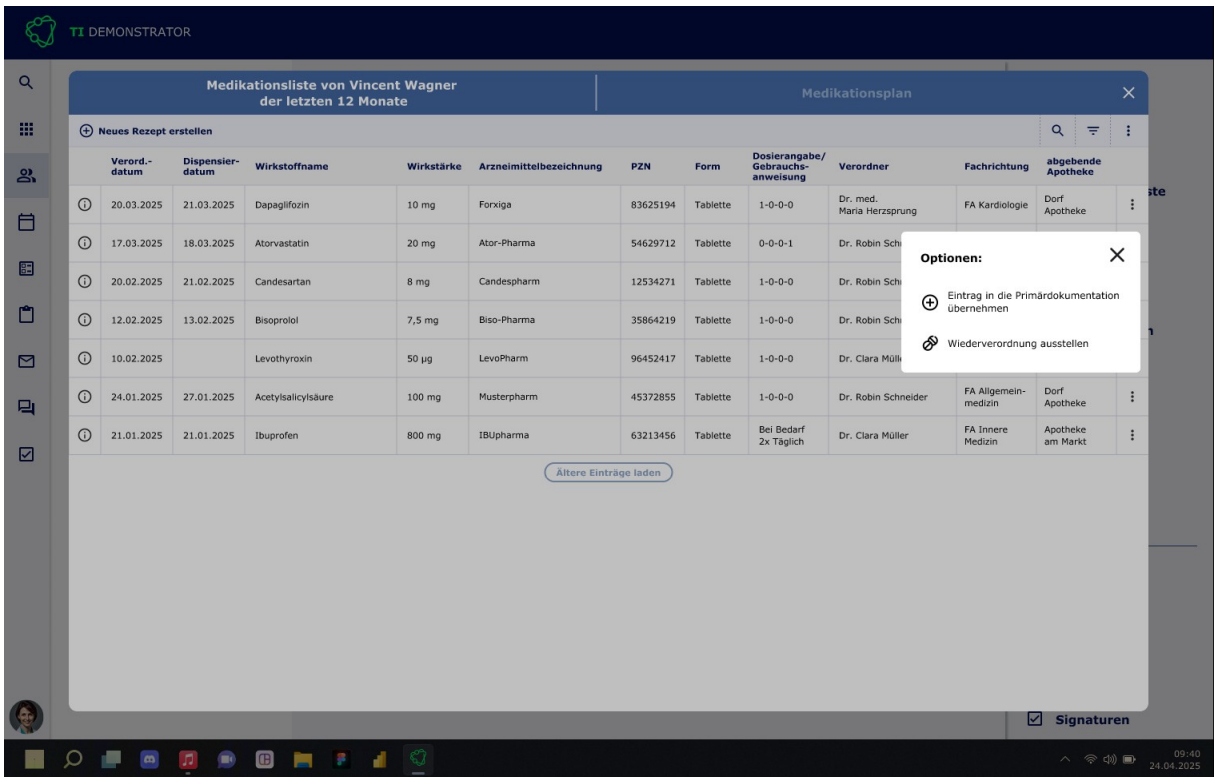

Abbildung 25 : Medikationsliste on FHIR

Der Nutzer des Primärsystems ist mithilfe der eML on FHIR in der Lage die Informationen der Liste zur Kenntnis zu nehmen und bekommt vom Primärsystem idealerweise zusätzliche Operationen angeboten:

- Das Primärsystem kann Einträge der eML, die sich im Vergleich zur letzten abgerufenen eML geändert haben (Aktualisierungen) bzw. Einträge, die noch nicht in der Primärdokumentation enthalten sind, visuell hervorheben.
- Das Primärsystem kann benutzerdefinierte individuelle Darstellungsmöglichkeiten unterstützen, z. B. mit der Möglichkeit, Details zu einer Medikation gezielt aufzuklappen oder aus Gründen der Übersichtlichkeit zu verbergen.
- Das Primärsystem kann eine Wiederverordnung eines Medikaments direkt auf Basis der Daten anbieten. Der sich anschließende Verordnungsprozess erfolgt dann wie gewohnt.
- Das Primärsystem kann es einem Nutzer ermöglichen, mit einem Klick ein oder mehrere Einträge aus der eML in die Primärdokumentation zu übernehmen.
- Das Primärsystem kann die Funktionen Suche, Filtern und Sortieren in der eML ermöglichen. Dabei kann sowohl eine einfache Suche (ein Suchfeld und alles wird durchsucht) als auch die gezielte Suche und das Filtern von einzelnen Informationen angeboten werden sein (z.B. nur die Medikation der letzten drei Monate oder alle Verordnungen eines bestimmten Leistungserbringers).

Eine detaillierte Beschreibung des dgMP und der FHIR Operationen finden sich unter:

- https://simplifier.net/epa-medication

Die gematik empfiehlt allen Primärsystemherstellern eine native Umsetzung und die Benutzung der FHIR Schnittstelle, um Mehrwertfunktionen zu ermöglichen.

7 Fehlerbehandlung

7.1 Fehlermeldungen der REST-Schnittstellen

Für jede REST-Schnittstelle sind in der OpenAPI die möglichen Fehlersituationen beschrieben. In dieser Tabelle werden Beispiele gezeigt und ein Vorschlag für den Hinweis an Nutzer gemacht:

Tabelle 32: Tab_ILF_ePA- Beispiele für REST-Fehlermeldungen

Situation	Status Code	ErrorCode	Vorschlag für Hinweis an den Nutzer
Response ok, content	200		
Response ok, resource created	201		
Response ok, no content	204		
invalid parameters invalid request body (schema)	400	malformedRequest	Meldung an den technischen Service
Requestor role is not in the list of allowed usergroups	403	invalidOid	Der gewünschte Aktenzugriff ist für diese Berufsgruppe nicht erlaubt
HSM verification failed	403	invalidToken	Aktion wiederholen, bei Misserfolg Meldung an den technischen Service
Requestor has no valid entitlement	403	notEntitled	Die Praxis ist nicht befugt auf das Aktenkonto zuzugreifen. Versichertenkarte einlesen oder Versicherten bitten, die Praxis für den Zugriff zu befugen.
Invalid request, bearerToken is invalid by means of HSM rule 'rr0' or timestamp	403	invalAuth	Aktion wiederholen, bei Misserfolg Meldung an den technischen Service
Health record	404	noHealthRecord	Das Aktenkonto existiert nicht (mehr).

does not exist			
Health record is not in state ACTIVATED	409	statusMismatch	Das Aktenkonto befindet sich im Umzug, ca. 24 warten
the insurant objects to the medication process	423	Locked	Versicherter nimmt nicht am Medikationsprozess teil
any other error	500	internalError	Aktion wiederholen nach ca. 10 Minuten, sonst Meldung an den technischen Service

Bei den FHIR-Schnittstellen werden die Fehlermeldungen mit einem Operation Outcome gemäß https://hl7.org/fhir/R4/operationoutcome.html gebildet.

7.1.1 Fehlerbehandlung im XDS Document Service

Auftretende Fehlertypen unterscheiden sich je nach Architekturebene:

- http-Fehler auf Transportebene
- Fehler auf Ebene des Dokumentenmanagements und der Aktenermittlung.

Tabelle 33: Tab_ILF_ePA_DifferenzFehlerhandling

Aspekt	IHE-Error
Fehlercodes	als String mit Kurzbeschreibung
Fehlerlisten	`RegistryErrorList`
Kritikalität Warning	`RegistryErrorList.highestSeverity="Warning"`
Kritikalität Error	`RegistryErrorList.highestSeverity="Error"`
SOAP-Fehlertyp	SOAP 1.2

A_14179 - Verständliche Fehlermeldung
Das PS MUSS im Falle von Fehlern Fehlermeldungen bereitstellen, die es den Mitarbeitern der Leistungserbringerinstitution ermöglichen, die Ursache des Fehlers zu identifizieren und mögliche Gegenmaßnahmen zu ergreifen.**[<=]**

7.1.2 IHE-Error

In der Response der IHE-Schnittstellen-Aufrufe können [ITI-TF-3#Table 4.2.4.1-2]: Error Codes auftreten, die drei ResponseStatusType aufweisen können.

Das Vorhandensein einer Error-List ist prinzipiell vereinbar mit einer teilweise erfolgreichen Verarbeitung. Falls die ErrorList nur Warnings enthält

(RegistryError elements mit warning severity, aber ohne error severity), kann die Verarbeitung als erfolgreich angesehen werden.

Fehler aus Aufrufen des Dokumentenmanagements haben das in [ITI TF Vol 3#4.2.4] "Success and Error Reporting" beschriebene Format. Es wird im Fehlerfall ggf. eine Fehlerliste (`RegistryErrorList`) und darin Fehler (`RegistryError`) mit den Attributen `errorCode`, `errorContext`, `codeContext` und `severity` zurückgegeben.

Für die Analyse der Fehlerquelle enthält insbesondere auch der `codeContext` hilfreiche Informationen, um den Nutzer über die Ursache des Fehlers hinzuweisen und daraus Handlungen abzuleiten, mit denen die Ursache des Fehlers behoben wird.

A_14691 - Meldung über partielle Erfolgsmeldungen
Das PS MUSS im Falle einer partiellen Erfolgsmeldung (oder eines vorliegenden Warning-Elementes) eine Warnung bereitstellen, die es den Mitarbeitern der Leistungserbringerinstitution ermöglichen, die Ursache des (partiellen) Fehlers zu identifizieren und mögliche Gegenmaßnahmen zu ergreifen und die partiellen Fehler vom partiellen Erfolg unterscheiden helfen. **[<=]**

Bei IHE-Operationen stellt der in Im rs:RegistryResponse/@status Attribut den Verarbeitungsstatus der Anfrage dar:

Tabelle 34: Tab_ILF_ePA_IHE_Success_and_Error_Reporting

Wert	Beschreibung	Erläuterung	Beispiel Anzeigetext
urn:ihe:iti:2007:ResponseStatusType:PartialSuccess	[IHE-ITT-TF3]#Table 4.2.4.2-3, 4.2.4.2-4.	In der Response einer Transaktion sind Error-Elemente enthalten, mindestens eines davon hat die Error Severity. Andere Teile der Transaktion sind erfolgreich verlaufen.	Transaktion in Teilen erfolgreich
urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Failure	[IHE-ITT-TF3#Table 4.2.4.2-1, 4.2.4.2-3,4.2.4.2-4]	Transaktion gescheitert	Der ePA-Anwendungsfall konnte nicht erfolgreich beendet werden.

A_14920 - Fehlertexte aus der RegistryErrorList zur Anzeige von Fehlertexten
Das PS SOLL für Fehler aus der `RegistryErrorList` eine deutschsprachige Fehlermeldung erstellen.**[<=]**

A_15092 - Eigene Übersetzungen von Fehlertexten
Das PS KANN die IHE-Error-Fehlertexte mit eigenen Übersetzungen zur Anzeige bringen. Andernfalls KANN der Fehlertext für Fehler, bei denen keine Handlungsanweisung besteht, mit dem generischen Fehlertext "Der ePA-Anwendungsfall konnte nicht erfolgreich beendet werden." zur Anzeige gebracht werden.**[<=]**

7.1.3 Fehlermeldungen aus dem XDS Document Service

Das Aktensystem kann mindestens die Fehler der Tabelle Tab_ILF_ePA_IHE-Fehlermeldungen_Aktensystem werfen, die an das PS durchgereicht werden.

Tabelle 35: Tab_ILF_ePA_IHE-Fehlermeldungen_Aktensystem

Code	Hinweis	Referenz
InvalidDocumentContent	Dokument passt nicht zu Metadaten	[gemSpec_Aktensystem_ePAfuerAlle#A_24512*] [IHE-ITI-TF3#4.2.4]
PolicyViolation	Zugriffsunterbindungsregeln wurden verletzt	[gemSpec_Aktensystem_ePAfuerAlle#A_24509*]
UnresolvedReferenceException	entryUUID kann nicht aufgelöst werden	[IHE-ITI-TF3#4.2.4]
XDSDocumentUniqueIdError	uniqueId kann nicht aufgelöst werden, weil Dokument verborgen	[gemSpec_Aktensystem_ePAfuerAlle#A_24510*] [IHE-ITI-TF3#4.2.4]
XDSDuplicateUniqueIdInRegistry	uniqueId ist nicht eindeutig	[IHE-ITI-TF3#4.2.4]
XDSMissingDocument	Dokument zu den Metadaten fehlt	[IHE-ITI-TF3#4.2.4]
XDSMissingDocumentMetadata	Metadaten zum Dokument fehlen	[IHE-ITI-TF3#4.2.4]
XDSPatientIdDoesNotMatch	PatientID fehlt	[IHE-ITI-TF3#4.2.4]
XDSRegistryBusy	Zu viele Aktivitäten in der Registry	[IHE-ITI-TF3#4.2.4]
XDSRepositoryBusy	Zu viele Aktivitäten	[IHE-ITI-TF3#4.2.4]
XDSRegistryError	interner Fehler	[IHE-ITI-TF3#4.2.4]
XDSRepositoryError	interner Fehler	[IHE-ITI-TF3#4.2.4]
XDSRegistryMetadataError	Fehlerhafte Metadaten	[IHE-ITI-TF3#4.2.4] Der codeContext kann je nach Anwendungsfall

		zusätzliche Informationen liefern: - Metadatenattribut, welches nicht den Nutzungsvorgaben entspricht (A_14938*) - im codeContext-Attribut kann im zurückgegebenen XDSRepositoryMetadataError-Element der Text „Version of submitted structured document is not supported“ zurückgegeben werden (A_23098*).
XDSRepositoryMetadataError	Fehlerhafte Metadaten	[IHE-ITI-TF3#4.2.4]
XDSRegistryNotAvailable	Fehler Zugriff Registry	[IHE-ITI-TF3#4.2.4]
XDSRegistryOutOfResources	Resourcenengpass	[IHE-ITI-TF3#4.2.4]
XDSRepositoryOutOfResources	Resourcenengpass	[IHE-ITI-TF3#4.2.4]
XDSStoredQueryMissingParam	Parameterfehler Stored Query	[IHE-ITI-TF3#4.2.4]
XDSStoredQueryParamNumber	Parameterfehler Stored Query	[IHE-ITI-TF3#4.2.4]
XDSTooManyResults		Tab_ILF_ePA_Fehlerbehandlung_Dokumente_Suchen
XDSUnknownStoredQuery	Fehlerhafte Stored Query	[IHE-ITI-TF3#4.2.]
XDSUnreferencedObjectException	Fehler beim Löschen von Dokumenten	[gemSpec_Aktensystem_ePAfuerAlle#A_24511*] [IHE-ITI-TF3#4.2.4]

7.2 Umgang mit Fehlern in der Leistungserbringerinstitution

Da vom Nutzer des Primärsystems kein technisches Vorwissen erwartet werden darf, sind Fehlermeldungen so anzugeben, dass dieser nach Möglichkeit darauf reagieren kann. Eine Fehlermeldung muss nicht die von der Quelle erzeugte technische Fehlermeldung darstellen und dem Nutzer dennoch nach Möglichkeit mitteilen, welches System im Prozess den Fehler verursacht hat. Mit der Fehlermeldung sollen dem Nutzer Handlungsempfehlungen vorgeschlagen werden, um den Fehler zu beseitigen. Es ist darüber hinaus möglich, technische Details an den technischen Support zu übermitteln.

Gemäß gemKPT_Betr kann ein Dienstleister vor Ort (DVO) den Nutzer des Primärsystems bei der Problembehebung in der Leistungserbringerinstitution unterstützen. Störungsmeldungen werden durch den DVO über den User Help Desk (UHD) des VPN-Zugangsdienstes qualifiziert weitergeleitet. Sofern dieser die Störung nicht beheben

kann, erfolgen die Erstellung und die Weitergabe eines Tickets über das TI-ITSM-System an den Single Point of Contact (SPOC) des lösungsverantwortlichen Anbieters.

Von zentraler Seite wird das TI-ITSM (die ZIS) bereitgestellt um vor allem Störungen, Probleme und Änderungen zu managen und Service Requests abzusetzen. Zugang zum TI-ITSM haben in der Regel Anbieter bzw. deren Betreiber in der TI. Üblicherweise ist derjenige an das TI-ITSM angebunden, der die operative Betriebsleistung erbringt und dadurch schnell reaktions- und auskunftsfähig ist. Einige Hersteller (z.B. Konnektorhersteller oder PS-Hersteller) sind freiwillig im TI-ITSM um Probleme und Störungen schnell und direkt adressieren zu können.

Bei der Erfassung eines Tickets ist wichtig, dass beim Autor ein umfassendes Verständnis der Zusammenhänge vorhanden ist, damit bereits vom Client all die Informationen erhoben werden, die später für die Entstörung wichtig sein könnten. So ist z.B. wichtig zu erfassen, bei welcher Krankenkasse ein Versicherter (bei dem die Störung aufgetreten ist) versichert ist, da sonst nicht klar ist, welches Aktensystem angesprochen werden muss. Nur mit umfassendem Verständnis der Produktabhängigkeiten können von vornherein die richtigen potenziellen Ursachen identifiziert und vielversprechende Lösungsverantwortliche adressiert werden. Die Erfassung der relevanten Informationen ist umso wichtiger, wenn die Störsituation nicht oder nur schwer nachgestellt werden kann (z.B. weil der Versicherte die Praxis bereits verlassen hat).

Der Anwender erhält nach Lösung seiner Störung über seinen UHD eine Rückantwort (siehe Abbildung 25). Der UHD verantwortet demnach die Behebung von Störungen, die von Nutzern gemeldet werden.

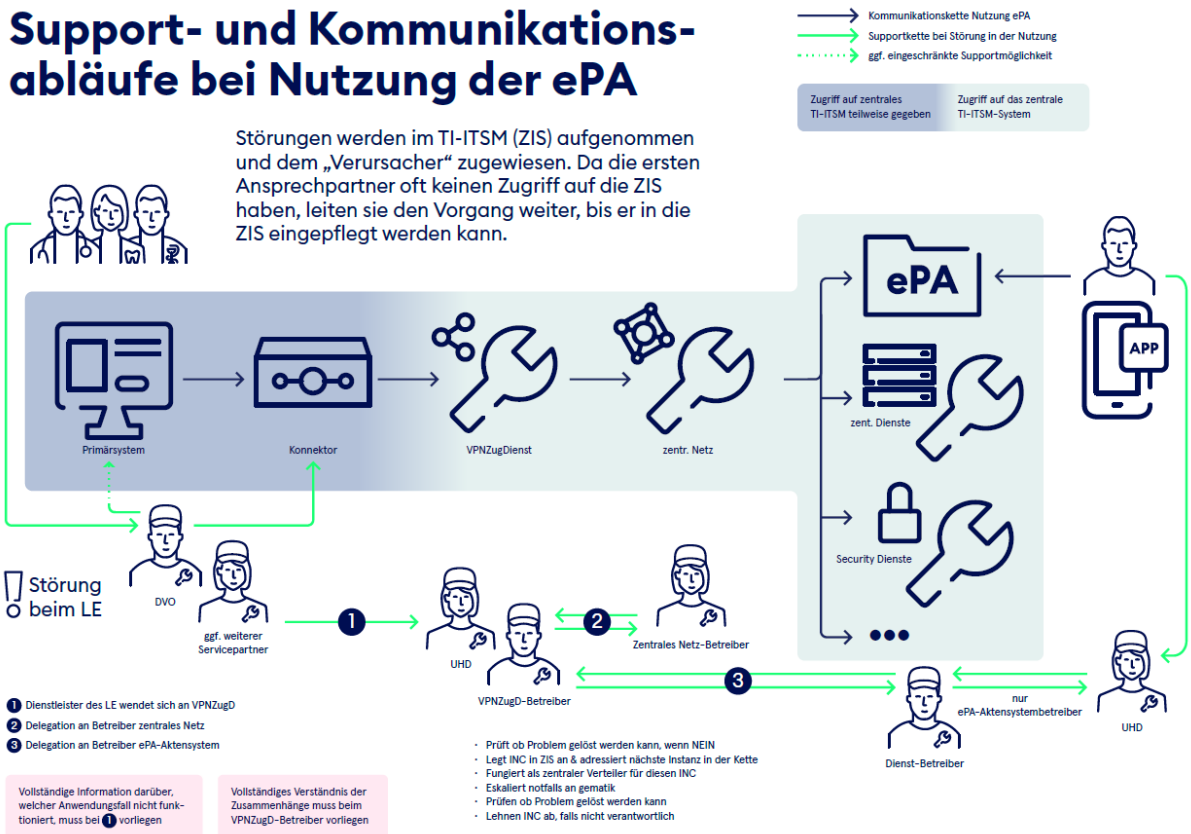

Abbildung 26: Support- und Kommunikationsabläufe bei Nutzung der ePA

8 Anhang A – Verzeichnisse

8.1 Abkürzungen

Kürzel	Erläuterung
AS	Aktensystem
BAG	Berufsausübungsgemeinschaft
CS	Clientsystem
DTBS	Data To Be Signed - zu signierende Daten
DTBSR	Data to be Signed Representation - maschinenlesbare Repräsentation der zu signierenden Daten
eML	elektronische Medikationsliste
FdV	Frontend des Versicherten gemäß gemSpec_ePA_FdV
KT	Kartenterminal
PS	Primärsystem
PTSB	Produkttypsteckbrief
TLS	Transport Layer security
Versicherten-ID	10-stelliger unveränderlicher Teil der 30-stelligen Krankenversicherungsnummer
VAU	Vertrauenswürdige Ausführungsumgebung

8.2 Glossar

Begriff	Erläuterung
Behandlungskontext	Ein Behandlungskontext beginnt, wenn sich der Patient bzw. die Patientin gegenüber der Leistungserbringerinstitution mittels elektronischer Gesundheitskarte oder digitaler Identität identifiziert hat. Er ist die Voraussetzung für den Zugriff einer LEI auf die ePA für alle. Der Behandlungskontext dauert je nach Rolle standardmäßig 3 oder 90 Tage und kann vom Versicherten über die ePA App jederzeit beendet werden oder auf einen beliebigen Zeitraum ausgeweitet werden.

ePA-Frontend des Versicherten	Softwareprogramm in der Verfügung des Versicherten, ausgestattet mit einer grafischen Benutzeroberfläche zum Starten fachlicher Anwendungsfälle der ePA und Darstellung des Ergebnisses der Anwendungsfälle.
Funktionsmerkmal	Der Begriff beschreibt eine Funktion oder auch einzelne, eine logische Einheit bildende Teilfunktionen der TI im Rahmen der funktionalen Zerlegung des Systems.
Ombudsstelle	Mit der ePA für alle gibt es neu die Ombudstelle: Jede Krankenkasse richtet eine Ombudsstelle ein. Diese haben zum Zweck den Versicherten zu allen Fragen, Anliegen und Problemen, die ePA für alle betreffend zu beraten. Zusätzlich dürfen diese Stellen Widersprüche, die ePA für alle betreffend annehmen und im Namen des Versicherten im Aktensystem durchsetzen. Weiterhin ist es ihnen erlaubt Protokolldaten abzurufen und dem Versicherten über ein, von der Krankenkasse festgelegtes, Verfahren zukommen zu lassen.

Das Glossar wird als eigenständiges Dokument, vgl. [gemGlossar] zur Verfügung gestellt.

8.3 Abbildungsverzeichnis

8.4 Tabellenverzeichnis

8.5 Referenzierte Dokumente

8.5.1 Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert. Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument passende jeweils gültige Versionsnummer sind in der aktuellsten, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber: Titel

[gemGlossar]	gematik: Glossar der Telematikinfrastruktur
[gemKPT_ePAfuerAlle]	gematik: Grobkonzept der "ePA für alle"
[gemSpec_Aktensystem_ePAfueralle]	gematik: Spezifikation gemSpec_Aktensystem_ePAfueralle
[gemSpec_Krypt]	gematik: Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_EPAAuditEvent]	Datenstruktur für Audit-Protokolle im Aktensystem: https://gematik.de/fhir/epa/StructureDefinition/EPAAuditEvent
[gemSpec_Kon]	gematik: Spezifikation Konnektor
[gemSpec_VZD_FHIR_Directory]	gematik: Spezifikation Verzeichnisdienst FHIR-Directory
[gemSpec_IDP_Frontend]	gematik: Spezifikation Identity Provider – Frontend
gemSpec_IDP_Dienst]	gematik: Spezifikation Identity Provider-Dienst
[gemSpec_OM]	gematik: Übergreifende Spezifikation Operations und Maintenance
[gemSpec_PKI]	gematik: Spezifikation PKI
[gemSpec_Voc_ePA]	gematik: Vocabulary ePA GitHub: https://github.com/gematik/ePA-XDS-Document Path: src/vocabulary
[gemSpec_IG_ePA]	gematik: Implementation Guides für strukturierte Dokumente GitHub: https://github.com/gematik/ePA-XDS-Document Path: src/implementation_guides
[I_Information_Service]	gematik: I_Information_Service REST-Schnittstelle zum Abruf Informationen zu einem Aktenkonto GitHub: https://github.com/gematik/ePA-Basic Path: src/openapi/I_Information_Service.yaml
[I_Authorization_Service]	gematik: I_Authorization_Service REST-Schnittstelle zur Nutzerauthentifizierung GitHub: https://github.com/gematik/ePA-Basic Path: src/openapi/I_Authorization_Service.yaml
[I_Entitlement_Management]	gematik: I_Entitlement_Management REST-Schnittstelle zur Verwaltung von Befugnissen und Befugnisausschlüssen GitHub: https://github.com/gematik/ePA-Basic Path: src/openapi/I_Entitlement_Management.yaml

[I_Health_Record_Relocation_Service]	gematik: I_Health_Record_Relocation_Service REST-Schnittstelle zum Aktenumzug GitHub: https://github.com/gematik/ePA-Basic Path: src/openapi/I_Health_Record_Relocation_Service.yaml
[I_Consent_Decision_Management]	gematik: I_Consent_Decision_Management REST-Schnittstell zum Management der Widersprüche zu Versorgungsprozessen GitHub: https://github.com/gematik/ePA-Basic Path: src/openapi/I_Consent_Decision_Management.yaml
[I_Audit_Event]	gematik: I_Audit_Event REST-Schnittstelle (FHIR-Service) zum Abruf der Protokolldaten GitHub: https://github.com/gematik/ePA-Basic Path: src/openapi/I_Audit_Event.yaml
[I_Audit_Event_Render]	gematik: I_Audit_Event_Render REST-Schnittstelle (FHIR-Service) zum Abruf der gerenderten Protokolldaten GitHub: https://github.com/gematik/ePA-Basic Path: src/openapi/I_Audit_Event_Render.yaml
[I_Email_Management]	gematik: I_Email_Management REST-Schnittstelle zum Management von email-Adressen eines Versicherten GitHub: https://github.com/gematik/ePA-Basic Path: src/openapi/I_Email_Management.yaml
[PHR_Common.xsd]	Schemadefinition für einen Arztbrief nach § 383 SGB V GitHub: https://github.com/gematik/ePA-XDS-Document Path: src/schema/PHR_Common.xsd
[IG_Patient_Information_Service]	gematik: FHIR Implementation Guide "Patient Information Service" Simplifer: https://simplifier.net/guide/patient-information-service?version=current
[IG_Medication_Service]	gematik: FHIR Implementation Guide "Medication Service" Simplifier: https://simplifier.net/guide/medication-service?version=current

8.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[BasicProfile1.2]	Basic Profile Version 1.2 http://www.ws-i.org/Profiles/BasicProfile-1.2-2010-11-09.html

[BasicProfile2.0]	Basic Profile Version 2.0 http://ws-i.org/Profiles/BasicProfile-2.0-2010-11-09.html
[IHE-ITI-RMD], enthält [ITI-62], [ITI-86]	IHE International (2023): IHE IT Infrastructure (ITI) Technical Framework Supplement, Remove Metadata and Documents (RMD), Revision 1.6 – Trial Implementation, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RMD.pdf
[IHE-ITI-RMU], enthält [ITI-92]	IHE International (2021): IHE IT Infrastructure (ITI) Technical Framework Supplement, Restricted Metadata Update (RMU), Revision 1.3 – Trial Implementation, https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RMU.pdf
[IHE-ITI-TF1]	IHE International (2023): IHE IT Infrastructure (ITI) Technical Framework, Volume 1 (ITI TF-1) – Profile definition, use-case analysis, actor definition, and use of transactions and content, Revision 20.0, https://profiles.ihe.net/ITI/TF/Volume1/
[IHE-ITI-TF2a], enthält [ITI-18]	IHE International (2023): IHE IT Infrastructure (ITI) Technical Framework, Volume 2 (ITI TF-2) – Transaction definitions and constraints, Revision 20.0, https://profiles.ihe.net/ITI/TF/Volume2/
[IHE-ITI-TF-2b], enthält [ITI-38], [ITI-39], [ITI-41], [ITI-43], [ITI-45]	IHE International (2023): IHE IT Infrastructure (ITI) Technical Framework, Volume 2 (ITI TF-2) – Transaction definitions and constraints, Revision 20.0, https://profiles.ihe.net/ITI/TF/Volume2/
[IHE-ITI-TF2x]	IHE International (2023): IHE IT Infrastructure (ITI) Technical Framework, Volume 2 (ITI TF-2) – Transaction definitions and constraints, Revision 20.0, https://profiles.ihe.net/ITI/TF/Volume2/
[IHE-ITI-TF3]	IHE International (2023): IHE IT Infrastructure (ITI) Technical Framework, Volume 3 (ITI TF-3) – Cross-Document Sharing Metadata and Content Profiles, Revision 20.0, https://profiles.ihe.net/ITI/TF/Volume3/
[IHE-ITI-VS]	IHE Deutschland (2021): Value Sets für Aktenprojekte im deutschen Gesundheitswesen, Implementierungsleitfaden, Version 3.0 http://www.ihe-d.de/projekte/xds-value-sets-fuer-deutschland/
[KBV Portal]	Portal der Kassenärztliche Bundesvereinigung https://kbv.de
[KDL-ILF]	DVMD: KDL Implementierungsleitfaden https://simplifier.net/guide/KDL-Implementierungsleitfaden-2024/Hauptseite/ConceptMap-2024/MappingvonKDLnachIHEClassCode-2024.page.md?version=current und https://simplifier.net/kdl/kdl-ihe-typecode und https://simplifier.net/kdl/kdl-ihe-classcode

[MTOM]	W3C (2005): SOAP Message Transmission Optimization Mechanism, https://www.w3.org/TR/soap12-mtom/
[Richtlinie eArztbrief]	Kassenärztliche Bundesvereinigung (2021): Richtlinie über die Übermittlung elektronischer Briefe in der vertragsärztlichen Versorgung gemäß § 383 SGB V, Richtlinie Elektronischer Brief https://www.kbv.de/media/sp/RL-eArztbrief.pdf
[SOAP]	W3C (2007): SOAP Version 1.2 Part 1: Messaging Framework (Second Edition), https://www.w3.org/TR/soap12-part1/
[VHITG_AB]	VHTIG (2006), Arztbrief auf Basis der HL7 Clinical Document Architecture Release 2 für das Deutsche Gesundheitswesen, Implementierungsleitfaden, Version 1.50, http://download.hl7.de/documents/cdar2-arztbrief/Leitfaden-VHitG-Arztbrief-v150.pdf
[DKG_Übermittlung_MD]	DKG (2022): Anhang 1 zur Technischen Anlage zur elektronische-Vorgangsübermittlung-Vereinbarung – eVV https://www.dkgev.de/fileadmin/default/Mediapool/2_Themen/2.1_Digitalisierung_Daten/2.1.3._Elektronische_Datenuebermittlung/2.1.3.4._Datenuebermittlung_mit_dem_MD/2022_04_29_DTA_MD-KH_eVV_Anlage_1_Anhang_V.1.2_final.pdf

9 Anhang B - Vorschläge zur verkürzten Ansicht der Auswahl von Werten aus Value Sets

Die in [gemSpec_Voc_ePA] vorgegebenen Value Sets beinhalten in der Regel eine hohe Anzahl von Werten, die nicht für jeden Sektor oder jede Berufsgruppe gleichermaßen relevant sind. Um dem Anwender die Nutzung zu erleichtern, wird für die Auswahl der Werte die Anzeige einer gefilterten Ansicht der Tabellen empfohlen.

Hinweis: Neue Nutzergruppen, die im Folgenden noch nicht berücksichtigt sind, sollten sich nach Vorbild der vorliegenden Vorschläge eine verkürzte Ansicht bilden. Neue Nutzergruppen werden schrittweise auch explizit Berücksichtigung finden.

Tabelle 36: Value Set authorRole

Code	Anzeigename	Code-System	Arzt / Rolle Med	Zahnarzt	Krankenhaus	Apotheke
1	Einweiser	Prozessrollen für Autoren (OID 1.3.6.1.4.1.19376.3.276.1.5.13)	x	x		
2	Entlassender				x	
3	Überweiser		x	x		
4	Durchführender		x	x	x	x
5	durchführendes Gerät					
6	Betreuer					
7	Pflegender					
17	Begutachtender					
8	Behandler		x	x	x	
9	Erstbehandler		x	x		

	außerhalb einer Einrichtung					
10	Bereitstellender					
11	Dokumentierender		x	x	x	x
12	dokumentierendes Gerät					
13	Validierer					
14	Gesetzlich Verantwortlicher					
15	Beratender					
16	Informierender					
101	Hausarzt	Patientenbeziehungsrollen für Autoren (OID 1.3.6.1.4.1.19376.3.276.1.5.14)	x			
102	Patient					
103	Arbeitgebervertreter					
104	Primärbetreuer (langfristig)		x	x		x
105	Kostenträgervertreter					

Tabelle 37: Value Set authorSpecialty

Code	Anzeigename	Code-System	Arzt	Zahna	Kranken	Apoth

			/ Rolle Med	rzt	haus	eke
11001	FA Allgemeinmedizin	Facharzttitel der Ärztekammern (OID: 1.2.276.0.76.5.514)	x		x	
12901	SP Geriatrie					
21001	FA Anästhesiologie				x	
21002	FA Anästhesiologie und Intensivtherapie					
31001	FA Anatomie					
41001	FA Arbeitshygiene					
41002	FA Arbeitsmedizin					
51001	FA Augenheilkunde		x		x	
61001	FA Biochemie					
71107	FA Allgemeinchirurgie		x		x	
71101	FA Allgemeine Chirurgie					
71001	FA Chirurgie					
71102	FA Gefäßchirurgie				x	
71002	FA Herzchirurgie		x		x	
71202	FA Kinder- und Jugendchirurgie					

71003	FA Kinderchirurgie		x		x	
71004	FA Orthopädie					
71103	FA Orthopädie und Unfallchirurgie					
71005	FA Plastische Chirurgie					
71106	FA Plastische und Ästhetische Chirurgie				x	
71201	FA Plastische; Rekonstruktive und Ästhetische Chirurgie					
71104	FA Thoraxchirurgie				x	
71105	FA Visceralchirurgie				x	
71108	FA Viszeralchirurgie				x	
72001	SP Gefäßchirurgie					
72002	SP Rheumatologie (Orthopädie)					
72003	SP Thoraxchirurgie in der Chirurgie					
72004	SP Thoraxchirurgie in der Herzchirurgie					
72005	SP Unfallchirurgie					
72006	SP Visceralchirurgie					
73001	TG Echokardiologie herznaher Gefäße					
73002	TG Gefäßchirurgie					
730	TG Herz- und Gefäßchirurgie					

02						
930 03	TG Phoniatrie und Pädaudiologie					
101 001	FA Dermatologie und Venerologie					
101 002	FA Haut- und Geschlechtskrankheiten		x		x	
111 001	FA Humangenetik					
121 001	FA Hygiene					
121 002	FA Hygiene und Umweltmedizin					
131 001	FA Immunologie					
141 002	FA Innere Medizin		x		x	
141 110	FA Innere Medizin und Angiologie					
141 111	FA Innere Medizin und Endokrinologie und Diabetologie					
141 112	FA Innere Medizin und Gastroenterologie					
141 903	FA Innere Medizin und Geriatrie					
141 113	FA Innere Medizin und Hämatologie und Onkologie					
141 904	FA Innere Medizin und Infektiologie					
141 114	FA Innere Medizin und Kardiologie					
141 115	FA Innere Medizin und Nephrologie					

141 116	FA Innere Medizin und Pneumologie					
141 117	FA Innere Medizin und Rheumatologie					
141 102	FA Innere Medizin und Schwerpunkt Angiologie					
141 103	FA Innere Medizin und Schwerpunkt Endokrinologie und Diabetologie					
141 104	FA Innere Medizin und Schwerpunkt Gastroenterologie					
141 901	FA Innere Medizin und Schwerpunkt Geriatrie					
141 902	FA Innere Medizin und Schwerpunkt gesamte Innere Medizin					
141 105	FA Innere Medizin und Schwerpunkt Hämatologie und Onkologie					
141 106	FA Innere Medizin und Schwerpunkt Kardiologie					
141 107	FA Innere Medizin und Schwerpunkt Nephrologie					
141 108	FA Innere Medizin und Schwerpunkt Pneumologie					
141 109	FA Innere Medizin und Schwerpunkt Rheumatologie					
141 003	FA Internist/Lungen- und Bronchialheilkunde					
141 005	FA Lungen- und Bronchialheilkunde					
141 004	FA Lungenheilkunde					
142	SP Angiologie					

001						
142 002	SP Endokrinologie					
142 901	SP Endokrinologie und Diabetologie					
142 003	SP Gastroenterologie					
142 004	SP Geriatrie					
142 005	SP Hämatologie und Internistische Onkologie					
142 006	SP Infektiologie					
142 007	SP Kardiologie					
142 008	SP Nephrologie					
142 009	SP Pneumologie					
142 010	SP Rheumatologie					
143 001	TG Diabetologie					
143 002	TG Endokrinologie					
143 003	TG Gastroenterologie					
143 004	TG Hämatologie					
143 005	TG Infektions- und Tropenmedizin					
143 006	TG Kardiologie					
143	TG Kardiologie und					

901	Angiologie					
143 007	TG Lungen- und Bronchialheilkunde					
143 008	TG Nephrologie					
143 009	TG Rheumatologie					
151 002	FA Kinder- und Jugendmedizin		x			
151 001	FA Kinderheilkunde					
152 901	SP Endokrinologie und Diabetologie in der Kinder- und Jugendmedizin					
152 902	SP Gastroenterologie in der Kinder- und Jugendmedizin					
152 001	SP Infektiologie					
152 201	SP Kinder- und Jugend-Hämatologie und -Onkologie					
152 202	SP Kinder- und Jugend-Kardiologie					
152 101	SP Kinder-Hämatologie und -Onkologie					
152 002	SP Kinder-Kardiologie					
152 906	SP Kinderpneumologie					
152 003	SP Neonatologie					
152 903	SP Nephrologie					
152 102	SP Neuropädiatrie					

152 904	SP Pädiatrische Rheumatologie					
152 905	SP Pulmologie in der Kinder- und Jugendmedizin					
153 001	TG Kinderdiabetologie					
153 002	TG Kindergastroenterologie					
153 003	TG Kinderhämatologie					
153 004	TG Kinderkardiologie					
153 005	TG Kinderlungen- und -bronchialheilkunde					
153 006	TG Kinderneonatologie					
153 007	TG Kindernephrologie					
153 008	TG Kinderneuropsychiatrie					
161 001	FA Kinder- und Jugendpsychiatrie					
161 002	FA Kinder- und Jugendpsychiatrie und -psychotherapie					
171 001	FA Laboratoriumsmedizin		x	x	x	
173 001	TG Medizinische Mikrobiologie					
181 001	FA Mikrobiologie					
181 002	FA Mikrobiologie und Infektionsepidemiologie					
181 101	FA Mikrobiologie; Virologie und Infektionsepidemiologie					

191 001	FA Kieferchirurgie			x	x	
191 002	FA Mund-Kiefer-Gesichtschirurgie		x	x	x	
191 901	FA Oralchirurgie					
201 001	FA Nervenheilkunde					
201 002	FA Nervenheilkunde (Neurologie und Psychiatrie)					
201 003	FA Neurologie und Psychiatrie (Nervenarzt)					
203 001	TG Kinderneuropsychiatrie					
211 001	FA Neurochirurgie					
221 001	FA Neurologie		x		x	
222 901	SP Geriatrie					
231 001	FA Nuklearmedizin					
241 001	FA Öffentliches Gesundheitswesen			x		
251 001	FA Neuropathologie					
251 002	FA Pathobiochemie und Labordiagnostik					
251 003	FA Pathologie		x		x	
251 004	FA Pathologische Anatomie					
251 005	FA Pathologische Physiologie					

253 001	TG Neuropathologie					
261 001	FA Klinische Pharmakologie					
261 002	FA Pharmakologie					
261 003	FA Pharmakologie und Toxikologie					
263 001	TG Klinische Pharmakologie					
381 201	Phoniatrie und Pädaudiologie					
271 001	FA Physikalische und Rehabilitative Medizin					
271 002	FA Physiotherapie					
281 001	FA Physiologie					
291 001	FA Psychiatrie					
291 002	FA Psychiatrie und Psychotherapie		x		x	
292 101	SP Forensische Psychiatrie					
292 901	SP Geriatrie					
301 101	FA Psychosomatische Medizin und Psychotherapie					
301 001	FA Psychotherapeutische Medizin					
301 002	FA Psychotherapie					
311 001	FA Diagnostische Radiologie					

311 002	FA Radiologie					
311 003	FA Radiologische Diagnostik					
312 201	SP Kinder- und Jugendradiologie					
312 001	SP Kinderradiologie					
312 002	SP Neuroradiologie					
313 001	TG Kinderradiologie					
313 002	TG Neuroradiologie					
313 003	TG Strahlentherapie					
321 001	FA Rechtsmedizin					
351 001	FA Strahlentherapie					
361 001	FA Blutspende- und Transfusionswesen					
361 002	FA Transfusionsmedizin					
371 001	FA Urologie		x			
1	Zahnärztin/Zahnarzt	Qualifikationen zahnärztlicher Autoren (OID 1.2.276.0.76.5.492)		x		
2	FZA Allgemeine Zahnheilkunde			x		
3	FZA Parodontologie			x		
4	FZA Oralchirurgie			x		

5	FZA Kieferorthopädie			x		
6	FZA öffentliches Gesundheitswesen			x		
1	Gesundheits- Sozial-, Sportmanagement	Qualifikationen nicht ärztlicher Autoren (OID 1.3.6.1.4.1.19376.3.276.1.5.11)				
2	Arzthilfe, Praxisorganisation, -verwaltung		x	x		
3	Kaufmann/-frau - Gesundheitswesen					
4	Medizinischer Fachangestellter					
6	Zahnmedizinischer Fachangestellter			x	x	
7	Arztsekretär					
8	Sozial-, Gesundheitsmanagement					
9	Gesundheitsaufseher/ Hygienekontrolleur					
10	Assistent Gesundheits- und Sozialwesen					
11	Beamte Sozialversicherung					
12	Beamte Sozialverwaltung					
13	Betriebswirt					
14	Gesundheitsmanager					
15	Sozialökonom, -wirt					
16	Sozialversicherungsfachange					

33	Kranken-, Altenpflege, Geburtshilfe					
34	Altenpflegehelfer					
35	Altenpfleger					
36	Fachkraft Pflegeassistenz					
37	Gesundheits- und Kinderkrankenpfleger					
38	Gesundheits- und Krankenpflegehelfer					
39	Gesundheits- und Krankenpfleger					
40	Haus- und Familienpfleger					
41	Hebamme/ Entbindungspfleger		x		x	
42	Heilerziehungspfleger					
43	Helfer Altenpflege					
44	Helfer stationäre Krankenpflege					
45	Heilerziehungspflegehelfer					
46	Pflegewissenschaftler					
47	Nichtärztliche Behandlung, Therapie (außer Psychotherapie)					
48	Akademischer Sprachtherapeut					

49	Atem-, Sprech- und Stimmlehrer					
50	Ergotherapeut					
51	Fachangestellter für Bäderbetriebe					
52	Heilpraktiker					
53	Klinischer Linguist					
54	Kunsttherapeut					
55	Logopäde					
56	Masseur und medizinische Bademeister					
57	Motologe					
58	Musiktherapeut					
59	Orthoptist					
60	Physiotherapeut					
61	Podologe					
62	Sporttherapeut					
63	Sprechwissenschaftler					
64	Staatlich anerkannter Sprachtherapeut					
65	Stomatherapeut					

66	Tanz- und Bewegungstherapeut					
68	Sozialtherapeut					
69	Pharmazeutische Beratung, Pharmavertrieb					
70	Apotheker/Fachapotheker					x
71	Pharmazeut					
72	Pharmazeutisch-technischer Assistent – PTA					x
73	Pharmazeutisch-kaufmännischer Angestellter					x
74	Psychologische Analyse, Beratung, Therapie					
75	Gesundheits- und Rehabilitationspsychologe					
76	Kinder- und Jugendpsychotherapeut					
77	Klinischer Psychologe					
78	Kommunikationspsychologe					
79	Pädagogischer Psychologe					
80	Psychoanalytiker					
81	Psychologe					
82	Psychologischer Psychotherapeut					

83	Sportpsychologe					
84	Verkehrspsychologe					
85	Wirtschaftspsychologe					
86	Rettungsdienst					
87	Ingenieur Rettungswesen					
88	Notfallsanitäter					
89	Rettungsassistent					
90	Rettungshelfer					
91	Rettungssanitäter					
92	med. Datenverarbeitung					
94	Medizinischer Dokumentar					
95	Medizinischer Dokumentationsassistent					
173	Fachangestellter f. Medien- und Informationsdienste - Medizinische Dokumentation					
174	Medizinischer Informationsmanager					
96	Soziales, Pädagogik					
97	Kinderbetreuung, -erziehung					
98	Pädagoge					
99	Kinderdorfmutter, -vater					

100	Kinderpfleger					
101	Erzieher					
102	Erzieher Jugend- und Heimerziehung					
103	Lehrer					
104	Orientierungs- und Mobilitätslehrer					
105	Medien-, Kulturpädagogik					
106	Musikpädagoge					
107	Sozialberatung, -arbeit					
108	Sozialarbeiter/ Sozialpädagoge					
109	Betreuungskraft/ Alltagsbegleiter					
110	Gerontologe					
111	Psychosozialer Prozessbegleiter					
112	Rehabilitationspädagoge					
113	Sozialassistent					
114	Seelsorge					
115	Religionspädagoge					
116	Gemeindehelfer,					

	Gemeindediakon					
117	Theologe					
118	Medizintechnik, Laboranalyse					
119	Medizin-, Orthopädie- und Rehatechnik					
120	Assistent Medizinische Gerätetechnik					
121	Augenoptiker					
122	Hörakustiker/ Hörgeräteakustiker					
123	Hörgeräteakustikermeister					
124	Ingenieur Augenoptik					
125	Ingenieur - Hörtechnik und Audiologie					
126	Ingenieur - Medizintechnik					
127	Ingenieur - Orthopädie- und Rehatechnik					
128	Medizinphysiker (z.B. in Strahlenmedizin)					
129	Orthopädieschuhmacher					
130	Orthopädietechnik - Mechaniker					
131	Zahntechniker			x		

132	Glasbläser (Fachrichtung Kunstaugen)					
133	staatlich geprüfter Techniker der Fachrichtung Medizintechnik					
134	Medizinisch-technische Assistenz					
135	Anästhesietechnischer Assistent					
136	HNO Audiologieassistent					
137	Medizinisch-Technischer Assistent Funktionsdiagnostik – MTA-F					
138	Medizinisch-Technischer Laboratoriumsassistent – MTA-L					
139	Medizinisch-Technischer Radiologieassistent – MTA-R					
140	Operationstechnischer Angestellter					
141	Operationstechnischer Assistent					
143	Zytologieassistent					
144	Chemie, naturwissenschaftliche Laboranalyse (außer MTA)					
145	Biochemiker (z.B. klinische Chemie)					
146	Chemiker (z.B. klinische Chemie)					

147	Humangenetiker					
148	Mikrobiologe					
149	Dienstleistungen am Menschen (außer medizinische)					
150	Körperpflege					
151	Fachkraft Beauty und Wellness					
152	Friseur					
153	Kosmetiker					
154	Bestattungswesen					
155	Bestattungsfachkraft					
156	Berufe aus sonstigen Berufsfeldern					
157	Umwelt					
165	Jurist					
169	Taxifahrer bei Krankentransport					
180	Pharmazieingenieur					
182	Apothekerassistent					
181	Apothekenassistent					
1	Arzt in Facharztausbildung	Ärztliche				

		Berufsvarianten (OID: 1.2.276.0.76.5.493)				
2	Hausarzt					
3	Praktischer Arzt					

Hinweis: Im Zuge der Value Set-Pflege wurde das Code-System "S_BAR2_WBO" (OID 1.2.276.0.76.5.114) für Fachgruppen-Codes nach der Weiterbildungsordnung Bundesarztregister in das neue Code-System "Facharzttitel der Ärztekammern" (OID: 1.2.276.0.76.5.514) konsolidiert, welches zukünftig das alte System ersetzt. Aufgrund der notwendigen Abwärtskompatibilität muss im Value Set "DocumentEntry.authorSpecialty" (OID: 1.2.276.0.76.11.31) für Spezialisierungen eines Dokumentenautors weiterhin das Code-System "S_BAR2_WBO" durch ePA-Produkttypen, welche IHE ITI XDS-Metadaten verarbeiten, lesend unterstützt werden. Für das Value Set "SubmissionSet.authorSpecialty" gilt dies analog. Neue Dokumente oder SubmissionSets dürfen nicht mehr mit Codes aus "S_BAR2_WBO" gekennzeichnet werden.

Tabelle 38: Value Set classCode

Code	Anzeigename	Code-System	Arzt / Rolle Med	Zahnarzt	Krankenhaus	Apotheke
ADM	Administratives Dokument	Dokumentenklassen (OID: 1.3.6.1.4.1.19376.3.276.1.5.8)	x	x	x	x
ANF	Anforderung					
ASM	Assessment					
BEF	Befundbericht		x	x	x	x
BIL	Bilddaten		x	x	x	x
BRI	Brief		x	x	x	x
DOK	Dokumente ohne besondere Form (Notizen)		x	x	x	x
DUR	Durchführungsprotokoll		x	x	x	
FOR	Forschung					

GUT	Gutachten und Qualitätsmanagement					
LAB	Laborergebnisse		x	x	x	x
AUS	Medizinischer Ausweis		x	x	x	x
PLA	Planungsdokument		x	x	x	x
57016-8	Patienteneinverständniserklärung	Logical Observation Identifier Names and Codes (OID: 2.16.840.1.113883.6.1)	x	x	x	x
VER	Verordnung	Dokumentenklassen (OID: 1.3.6.1.4.1.19376.3.276.1.5.8)	x	x	x	x
VID	Videodaten		x	x	x	x

Tabelle 39: Value Set confidentialityCode

Code	Anzeigename	Code-System	Arzt / Rolle Med	Zahnarzt	Krankenhaus	Apotheke
LEI	Dokument einer Leistungserbringerinstitution	ePA-Vertraulichkeit (OID: 1.2.276.0.76.5.491)	x	x	x	x
KTR	Dokument eines Kostenträgers		x	x	x	x
PAT	Dokument eines Versicherten		x	x	x	x
LEÄ	Leistungserbringeräquivalentes Dokument eines Versicherten oder Kostenträgers		x			

N	normal	Confidentiality (OID: 2.16.840.1.113883.5.25)	x	x	x	x
R	restricted		x	x	x	x
V	very restricted		x	x	x	x
PV	gesperrt	Betroffeneneinschätzung der Vertraulichkeitsstufe (OID: 1.3.6.1.4.1.19376.3.276.1.5.10)				
PR	erhöhte Vertraulichkeit					
PN	übliche Vertraulichkeit					

Tabelle 40: Value Set eventCodeList

Code	Anzeigename	Code-System	Arzt/ Rolle Med	Zahnarzt	Kranken-haus	Apotheke
urn:ihe:iti:xdw:2011:eventCode:open	Workflow offen	DocumentReference Format Code Set (OID: 1.3.6.1.4.1.19376.1.2.3)				
urn:ihe:iti:xdw:2011:eventCode:closed	Workflow abgeschlossen					
H1	vom Patienten mitgebracht	Dokumenten-Warnhinweise (OID: 1.3.6.1.4.1.19376.3.276.1.5.15)	x	x	x	x
H2	noch nicht mit Patient besprochen					
H3	eventuell veraltete Daten					
H4	vorläufiges Dokument					

E100	ambulanter Kontakt	Fallkontext bei Dokumentenerstellung (OID: 1.3.6.1.4.1.19376.3.276.1.5.16)	x	x	x	x
E110	ambulante OP		x	x	x	
E200	stationärer Aufenthalt				x	
E210	stationäre Aufnahme					
E211	Aufnahme vollstationär					
E212	Aufnahme/ Wiederaufnahme teilstationär					
E213	Aufnahme Entbindung stationär					
E214	Aufnahme eines Neugeborenen					
E215	Aufnahme des Spenders zur Organentnahme					
E230	stationäre Entlassung					
E231	stationäre Entlassung nach Hause					
E232	stationäre Entlassung in eine Rehabilitationseinrichtung					
E233	stationäre Entlassung in					

	eine Pflegeeinrichtung /Hospiz					
E234	Entlassung zur nachstationären Behandlung					
E235	Patient während stationärem Aufenthalt verstorben					
E250	stationäre Verlegung					
E251	Verlegung innerhalb eines Krankenhauses					
E252	Verlegung in ein anderes Krankenhaus					
E253	externe Verlegung in Psychiatrie					
E270	kurzzeitige Unterbrechung einer stationären Behandlung					
E280	Konsil		x	x	x	
E300	Behandlung im häuslichen Umfeld		x	x		
E400	Virtual Encounter		x	x	x	

Tabelle 41: Value Set healthcareFacilityTypeCode

Co	Anzeigename	Code-System	Arzt	Zahna	Kranke	Apothe

de			/ Rolle Med	rzt	n-haus	ke
APD	Ambulanter Pflegedienst	Einrichtungsarten der patientenbezogenen Gesundheitsversorgung (OID: 1.3.6.1.4.1.19376.3.276.1.5.2)				
APO	Apotheke					x
BER	Ärztlicher Bereitschaftsdienst		x			
PRA	Arztpraxis		x	x		
BAA	Betriebsärztliche Abteilung		x			
BHR	Gesundheitsbehörde					
HEB	Hebamme/ Geburtshaus		x		x	
HOS	Hospiz				x	
KHS	Krankenhaus				x	
MVZ	Medizinisches Versorgungszentrum		x	x		x
HAN	Medizinisch-technisches Handwerk					
REH	Medizinische Rehabilitation					

HEI	Nicht-ärztliche Heilberufs-Praxis					
PFL	Pflegeheim					
RTN	Rettungsdienst					
SEL	Selbsthilfe					
TMZ	Telemedizinisches Zentrum		x			
BIL	Bildungseinrichtung	Einrichtungsarten außerhalb der patientenbezogenen Gesundheitsversorgung (OID: 1.3.6.1.4.1.19376.3.276.1.5.3)				
FOR	Forschungseinrichtung					
GEN	Gen-Analysedienste					
MDK	Medizinischer Dienst der Krankenversicherung					
PAT	Patient außerhalb der Betreuung					
SPE	Spendedienste					
VER	Versicherungsträger					

Tabelle 42: Value Set practiceSettingCode

Co	Anzeigename	Code-System	Arzt	Zahna	Kranke	Apothe

de			/ Rolle Med	rzt	n-haus	ke
ALLG	Allgemeinmedizin	Ärztliche Fachrichtungen (OID: 1.3.6.1.4.1.19376.3.276.1.5.4)	x			
ANAE	Anästhesiologie		x	x	x	
ARBE	Arbeitsmedizin		x			
AUGE	Augenheilkunde		x		x	
CHIR	Chirurgie		x		x	
ALCH	Allgemeinchirurgie					
GFCH	Gefäßchirurgie					
HZCH	Herzchirurgie					
KDCH	Kinderchirurgie					
ORTH	Orthopädie					
PLCH	Plastische und Ästhetische Chirurgie					
THCH	Thoraxchirurgie					
UNFC	Unfallchirurgie					

VICH	Viszeralchirurgie					
FRAU	Frauenheilkunde und Geburtshilfe		x		x	
GEND	Gynäkologische Endokrinologie und Reproduktionsmedizin					
GONK	Gynäkologische Onkologie					
PERI	Perinatalmedizin					
GERI	Geriatrie		x		x	
HNOH	Hals-Nasen-Ohrenheilkunde		x		x	
HRST	Sprach-, Stimm- und kindliche Hörstörungen					
HAUT	Haut- und Geschlechtskrankheiten		x		x	
HUMA	Humangenetik		x		x	
HYGI	Hygiene und Umweltmedizin		x		x	
INNE	Innere Medizin		x		x	
ANGI	Angiologie					
EN	Endokrinologie und					

DO	Diabetologie					
GAST	Gastroenterologie					
HAEM	Hämatologie und internistische Onkologie					
KARD	Kardiologie					
NEPH	Nephrologie					
PNEU	Pneumologie					
RHEU	Rheumatologie					
INTM	Intensivmedizin		x		x	
INTO	Interdisziplinäre Onkologie		x		x	
INTS	Interdisziplinäre Schmerzmedizin		x		x	
KIJU	Kinder- und Jugendmedizin		x		x	
KONK	Kinder-Hämatologie und -Onkologie					
KKAR	Kinder-Kardiologie					
NNAT	Neonatologie					
NP	Neuropädiatrie					

AE						
KP SY	Kinder- und Jugendpsychiatrie und -psychotherapie		x		x	
LA BO	Laboratoriumsmedizin		x	x	x	
MI KR	Mikrobiologie, Virologie und Infektionsepidemiologie		x		x	
MK GC	Mund-Kiefer-Gesichtschirurgie		x	x	x	
NA TU	Naturheilverfahren und alternative Heilmethoden		x		x	
NO TF	Notfallmedizin		x	x	x	
NR CH	Neurochirurgie		x		x	
NE UR	Neurologie		x		x	
NU KL	Nuklearmedizin		x		x	
GE SU	Öffentliches Gesundheitswesen		x	x	x	x
PA LL	Palliativmedizin		x		x	
PA TH	Pathologie		x		x	
NP AT	Neuropathologie					

PHAR	Pharmakologie		x	x	x	x
TOXI	Toxikologie					
REHA	Physikalische und Rehabilitative Medizin		x		x	
PSYC	Psychiatrie und Psychotherapie		x		x	
FPSY	Forensische Psychiatrie					
PSYM	Psychosomatische Medizin und Psychotherapie		x		x	
RADI	Radiologie		x		x	
KRAD	Kinderradiologie					
NRAD	Neuroradiologie					
RECH	Rechtsmedizin		x	x	x	
SCHL	Schlafmedizin		x		x	
SPOR	Sport- und Bewegungsmedizin		x		x	
STRA	Strahlentherapie		x		x	
TRAN	Transfusionsmedizin		x		x	

TROP	Tropen-/Reisemedizin		x		x	
UROL	Urologie		x		x	
MZKH	Zahnmedizin			x	x	
ORAL	Oralchirurgie			x	x	
KIEF	Kieferorthopädie			x		
MZAH	Allgemeine Zahnheilkunde	Zahnärztliche Fachrichtungen (OID: 1.2.276.0.76.5.494)		x		
PARO	Parodontologie	Ärztliche Fachrichtungen (OID: 1.3.6.1.4.1.19376.3.276.1.5.4)		x		
ZGES	Öffentliches Gesundheitswesen (Zahnheilkunde)	Zahnärztliche Fachrichtungen (OID: 1.2.276.0.76.5.494)		x		
TRPL	Transplantationsmedizin	Ärztliche Fachrichtungen (OID: 1.3.6.1.4.1.19376.3.276.1.5.4)			x	
ERG	Ergotherapie	Nicht-ärztliche Fachrichtungen (OID: 1.3.6.1.4.1.19376.3.276.1.5.5)			x	
ERN	Ernährung und Diätetik		x		x	
FOR	Forschung					
PFL	Pflege und Betreuung					

ALT	Altenpflege					
KIN	Kinderpflege					
PAT	Patient außerhalb der Betreuung					
PHZ	Pharmazeutik				x	x
POD	Podologie		x		x	
PRV	Prävention					
SOZ	Sozialwesen					
SPR	Sprachtherapie					
VKO	Versorgungskoordination					
VER	Verwaltung					
PST	Psychotherapie		x		x	

Tabelle 43: Value Set typeCode

Code	Anzeigename	Code-System	Arzt / Rolle Med	Zahnarzt	Krankenhaus	Apotheke
ABRE	Abrechnungsdokumente	Dokumententypen (OID: 1.3.6.1.4.1.19376.3.276.1	x	x	x	x

ADCH	Administrative Checklisten	.5.9)			x	
ANTR	Anträge und deren Bescheide		x	x	x	x
ANAE	Anästhesiedokumente		x	x	x	
BERI	Arztberichte		x	x	x	
BESC	Ärztliche Bescheinigungen		x	x	x	x
BEFU	Ergebnisse Diagnostik		x	x	x	
BSTR	Bestrahlungsdokumentation				x	
AUFN	Einweisungs- und Aufnahmedokumente				x	
EINW	Einwilligungen/ Aufklärungen		x	x	x	x
FUNK	Ergebnisse Funktionsdiagnostik		x		x	
BILD	Ergebnisse bildgebender Diagnostik		x	x	x	x
FALL	Fallbesprechungen		x	x	x	
FOTO	Fotodokumentation		x	x	x	
FPRO	Therapiedokumentation		x	x	x	
IMM	Ergebnisse Immunologie		x		x	

U						
INTS	Intensivmedizinische Dokumente		x		x	
KOMP	Komplexbehandlungsbögen		x		x	
MEDI	Medikamentöse Therapien		x	x	x	x
MKRO	Ergebnisse Mikrobiologie		x	x	x	x
OPDK	OP-Dokumente		x	x	x	
ONKO	Onkologische Dokumente		x		x	
PATH	Pathologiebefundberichte		x		x	
PATD	Patienteneigene Dokumente					
PATI	Patienteninformationen		x	x	x	x
PFLG	Pflegedokumentation		x		x	
57016-8	Patienteneinverständniserklärung	Logical Observation Identifier Names and Codes (OID: 2.16.840.1.113883.6.1)				
QUAL	Qualitätssicherung	Dokumententypen (OID: 1.3.6.1.4.1.19376.3.276.1.5.9)	x	x	x	x
RETT	Rettungsdienstliche Dokumente		x		x	

SCHR	Schriftwechsel (administrativ)		x	x	x	x
GEBU	Schwangerschafts- und Geburtsdokumentation		x		x	
SOZI	Sozialdienstdokumente					
STUD	Studiendokumente		x	x	x	x
TRFU	Transfusionsdokumente		x	x	x	
TRPL	Transplantationsdokumente		x	x	x	
VERO	Verordnungen		x	x	x	x
VERT	Verträge		x	x	x	
VIRO	Ergebnisse Virologie		x	x	x	
WUND	Wunddokumentation		x	x		