Elektronische Gesundheitskarte und Telematikinfrastruktur

Implementierungsleitfaden Primärsysteme ePA für alle

Version:	4.0.0 CC
Revision:	1755831
Stand:	15.10.2026
Status:	zur Abstimmung freigegeben
Klassifizierung:	öffentlich_Entwurf
Referenzierung:	gemILF_PS_ePA

Dokumenteninformationen

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

Änderungen zur Vorversion

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 Kapitel 1 und 2, Überarbeitung Kapitel 6)	gematik
3.2.1	07.08.2024		ePA für alle - Releasestand 3.0.2 (Anpassungen)	gematik
			...	
3.3.0	22.08.2024		ePA für alle - Releasestand 3.1.0	gematik
3.4.0	28.02.2025		ePA für alle - Release 3.0.5	gematik
3.5.0	27.05.2025		ePA für alle - Release 3.1.2	gematik
3.6.0	12.09.2025		ePA für alle - Release 3.1.3 (inkl. Release 3.1.2-1)	gematik
3.7.0	15.12.2025		ePA für alle - Release 3.1.3-1	gematik
3.8.0	23.03.2026		Aktualisierung zu ePA für alle 3.1.3-2	gematik
3.8.1	24.03.2026		Anpassung Prozess Client-ID-/product-id-Registrierung	gematik
4.0.0 CC	15.10.2026		ePA für alle 27	gematik

Inhaltsverzeichnis

1 Einordnung des Dokumentes....7
1.1 Zielsetzung....7
1.2 Zielgruppe....7
1.3 Geltungsbereich....7
1.4 Abgrenzungen....8
1.5 Methodik....8
1.6 Referenzen für die technische Entwicklung....9
1.7 Namenskonvention und IHE....9
1.8 Formate beim Einstellen von Dokumenten....10
1.9 Medizinische Informationsobjekte....11
1.10 Die ePA nach § 341 SGB V....11
2 Systemüberblick....13
2.1 Einführung....13
2.2 Prozesssichten und Funktionsumfänge der Primärsysteme....14
2.2.1 Behandlungskontext und Zugriffsbefugnisse....14
2.2.2 Niedergelassener Sektor....15
2.2.2.1 Prozesssicht....15
2.2.2.2 Anwendungsfälle....18
2.2.3 Apotheken....18
2.2.3.1 Prozesssicht....18
2.2.3.2 Anwendungsfälle....20
2.2.4 Stationärer Sektor....20
2.2.4.1 Prozesssicht....20
2.2.4.2 Aufnahmeprozess....22
2.2.4.3 Versorgungsprozess....23
2.2.4.4 Entlassprozess....23
2.2.4.5 Anwendungsfälle....25
2.2.5 Pflege....25
2.2.5.1 Prozessmodell....25
2.2.5.2 Anwendungsfälle....26
2.2.6 Heilmittelerbringer....27
2.2.6.1 Prozessmodell....27
2.2.6.2 Anwendungsfälle....27
2.3 Akteure und Rollen....28
2.4 IT-Sicherheit in den Systemen der Leistungserbringerinstitution....30
3 Übergreifende Festlegungen....31
3.1 TLS....31
3.2 Aktensystem- und Service-Lokalisierung....32
3.3 Aufbau der User Session zum Aktensystem....33
3.3.1 VAU....34

3.3.2 Nutzerauthentifizierung per IDP-Dienst mittels OIDC-Flow....34
3.3.2.1 Übergreifende Festlegungen zur Nutzung des IDP-Dienstes....40
3.4 Lokalisierung der Akte eines Versicherten....41
3.4.1 Aktenkontokennung....42
3.4.2 Logout....43
3.4.3 Zertifikate....43
3.5 SOAP....45
3.6 REST....46
3.7 Mandantenverwaltung....46
3.8 Funktionsmerkmale....47
3.9 Erstellen einer Befugnis....48
3.9.1 Erstellen einer Befugnis mittels PoPP....49
3.9.1.1 Umsetzung....50
3.9.1.2 Nutzung....50
3.9.2 Erstellen einer Befugnis mittels VSDM....51
3.9.2.1 Umsetzung....52
3.9.2.2 Nutzung....53
3.10 Versorgungsspezifische Services....53
3.10.1 Widersprüche zu Versorgungsprozessen abrufen....53
3.10.2 Medikationsprozess....54
3.11 Dokumentenmanagement....54
3.11.1 Grundlegende Anforderungen für XDS....55
3.11.2 Anforderungen für MHD....56
3.11.3 Dokumente einstellen [ITI-41]....57
3.11.3.1 Umsetzung....59
3.11.3.2 Nutzung....59
3.11.4 Dokumente suchen....65
3.11.4.1 Dokumente suchen [ITI-18]....65
3.11.4.1.1 Umsetzung....66
3.11.4.1.2 Nutzung....66
3.11.4.2 Dokumente suchen [ITI-67]....69
3.11.5 Dokumente laden....69
3.11.5.1 Dokumente laden [ITI-43]....69
3.11.5.1.1 Umsetzung....69
3.11.5.1.2 Nutzung....70
3.11.5.2 Dokumente laden [ITI-68]....71
3.11.6 Dokumente löschen [ITI-62]....71
3.11.6.1 Umsetzung....72
3.11.6.2 Nutzung....72
3.11.7 Aktualisieren von Metadaten [ITI-92]....73
3.11.7.1 Umsetzung....73
3.11.7.2 Nutzung....73
3.11.8 Artefakte....74
3.11.8.1 Namensräume....74
3.11.8.2 WSDLs und Schemata....75
3.11.9 Testunterstützung....75
3.12 Informationsmodell....75
3.12.1 Metadaten....75
3.12.2 Vorgaben für bestimmte Dokumententypen....83
3.12.2.1 Medizinische Informationsobjekte....84

3.12.2.2 NFD und DPE (eGK)....84
3.12.2.3 Elektronischer Arztbrief (eArztbrief) der KBV....84
3.12.2.4 Arztbriefe und Krankenhausentlassbriefe....88
3.12.2.5 Laborergebnisse (inkl. Laborbefunde)....89
3.12.3 Selbstauskunft....89
3.12.4 Signieren von Dokumenten....91
3.12.4.1 Signaturen bei Medizinischen Informationsobjekten (MIOs)....91
3.12.4.2 Signaturen bei PDF/A....92

4 Spezielle Nutzungsumgebungen....93

4.1 Funktionsumfang Clientsystem des Kostenträgers....93
4.1.1 Einstellen von Daten durch Kostenträger....93
4.1.2 Ablauf eines betreiberübergreifenden Aktenumzugs (informativ)....94
4.1.2.1 Erstellung des Exportpakets auf Seiten des alten Kostenträgers....95
4.1.2.2 Einspielen des Exportpakets auf Seiten des neuen Kostenträgers....96
4.1.2.3 Verhalten bei Scheitern des Imports....96
4.1.3 Verwaltung von E-Mail-Adressen....96

4.2 Funktionsumfang Clientsystem der Ombudsstelle....97
4.2.1 Spezifische LEI für die Nutzung eines Aktenkontos sperren....97
4.2.2 Widersprüche....99
4.2.2.1 Widersprüche zum Medikationsprozess einstellen oder widerrufen....99
4.2.2.2 Widersprüche zur Sekundärdatennutzung durch das FDZ einstellen oder widerrufen....100
4.2.3 Protokolldaten dem Versicherten zur Verfügung stellen....103

4.3 Funktionsumfang Clientsystem DiGA....104
4.3.1 Einstellen von DiGA-Daten....104

5 Ergänzende Funktionalitäten....105

5.1 Betriebs- und Performancedaten....105

5.2 Übertragungsprotokolle speichern....106

5.3 Empfehlung zur Archivierung....106

6 UX Best practice für Primärsysteme....108

6.1 Standardeinstellungen und Konfigurationsmöglichkeiten des Systems 108
6.1.1 Befugniserzeugung aus der Leistungserbringerumgebung....108
6.1.2 Anzeige und Suche von Dokumenten eines ePA-Aktenkontos....110
6.1.3 Hochladen in ein ePA-Aktenkonto im Kontext der lokalen Dokumentenverwaltung....111
6.1.4 Hochladen in ein ePA-Aktenkonto als Standard für bestimmte Dokumententypen....112
6.1.5 Hochladen in ein ePA-Aktenkonto als Standard für ausgewählte Dokumententypen in der Benutzung von KIM....113
6.1.6 Vorgaben für eAU....113
6.1.7 Hochladen in ein ePA-Aktenkonto als Standard für NFDM (eGK)....114
6.1.8 Standardmäßige Vorbelegung von Werten beim Hochladen eines Dokuments in ein ePA-Aktenkonto....114
6.1.9 Nachträgliches Hochladen eines Dokuments in ein ePA-Aktenkonto....115
6.1.10 Widerspruch gegen das Hochladen eines Dokuments in ein ePA-Aktenkonto 115

6.2 XDS Document Service: Dokumentenverwaltung in der elektronischen Patientenakte....115
6.2.1 Dokumentenübersicht anzeigen....116

6.2.2 Dokumente suchen, filtern und sortieren....118
6.2.3 Dokumente herunterladen, aktualisieren oder löschen....122
6.2.4 Dokument hochladen aus Karteikarte oder Dokumentenmanagementkontext 125
6.2.5 Dokument hochladen aus KIM-Workflow....127
6.2.6 ePA MHD Service....129

7 Fehlerbehandlung....130

7.1 Fehlermeldungen der REST-Schnittstellen....130

7.2 Fehlerbehandlung im XDS Document Service....131
7.2.1 IHE-Error....132
7.2.2 Erweiterte Angaben des Aktensystems zum Fehler in codeContext....133
7.2.3 Fehlermeldungen aus dem XDS Document Service....134

7.3 Anforderungen an das Primärsystem bei IHE-Fehlern....136

7.4 Umgang mit Fehlern in der Leistungserbringerinstitution....137

8 Anhang A – Verzeichnisse....139

8.1 Abkürzungen....139

8.2 Glossar....141

8.3 Abbildungsverzeichnis....142

8.4 Tabellenverzeichnis....143

8.5 Referenzierte Dokumente....144
8.5.1 Dokumente der gematik....144
8.5.2 Weitere Dokumente....146

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.

Dieser Implementierungsleitfaden gibt einerseits spezifische Anforderungen für Primärsysteme vor, bietet aber andererseits auch allgemeine Hilfestellung bei der Verwendung der ePA-Schnittstellen. Dazu gehören bspw. informative Abschnitte, die die Nutzung der IHE XDS-Schnittstellen des Aktensystems beschreiben.

Die ePA setzt zu großen Teilen auf bestehenden Standards und Spezifikationen wie denen von IHE sowie HL7 (FHIR) auf. Diese Spezifikationen werden durch ePA und auch diesen Implementierungsleitfaden in aller Regel weiter eingeschränkt ("profiliert"). Dies soll die Verwendung bestehender Software-Bibliotheken ermöglichen oder zumindest vereinfachen und zudem auch eine Wiederverwendbarkeit der umzusetzenden Schnittstellen in anderen Kontexten erlauben.

Neben den Schnittstellen zur Verwaltung von Dokumenten ("XDS Document Service" im Aktensystems) werden von der ePA auch REST-Schnittstellen angeboten, bspw. FHIR-Schnittstellen im Rahmen des "Medication Service" zur Verwaltung von Medikationsliste und -plan eines Versicherten. Der Implementierungsleitfaden beschreibt, wie diese Schnittstellen zu nutzen sind und welche zusätzlichen Anforderungen gelten.

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] und [gemIG_TI_Terminology] beschrieben sind;
- Rendering-Vorschriften zur Form, in der ePA-Dokumente zur Anzeige gebracht werden (ggf. wird auf externe Festlegungen referenziert),
- Schnittstellenbeschreibungen, die hautpsächlich direkt in [gemSpec_Aktensystem_ePAfueralle] sowie [gemIG_ePA_MHD] zu finden sind. Der vorliegende Leitfaden enthält teilweise zusätzliche Anforderungen und Hinweise, wie diese Schnittstellen zu verwenden sind. Speziell [gemIG_ePA_MHD] enthält jedoch auch direkte Anforderungen an Primärsysteme und muss entsprechend beachtet werden.

Die ePA dient dem Austausch von medizinischer Dokumentation zwischen Leistungserbringern sowie dem Versicherten. Die medizinische Primärdokumentation der Versichertendaten verbleibt im Primärsystem des jeweiligen Leistungserbringers und wird hier 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 Inhalten, die unter GitHub verfügbar gemacht werden und größtenteils normativ sind. Sie werden auch aus der Spezifikation heraus dort, wo sie gebraucht werden, direkt über eine Literaturreferenz verlinkt.

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

- Das Fachkonzept [gemKPT_FK_ePAfueralle] beschreibt die fachlichen Anforderungen an die ePA unter Berücksichtigung der geltenden Gesetzeslage.
- Die Konzeption und Spezifikationen beschreiben die normativen Festlegungen auf Produktebene, u.a.:
  - [ePA_Basic]:GitHub Repository "ePA-Basic"
  - [gem_KPT_GK_ePAfueralle]:Grobkonzept "ePA für Alle"
  - [gem_KPT_GK_XDS]:Grobkonzept "ePA für Alle": XDS Document Service
  - [gemIG_ePA_Medication]: Implementation Guide ePA Medication Service
- Für Primärsystemhersteller werden die Anforderungen an die Umsetzung der ePA für unterschiedliche Typen von Primärsystemen bzw. Clientsystemen in einem sogenannten Steckbrief zusammengefasst. Die Steckbriefe der PS- und CS-Typen enthalten Listen der jeweils relevanten Anforderungen:
    - https://gemspec.gematik.de/docs/gemSST/

Das ePA-Aktensystem stellt die zentralen Schnittstellen der ePA bereit (passende Version auswählen):

- https://gemspec.gematik.de/docs/gemSpec/gemSpec_Aktensystem_ePAfueralle/latest/

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_24864-*] folgende MIME-Type-Formate und Dateiendungen:

- application/pdf (nur PDF/A-1 und 2) (pdf)
- 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 PDF-Dokumente im Format PDF-A erzeugen. PDF-Dokumente, die nicht im Format PDF-A vorliegen, müssen vor dem Einstellen in die ePA gemäß A_24967-* in ein PDF/A-Format konvertiert werden.

A_27258-01 -Zu verwendende Zeichenkodierung für Dokumente im Format txt, xml und json
Das Primärsystem MUSS Dokumente im Format text/plain (txt), application/xml (xml), application/json (json) beim Einstellen in das ePA-Aktensystem im Zeichensatz UTF-8 kodieren. Dabei gelten folgende Ausnahmen:
Falls es sich um einen Notfalldatensatz (NFD) oder einen Datensatz persönliche Erklärungen (DPE) gemäß [gemSpec_InfoNFDM] handelt, MUSS das Primärsystem diese Dokumente stattdessen im Zeichensatz ISO 8859-15 (mit Einschränkungen) im ePA-Aktensystem speichern.
[<=]

"Mit Einschränkungen" bedeutet hier, dass innerhalb von ISO-8859-15 die Zeilen 0 (bis auf 0x09, 0x0a und 0x0d), 1, 8, 9 sowie 0x7f verboten sind.

1.9 Medizinische Informationsobjekte

Die Kassenärztliche Bundesvereinigung (KBV) legt bei entsprechender Beauftragung gemäß § 355 SGB V für bestimmte strukturiert in die ePA einzustellende Inhalte medizinische Informationsobjekte (MIO - https://mio.kbv.de/site/mio#tab-Rund+um+die+MIOs) fest. Weitere Anwendungsfälle und strukturierte Datenformate werden im Fachkonzept und in den Spezifikationen der gematik zur ePA beschrieben und benannt (bspw. digital gestützte Medikationsprozess inkl. eML und eMP und eArztbrief der KBV).

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)
- Krankenhaus-Entlassbrief (nach stationärer Behandlung, sowohl vorläufige als auch endgültige Version) (im PDF/A Format)
- Laborbefund (früher PDF/A, ab ePA 27 im FHIR-Format gemäß [gemIG_ePA_Laboratory])
- 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)

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 hoch lädt.

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

2 Systemüberblick

2.1 Einführung

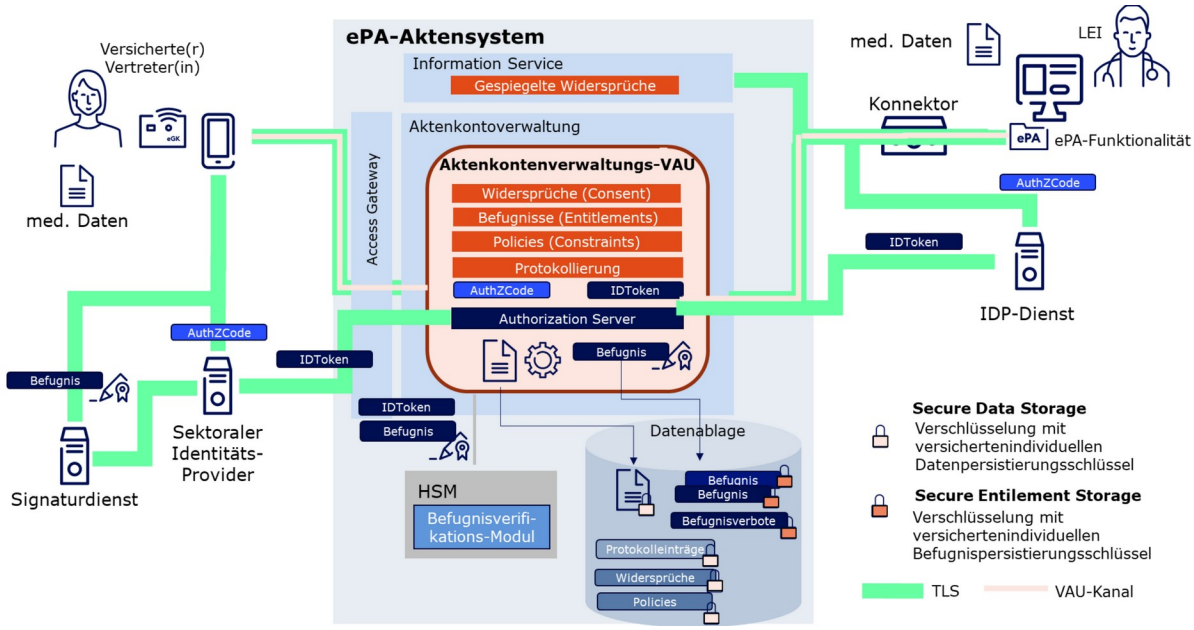


Abbildung 1: Überblick ePA für alle

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) und des elektronischen Medikationsplans (eMP) 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.

Die Verwendung eines TI-Gateways anstatt eines Konnektors hat keinen Einfluss auf die Nutzung der ePA. Wenn im Folgenden die Nutzung des Konnektors beschrieben wird, so treffen die Beschreibungen und Festlegungen auch auf die Nutzung des TI-Gateways zu.

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 durch den Nachweis einer Verbindung zwischen der LEI und dem Versicherten festgestellt, z.B. mit dem Stecken der eGK im Rahmen von VSDM oder Nutzung der GesundheitsID (für PoPP).

Das Dokument [gemKPT_FK_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) an.

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 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. Alternativ kann beim Einlesen der eGK oder durch Nutzung der GesundheitsID auch ein PoPP-Token vom PoPP Service bezogen werden und dieses in das ePA-Aktensystem übermittelt werden. 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. Außerdem können in der ePA-App 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 Befugnisvergabe 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 Befugnisdauer für die Leistungserbringerinstitution steht im Zusammenhang mit der Berufsgruppe. Für Arztpraxen, Zahnarztpraxen und psychotherapeutische Praxen sowie Krankenhäuser, Reha-Kliniken und Pflegeeinrichtungen beträgt die Befugnisdauer standardmäßig 90 Tage. In Apotheken, für den öffentlichen Gesundheitsdienst und die Arbeits- und Betriebsmedizin beträgt die Befugnisdauer standardmäßig 3 Tage.

Beim Einlesen der eGK soll die Befugnis automatisch erzeugt werden, d.h. die VSDM-Prüfziffer oder PoPP-Token werden automatisch an das ePA-Aktenkonto des Versicherten übermittelt, 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 oder Durchführen des PoPP-Verfahrens kann jedoch die Befugnisdauer erneuert und damit verlängert werden.

Wenn eine Befugnis nicht (mehr) vorhanden ist, weil z.B. die Befugnisdauer abgelaufen oder die Befugnis entzogen wurde, können keine Dokumente in ein ePA-Aktenkonto eingestellt und kein Inhalt mehr gelesen werden. Aus ärztlicher Sicht könnte nun bei Bedarf Kontakt zum Versicherten aufgenommen und um eine erneute Befugnisvergabe gebeten werden. Für langfristige oder permanente Behandlungskontexte 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 die Behandlung initial mit dem administrativen Anmeldeprozess. Mit Abgleich der Stammdaten des Versicherten wird der Behandlungskontext nachgewiesen und die Einrichtung erhält die Zugriffsbefugnis auf die ePA. Danach kann 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 werden, je nach Dokumentenart und -inhalt (siehe Abbildung 2). Ein Hochladen entfällt, wenn der Versicherte widersprochen hat.

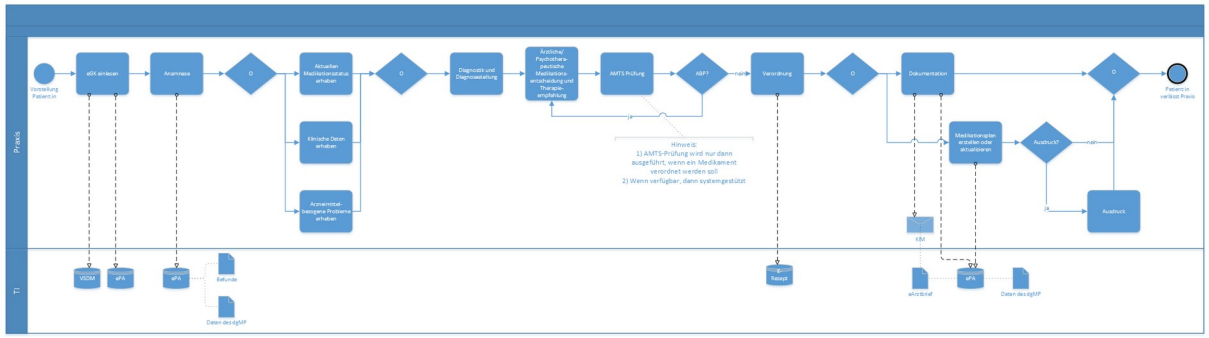


Abbildung 2: Schematisches Prozessmodell zur ePA für Arztpraxen, Zahnarztpraxen und psychotherapeutische Praxen

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 [gemSpec_Aktensystem_ePAfueralle#Legal Policy].

2.2.3 Apotheken

2.2.3.1 Prozesssicht

Für eine Apotheke wird der Zugriff auf die ePA mit dem Abruf der Rezepte, durch das Einlesen der eGKermöglicht oder durch das Aufrufen von einem Stammkunden, der vorhergehend eine Befugnis per ePA-App erteilt hat. Bei einer vorliegenden Befugnis 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, um beispielsweise einen systemgestützten AMTS-Check anzubieten oder die Daten aus der eML anderweitig maschinell weiterverarbeiten zu können.

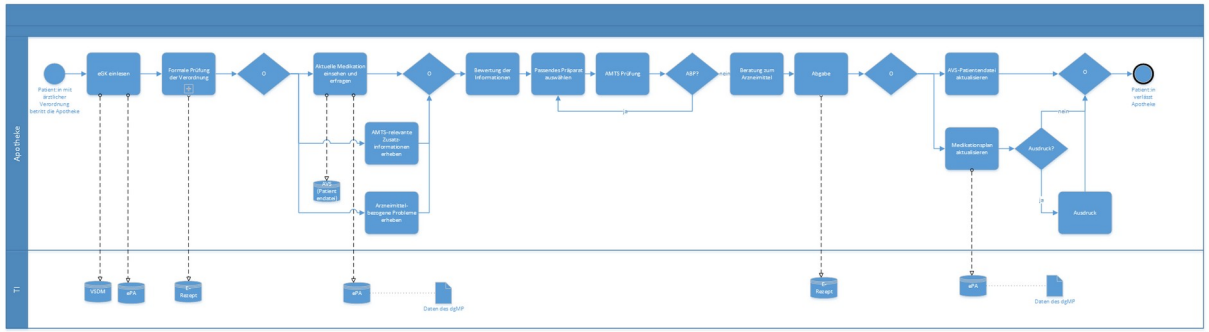


Abbildung 3: Schematisches Prozessmodell zur ePA für Apotheken

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 [gemSpec_Aktensystem_ePAfueralle#Legal Policy].

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.

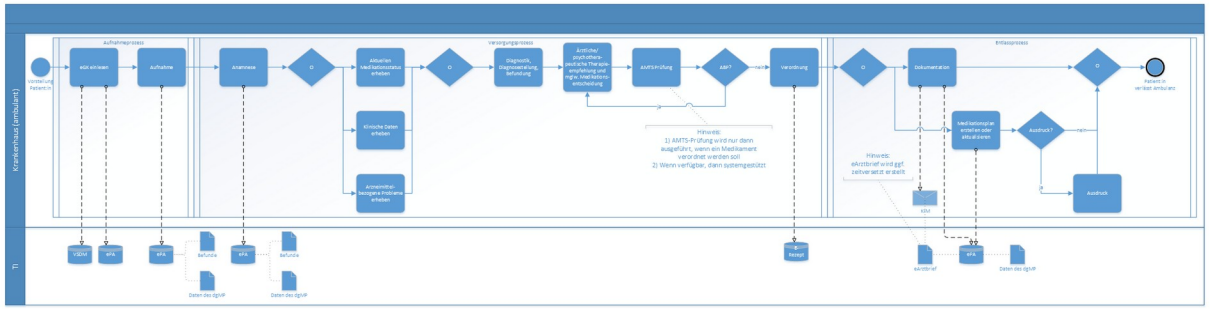


Abbildung 4: Schematisches Prozessmodell zur ePA für Krankenhäuser - ambulant

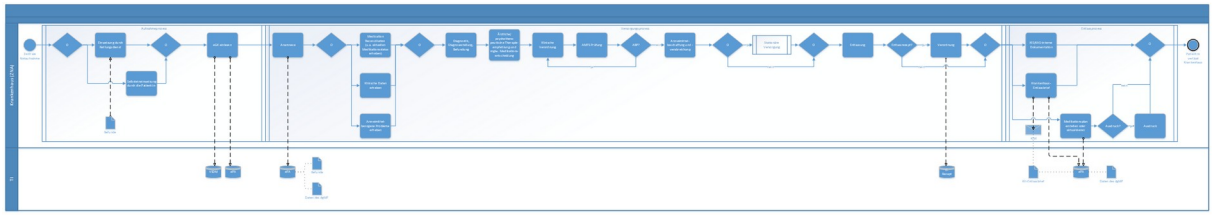


Abbildung 5: Schematisches Prozessmodell zur ePA für Krankenhäuser - zentrale Notaufnahme

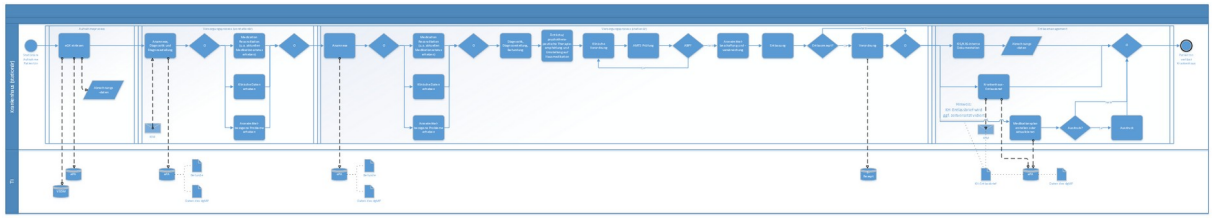


Abbildung 6: Schematisches Prozessmodell zur ePA für Krankenhäuser - stationär

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 startet in allen der drei o.g. Konstellationen mit dem Abgleich der Stammdaten womit der Behandlungskontext hergestellt und die Einrichtung Zugriff auf die ePA erhält. Ebenfalls können Versicherte dem Krankenhaus bereits im Rahmen einer Online-Voranmeldung in einem Patientenportal, bei der Terminbuchung oder über das ePA-FdV eine Zugriffsbefugnis erteilen.

Der Behandlungskontext bezieht sich auf den Behandlungsfall. Im Sinne der Orientierungshilfe KIS (https://www.datenschutzkonferenz-online.de/media/oh/201403_oh_krankenhausinformationssysteme.pdf#_ftn1) 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 ein Krankenhaus als "Vertrauensleistungserbringer" dauerhaft berechtigen möchte oder
  der Versicherte zum Zeitpunkt der Aufnahme seine eGK nicht mit sich führt, oder

- der Versicherte PKV versichert ist, über keine eGK verfügt aber 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. Aus Sicht des ePA-Aktenkontos sind Dokumente, die zur Vorschau im Primärsystem angezeigt werden, bereits heruntergeladen und als Zugriff protokolliert worden.

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. Ebenso können Medikationsdaten des Medication Service zum Zwecke der Medikationsanamnese bzw. der Medication Reconciliation berücksichtigt 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 Leistungserbringerinstitution (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 sie im Rahmen eines erneuten des Stammdatenabgleichs oder durch den Versicherten bzw. einem Vertreter über die ePA-App berechtigt werden.

Die weiteren Festlegungen und Anforderungen an Rollen- und Befugniskonzepte 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 bspw. 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 über seine ePA-App verlängert oder vorzeitig beendet werden. Vor dem Beenden einer Befugnis 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-Aktenkontoeinzustellen. 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 Befugnis 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 Einlesens 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. Der Stammdatenabgleich, der zu einer zur Erneuerung der ePA-Zugriffsbefugnis führt, sollte ebenfalls bei Versicherten durchgeführt werden, deren stationärer Aufenthalt über 90 Tage nach Aufnahme hinausgeht.

Über den E-Rezept-Fachdienst ausgestellte Entlassrezepte werden automatisch über den E-Rezept-Fachdienst in die Medikationsliste der ePA übertragen.

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 [gemSpec_Aktensystem_ePAfueralle#Legal Policy].

2.2.5 Pflege

2.2.5.1 Prozessmodell

In der ePA erfasste Behandlungsinformationen sollten gesichtet und auf Relevanz geprüft werden (siehe Abbildung 7). 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 Darstellung der aktuellen Medikation eines Patienten und umfasst Einnahmehinweise zum Medikament sowie Informationen zu Verordnungen und Dispensierungen. In der ePA ist darüber hinaus eine Medikationsliste vorhanden.Die Medikationsliste wird durch den eRezept Fachdienst erstellt und zeigt alle bislang verordneten Medikamente an. 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.

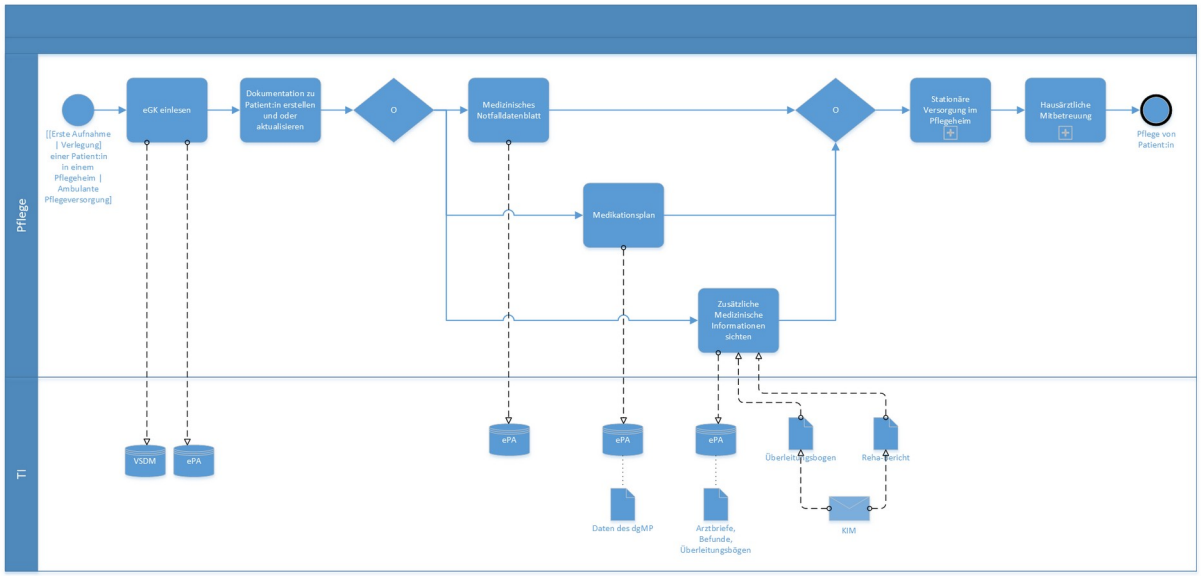


Abbildung 7: Schematisches Prozessmodell zur ePA für die Pflege

2.2.5.2 Anwendungsfälle

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

- Pflegedokumentation

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

- Diagnosen, Befunde, Therapiemaßnahmen
- Medikationsplan
- Notfalldaten
- eArztbrief
- Kinderuntersuchungsheft
- Mutterpass
- Impfpass
- Versichertendokumente
- DiGA-Daten

Eine detaillierte Auflistung der CRUD-Zugriffsrechte ist abrufbar unter [gemSpec_Aktensystem_ePAfueralle#Legal Policy].

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 ein Stammdatenabgleich durchgeführt und daraufhin eine Zugriffsbefugnis erzeugt wird. Zu den Heilmittelerbringern zählen Physiotherapeuten, Ergotherapeuten, Logopäden, Podologen und Ernährungstherapeuten, die sich nach heutigem Stand an die TI anbinden können.

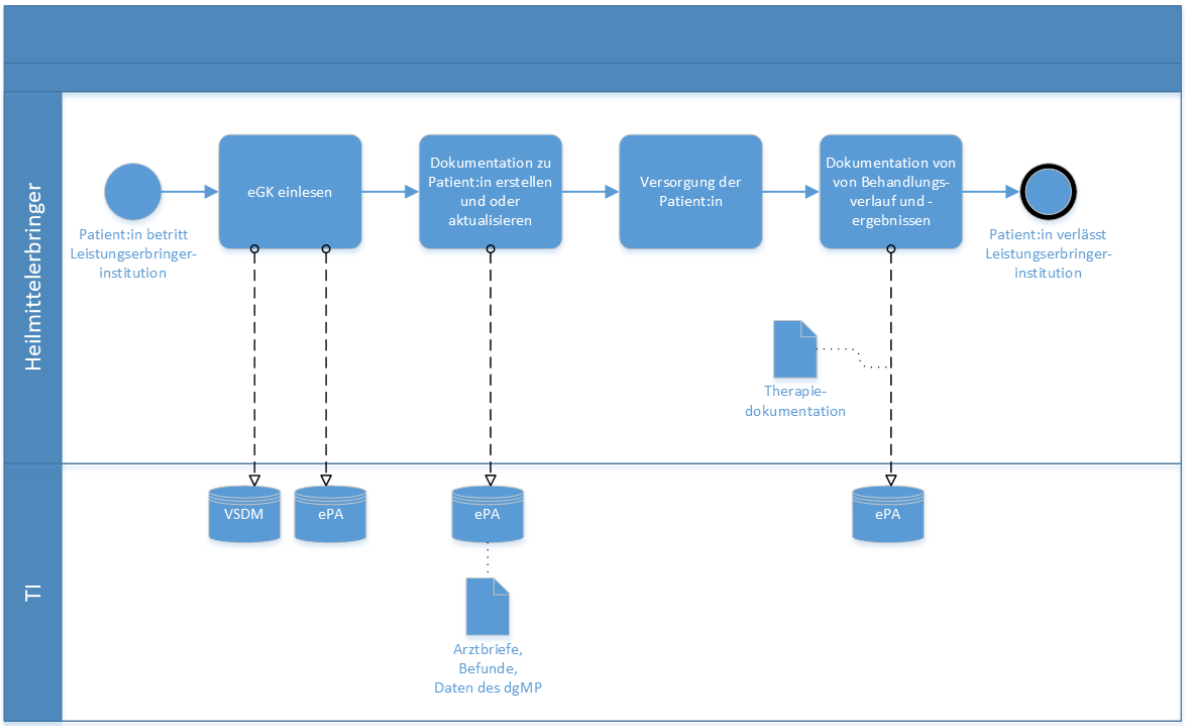


Abbildung 8: Schematisches Prozessmodell zur ePA bei Heilmittelerbringern

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 [gemSpec_Aktensystem_ePAfueralle#Legal Policy].

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

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 = In einer LEI installierter Client gegenüber dem Aktensystem (mit Userinteraktion)
- CS = Außerhalb einer LEI installierter 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	**PS**(alle PS-AFOs, keine CS-AFOs)	gemSST_PS_ePA

	nutzen.		
Kostenträger	Einstellen von Abrechnungsdaten, Aktualisierung der demographischen Daten des Versicherten 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
Ombudsstelle	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 • Widerspruch gegen das Einstellen von Verordnungsdaten und Dispensierinformation durch den E-Rezept-Fachdienst • Widerspruch gegen Übermittlung von pseudonymisierten medizinischen Daten an das Forschungsdatenzentrum Gesundheit (Sekundärdaten) • Widersprüche zu Sekundärnutzungszwecken von Sekundärdaten • Protokolldaten aus	**CS**(Untermenge PS-AFOs, Untermenge CS-AFOs)	gemSST_CS_ePA_Ombudsstelle

	dem Aktenkonto herunterladen.		
DiGA	Einstellen von DiGA-Daten	**CS**(Untermenge PS-AFOs, Untermenge CS-AFOs)	gemSST_CS_ePA_DiGA

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 und KZBV (siehe https://www.kbv.de/praxis/digitalisierung/it-sicherheit und https://www.kzbv.de/zahnaerzte/digitales/it%E2%80%90sicherheit/)

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_24680-01 -Useragent im Nachrichtenheader
Das PS MUSS den eigenen Useragent im x-header-Element "x-useragent" bei jedem Request (auch beim VAU-Handshake) sowohl im HTTP-Header der VAU-Nachricht, als auch im HTTP-Header der Nachricht an den Service einfügen [vgl. gemSpec_Aktensystem_ePAfueralle#2.7].**[<=]**

Hinweis zum x-useragent: gemäß gemSpec_Aktensystem_ePAfueralle#2.7 besteht der Useragent (welcher im x-useragent einzutragen ist) aus Client-ID und Versionsnummer des Primärsystems (durch "/" voneinander getrennt). Die Client-ID wird durch die gematik vergeben und übermittelt, sobald sich ein (Client-)Produkthersteller unter https://fachportal.gematik.de/formulare-product-id/neuanlage registriert hat. Dazu ist im Rahmen dieser Registrierung der Name des Herstellers und der Name des zu registrierenden Produktes zu übermitteln. Sollte für eine andere TI-Anwendung bereits eine Registrierung vorgenommen worden sein, kann die Client-ID auch im ePA-Kontext genutzt werden (sofern es sich um das gleiche Softwareprodukt handelt). In diesem Fall sollte eine Anpassung der Verwendungszwecke der Client-ID/product-id unter https://fachportal.gematik.de/formulare-product-id/aenderung-zwecke-der-product-id vorgenommen werden. Die Versionsnummer kann im Rahmen der erlaubten Zeichen vom Hersteller frei gewählt werden und sollte bei ePA-relevanten Änderungen des Produkts aktualisiert werden. In den Formularen ist immer von "product-id" die Rede, da der Useragent zukünftig aus product-id und Versionsnummer bestehen wird - es ändert sich dabei aber nur der Name.

A_27705 -Requestkennung im Nachrichtenheader
Das PS KANN für einen Request eine Requestkennung als UUID erzeugen und die Requestkennung im HTTP Header Element mit dem Namen "X-Request-ID" sowohl im HTTP-Header der VAU-Nachricht, als auch im HTTP-Header der Nachricht an den Service senden.**[<=]**

A_27447 -Nutzung Terminologiepaket
Das PS MUSS die relevanten Terminologien des Terminologiepakets gemäß [gemIG_TI_Terminology] verarbeiten und in allen Services des ePA-Aktensystems berücksichtigen.**[<=]**

Hinweis zu A_27447:
Das Terminologiepaket wird als FHIR-Package bereitgestellt und enthält z.B. Vocabulary ePA und Value Set für Berechtigungskategorien.

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 übergreifende 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 gemäß https://service.gematik.de/servicedesk/customer/kb/view/729781779 gebildet).

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 (die Parameter "ePA-Anbieter-Zahl" und "Umgebung" sind dem o.a. Link zu entnehmen).

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_24380-01 -Endpunkt Schnittstelle ePA-Aktensysteme
Das Primärsystem MUSS die URL für die Kommunikation mit den ePA-Aktensystemen je nach Service, ePA-Aktensystem und Umgebung gemäß `[gemSpec_Aktensystem_ePAfueralle#2.1]` 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 Initiierung des VAU-Kanals.

Das Dokumentenmanagement in der ePA für alle rund um das IHE-Kernprofil `XDS.b` (Cross-Enterprise Document Sharing) findet innerhalb des VAU-Kanals statt.

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.

Die Home Community ID, die in ePA 2.x zur Identifikation eines Aktensystems zum Einsatz kam, wird nicht mehr benötigt und wird entsprechend nicht mehr in den Operationen der Aktensystem-API gefordert.

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.

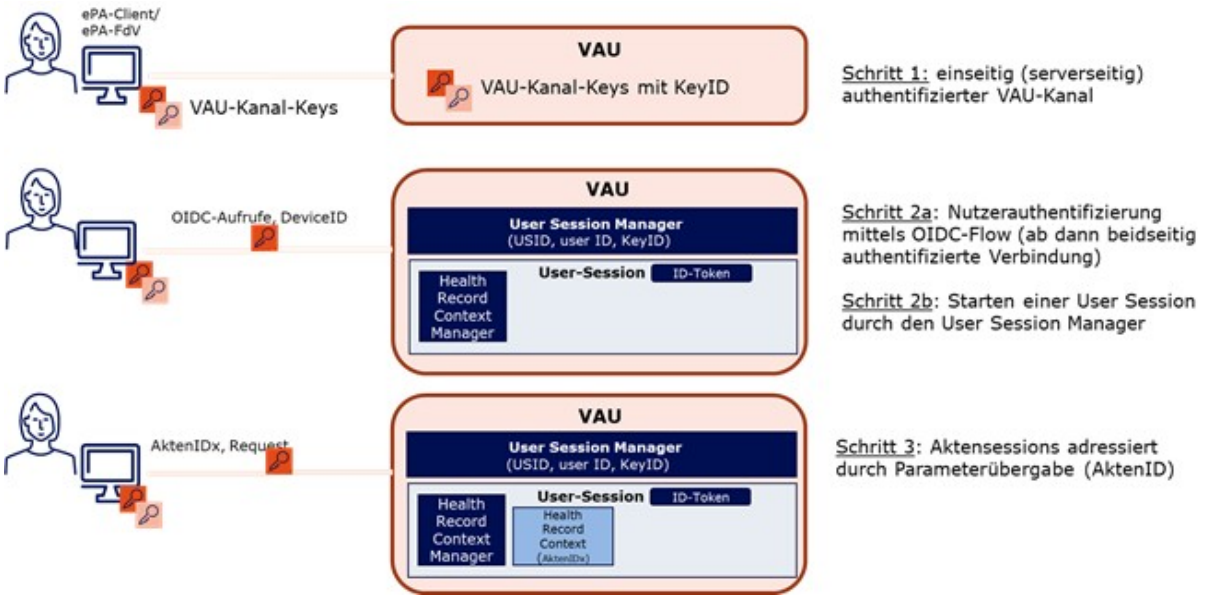


Abbildung 9: Überblick über Aufbau VAU, User Session und Aktensession

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:

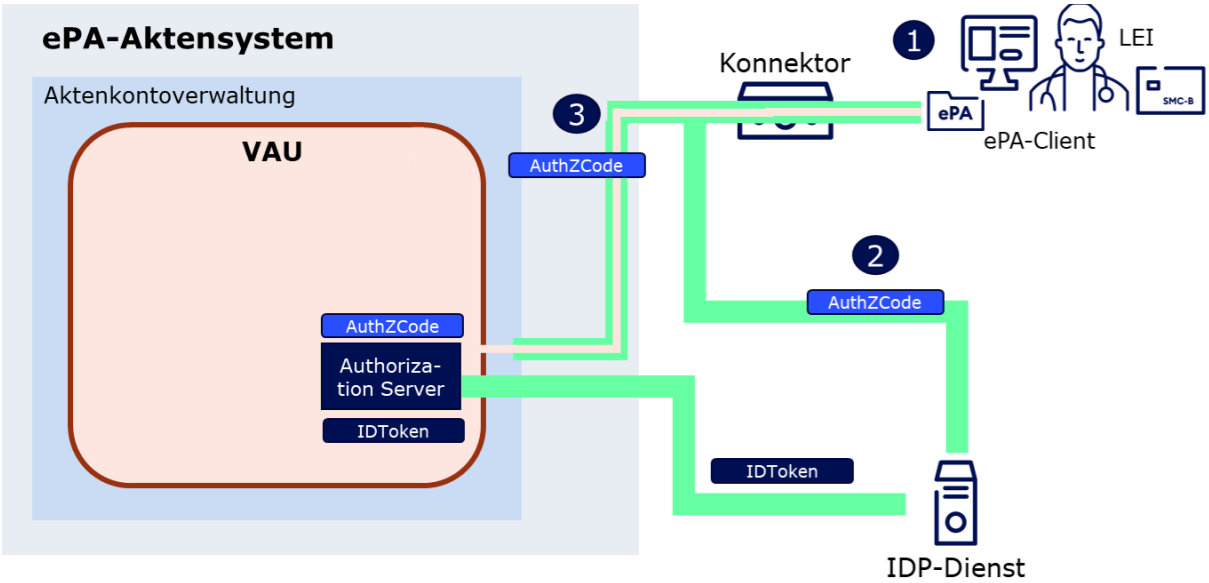


Abbildung 10: Überblick über Nutzerauthentifizierung

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:

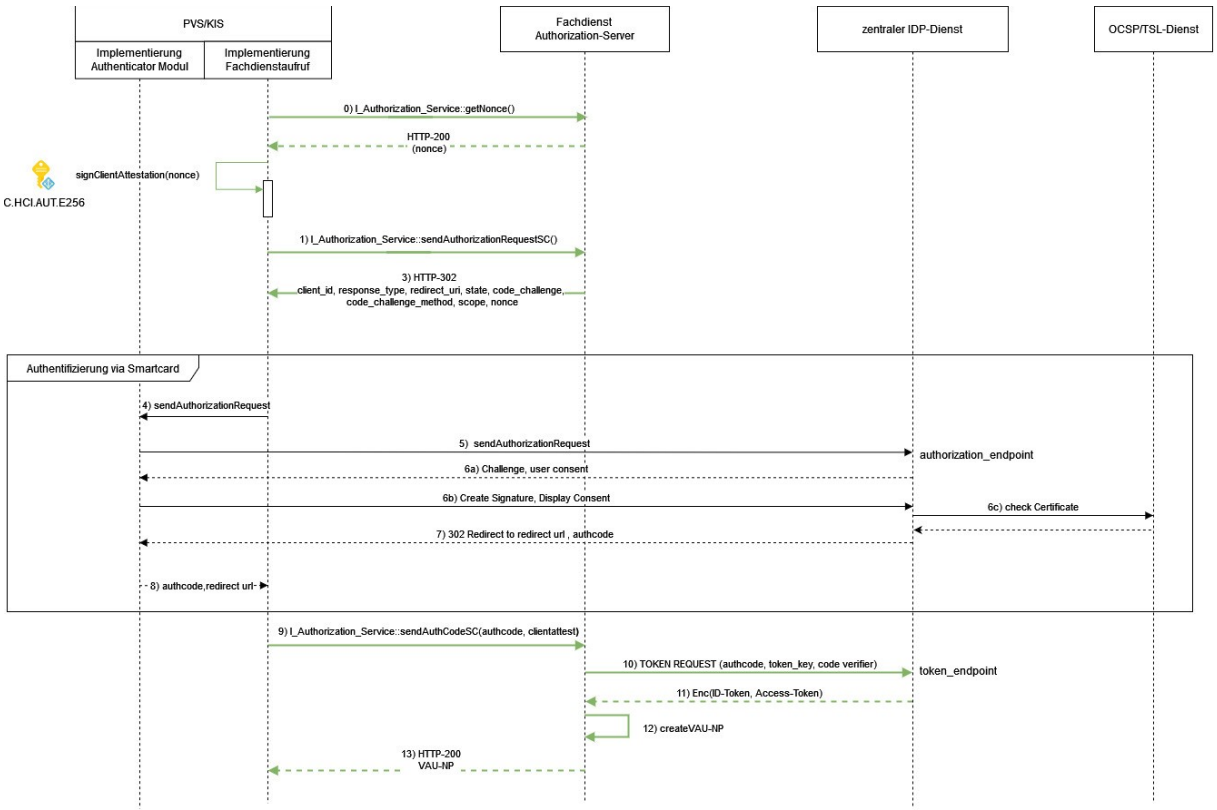


Abbildung 11: Detaillierter Nachrichten-Flow für die Nutzerauthentifizierung mit dem IDP-Dienst

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_24883-04 -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.**[<=]**

A_26818 -Formatkonvertierung bei ECDSA basierter clientAttest-Signatur
Das PS MUSS nach erfolgter Signatur des clientAttest-JWT mit Operation ExternalAuthenticate den Signatur-Typ ermitteln, indem aus der Response das XML-Attribut ausgewertet wird.
Ist der Wert des Signatur-Typ urn:bsi:tr:03111:ecdsa, so wurde durchExternalAuthenticate eine ECDSA-Signatur erstellt und das XML-Attribut`dss:SignatureObject/dss:Base64Signature` aus der Response MUSS vom PS vor weiterer Verwendung als signiertes clientAttest-JWT vom X9.62 Format gem. [BSI-TR-03111]#5.2.2 in das für ECDSA-Signaturen benötigte Concatenated-Format gem. [RFC 7518]#3.4 konvertiert werden.
[<=]

Referenzimplementierungen für die Konvertierung:

- https://github.com/gematik/app-Authenticator/blob/2d0f87968be5540d67e75f36fbdd3bc9cb444aad/src/renderer/modules/gem-idp/services/signing-service.ts#L68
- https://github.com/ere-health/ere-ps-app/blob/main/src/main/java/health/ere/ps/service/connector/auth/SmcbAuthenticatorService.java#L208
- https://bitbucket.org/andreas_hallof/vsdm2/src/main/sig-conv.py

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

siehe auch: [gemSpec_Aktensystem_ePAfueralle#A_25444-*]

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_25720-01 -Auslesen des Authentisierungszertifikates aus einem HSM
Ein Clientsystem MUSS bei Nutzung eines Basis-Consumers das Zertifikat `C.HCI.AUT` der SM-B über die Operation `ReadCertificate` gemäß [gemSpec_Kon#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.

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 "client-ID" (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_20662-01 -CS: Annahme des "user_consent" und des CHALLENGE_TOKEN
Das Clientsystem 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 Clientsystems.**[<=]**

A_20663-02 -CS: Prüfung der Signatur des CHALLENGE_TOKEN
Das Clientsystem MUSS die Signatur des CHALLENGE_TOKEN gegen den aktuellen öffentlichen Schlüssel des Authorization-Endpunktes PUK_IDP_SIG prüfen. Liegt dem Clientsystem 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_20665-02 -CS: Signatur der Challenge des IdP-Dienstes

Das Clientsystem MUSS, wenn es sich mit seiner SM-B authentisiert, den CHALLENGE_TOKEN des IdP-Dienstes mit der Identität ID.HCI.AUT der SM-B signieren. Das Clientsystem MUSS, wenn es den Konnektor oder den Basis-Consumer nutzt, für das Signieren die Operation ExternalAuthenticate 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_20667-02 -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: DerAufbau der Anfrage und der einzureichenden Objekte entspricht [gemSpec_IDP_Dienst#7.3].

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_20668-01 -CS: Annahme des AUTHORIZATION_CODE
Das Clientsystem MUSS den vom Authorization-Endpunkt als Antwort auf die signierte Challenge gesendeten AUTHORIZATION_CODE verarbeiten. Das Clientsystem 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_20655-01 -CS: Regelmäßiges Einlesen des Discovery Document
Das Clientsystem 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 Clientsystems beim IDP-Dienst übergeben.
Das Clientsystem MUSS den Downloadpunkt des Discovery Document als konfigurierbaren Parameter speichern.**[<=]**

A_20656-02 -CS: Prüfung der Signatur des Discovery Document
Das Clientsystem MUSS die JWS (JSON Web Signature) [RFC7515#section-3] Signatur des Discovery Document auf mathematische Korrektheit sowie auf Gültigkeit des ausstellenden Zertifikates innerhalb der TI prüfen.
Das Clientsystem MUSS, wenn es den Konnektor oder den Basis-Consumer nutzt, die Gültigkeit des Zertifikates mit der Operation "VerifyCertificate" prüfen.
[<=]

*Hinweis:*Der genaue Aufbau entspricht [gemSpec_IDP_Dienst#7.7].

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_20657-01 -CS: Prüfung Typ und Rolle des Signaturzertifikats des Discovery Document
Das Clientsystem 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 oder den **EHR Information Service** innerhalb 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" (http 404)

zurück, wiederholt das Primärsystem den Aufruf bei den weiteren Aktensystemen.

Gibt der Informationsdienst eine "Statusabweichung" (http 409) zurück, dann ist das Aktenkonto diesem Aktensystem zugeordnet, es kann aber derzeit nicht produktiv genutzt werden. Da die "Statusabweichung" (http 409) durch einen Umzug des Aktenkontos zu einem neuen Anbieter verursacht sein kann, und dort gegebenenfalls schon verfügbar ist, werden auch noch die weiteren Aktensysteme nach einem verfügbaren Aktenkonto (http 204) angefragt.Gibt es ein solches Aktensystem, welches ein verfügbares Aktenkonto meldet (http 204), dann wird dessen Endpunkt verwendet, ansonsten der Endpunkt des Aktensystems mit dem derzeit nicht produktiv nutzbaren Aktenkonto (http 409).C

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.

Tabelle 6: I_Information_Service::getRecordStatusV2

REST-Schnittstelle des Aktensystems (Nutzung innerhalb des VAU-Kanals)	
I_Ehr_Information_Service	
`getRecordStatusV2`	Diese Operation ermittelt, ob für die übergebene KVNR ein Aktenkonto existiert und in welchem Status es ist.

A_24499-01 -Nutzung der Operationen der Information Services
Das PS MUSS die Operation getRecordStatus gemäß [I_Information_Service] oder getRecordStatusV2 gemäß [I_Ehr_Information_Service] nutzen.**[<=]**

A_24435-02 -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.
Zur Ermittelung des Aktensystems für ein Aktenkonto werden diese in zufälliger Reihenfolge angefragt, bis ein aktiviertes Aktenkonto gefunden wird (http 204). Bleibt diese Suche erfolglos, wird nach einem aktiven, aber derzeit nicht produktiv nutzbarem Aktenkonto (http 409) gesucht.**[<=]**

Die Zuordnung zwischen KVNR und IK-Nummer des Versicherten erfolgt primärsystemspezifisch und ist nicht weiter vorgegeben.

Sind alle Abfragen negativ (http 404), 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_26259-01 -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 "`NoHealthRecord`" (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 für eine Operation über die Angabe der KVNR des Versicherten. Diese wird als HTTP Header Element mit dem Namen "x-insurantId" gesendet.
Die Verwendung ist für alle Operationen der Medical Services erforderlich (SOAP-Operationen des XDS Document Service und FHIR-Operation der FHIR Data Services). Für Services des Aktensystems mit OpenApi-Schnittstellen ist die Anforderung zur Verwendung des Elements in der jeweiligen Definition der Operation vorgegeben.

A_24998-01 -InsurantID im Nachrichtenheader
Das PS MUSS bei Aufrufen, die ein adressiertes Aktenkonto erfordern, die KVNR des Kontoinhabers (Versicherter) in einem HTTP Header Element mit dem Namen "x-insurantId" senden.**[<=]**

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 7: 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_24900-01 -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:

Tabelle 8 : Parameter der TI-Zertifikate

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

Zusätzlich MÜSSEN die im Zertifikat enthaltene Rollen-OIDs oid_epa_dvw bzw. oid_epa_vau sein.
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-Antwort 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. In diesem Kontext würden unterschiedliche Mandanten einer Einrichtung unterschiedliche Telematik-IDs verwenden. Wenn eine LEI mehrere Telematik-IDs besitzt, ist es womöglich erforderlich, innerhalb dieser LEI Befugnisse für mehrere Telematik-ID-Domänen (für mehrere Mandanten) separat zu generieren.

Die Nutzung ePA-fähiger Aufrufkontexte ist in kleineren Einrichtungen mit nur einer einzigen verwendeten SMC-B und Telematik-ID 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. Dadurch wird für einen Client mit dieser Telematik-ID Zugriff auf die Patientenakte gewährt, sofern eine Befugnis für diese Telematik-ID besteht.

A_24401-01 -Mandantenweite Verwendung der korrekten SMC-B
Das PS MUSS sicherstellen, dass bei Vorhandensein mehrerer Mandanten bzw. Telematik-IDs in einer LEI für jede Telematik-ID nur die zugehörige SM-B für den Aufbau der VAU, die Erstellung der Befugnis-Signatur und das IDP-Token verwendet wird.**[<=]**

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

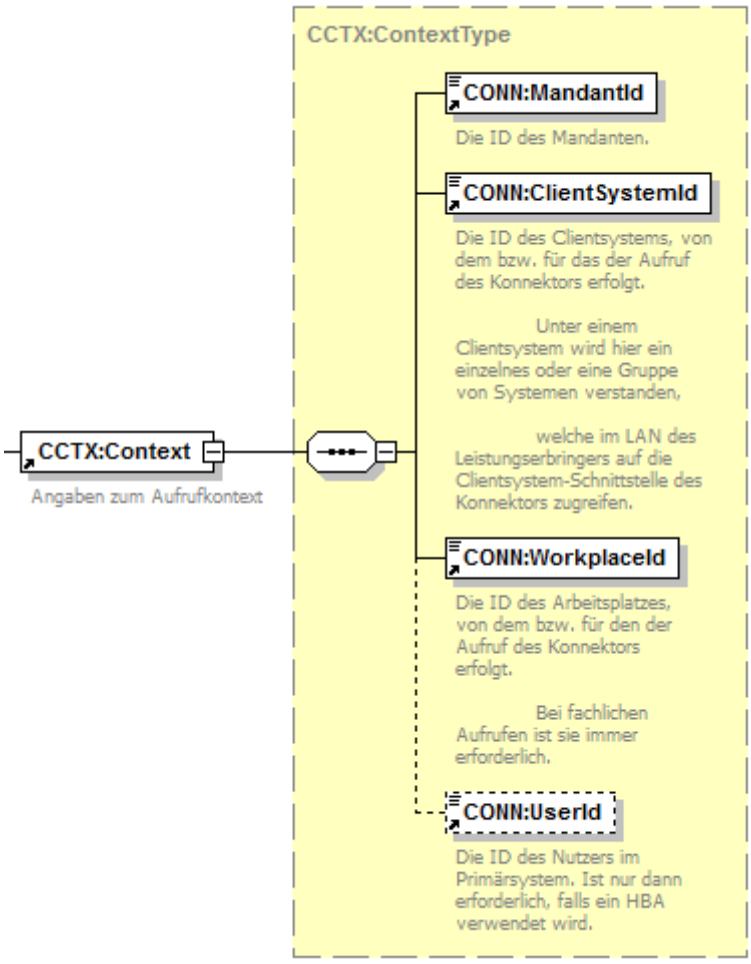


Abbildung 12: ILF_ePA_Element_Context

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 oder durch Durchführen eines alternativen PoPP-Verfahrens mittels GesundheitsID, eine Befugnis eingestellt.

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.

Der Auslöser zur Erstellung einer Befugnis ist der erste Praxisbesuch im Quartal, die Aufnahme im Krankenhaus oder die Einlösung eines E-Rezeptes mit eGK in der Apotheke.

Derzeit gibt es zwei Möglichkeiten einen Behandlungskontext in der ePA für alle nachzuweisen und eine Befugnis zu erlangen: Über ein PoPP-Token oder über eine signierte VSDM-Prüfziffer. Die VSDM-Prüfziffer wird aber nur noch für eine Übergangszeit akzeptiert, so dass zukünftig ausschließlich ein PoPP-Token vom Aktensystem akzeptiert wird.
Sowohl VSDM-Prüfziffer als auch PoPP-Token können nur einmalig zum Erzeugen einer Befugnis genutzt werden.

Der Zeitpunkt für die Abweisung von Befugnisregistrierungen mit VSDM-Prüfziffern ist abhängig von der Bereitstellung des PoPP-Services für ePA. Sobald diese Bereitstellung in der PU erfolgt, wird das Aktensystem seine Dualmode-Fähigkeit (Akzeptanz von PoPP-Token UND VSDM-Prüfziffer) für ein Jahr aufrecht erhalten.

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 Operationen des **Entitlement Management** des Aktensystems:

Tabelle 9: I_Entitlement_Management::setEntitlementPs

REST-Schnittstelle des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)	
I_Entitlement_Management	
`setEntitlementPs`	Diese Operation registriert eine Befugnis über eine VSDM-Prüfziffer im Entitlement Management.
`setEntitlementPsV2`	Diese Operation registriert eine Befugnis über ein PoPP-Token im Entitlement Management.

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].**[<=]**

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

3.9.1 Erstellen einer Befugnis mittels PoPP

In diesem Kapitel wird die Erstellung einer Befugnis mittels eines PoPP-Tokens beschrieben.

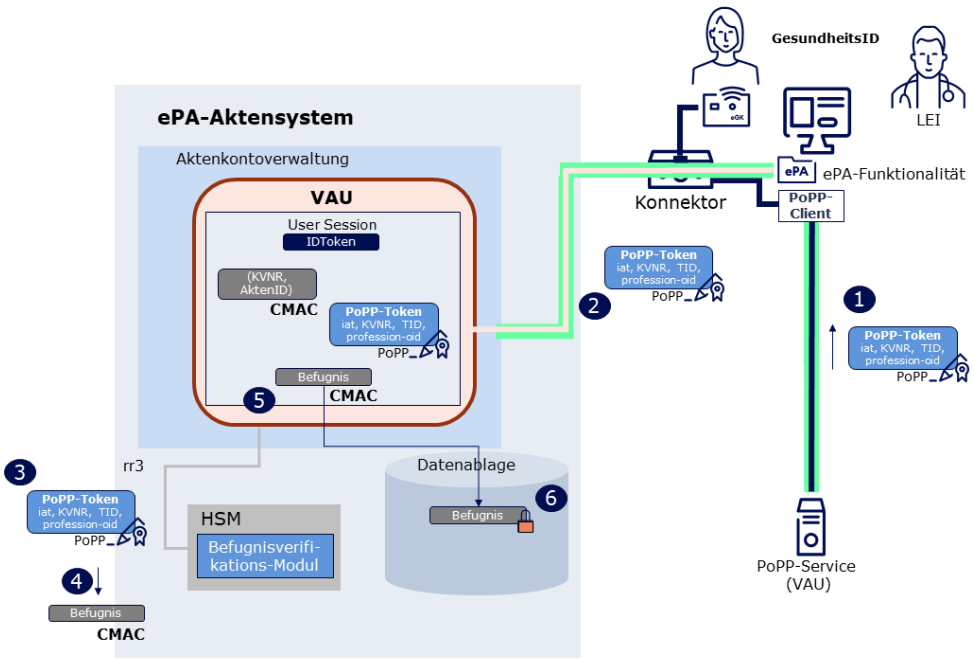


Abbildung 13: Ablauf Erstellung einer Befugnis mittels PoPP

Das PoPP-Token wird über den lokalen PoPP-Client in Verbindung mit dem PoPP-Service abgerufen und bestätigt den Behandlungskontext zwischen dem Versicherten und der Institution. Das PoPP-Token kann direkt im Entitlement Management des Aktensystems als Befugnis registriert werden.

3.9.1.1 Umsetzung

Die Aktivitäten des Anwendungsfalles *Erstellen einer Befugnis mittels PoPP* sind:

Vorbedingung:

- Ermittelter `Service-Endpunkt` zum Aktenkonto
- erfolgreicher Abruf eines PoPP-Tokens vom PoPP-Service

Auslöser:

- Erhalt des PoPP-Tokens z.B. im Zusammenhang mit dem Abruf der VSDM-Stammdaten
- manuelle Auslösung
- Nachfrage bei uploadpflichtigen PS-Aktionen und fehlender Befugnis

Aktivitäten:

- Auswahl KVNR
- Auswahl des `Service-Endpunkts` zum Aktenkonto
- Auswahl des PoPP-Tokens
- PoPP-Token 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 für die Erstellung des PoPP-Token nicht zur Gruppe der gesetzlich für diese Operation erlaubten Berufsrollen (professionOID) gehört oder wenn die konkrete LEI vom Versicherten geblockt wurde.
- Die Antwort enthält im Erfolgsfall mit dem *validTo* das Enddatum der Befugnisdauer. Das PS kann die Befugnisdauer persistieren.

3.9.1.2 Nutzung

A_27631 -Das Entitlement in zeitnahem Kontext des PoPP-Tokens in die ePA hochladen
Nach Abruf eines PoPP-Tokens für einen bestimmten Versicherten MUSS das PS das PoPP-Token innerhalb von 20 Minuten als Entitlement für einen Zugriff auf seine Akte über die Schnittstelle I_Entitlement_Management in die ePA einstellen.**[<=]**

A_27632 -Nutzung des PoPP Clients zum Abruf eines PoPP-Tokens
Das PS MUSS das PoPP-Token unter Verwendung des PoPP-Clients vom PoPP-Service beziehen.**[<=]**

3.9.2 Erstellen einer Befugnis mittels VSDM

In diesem Kapitel wird die Erstellung einer Befugnis mittels einer VSDM-Prüfziffer beschrieben.

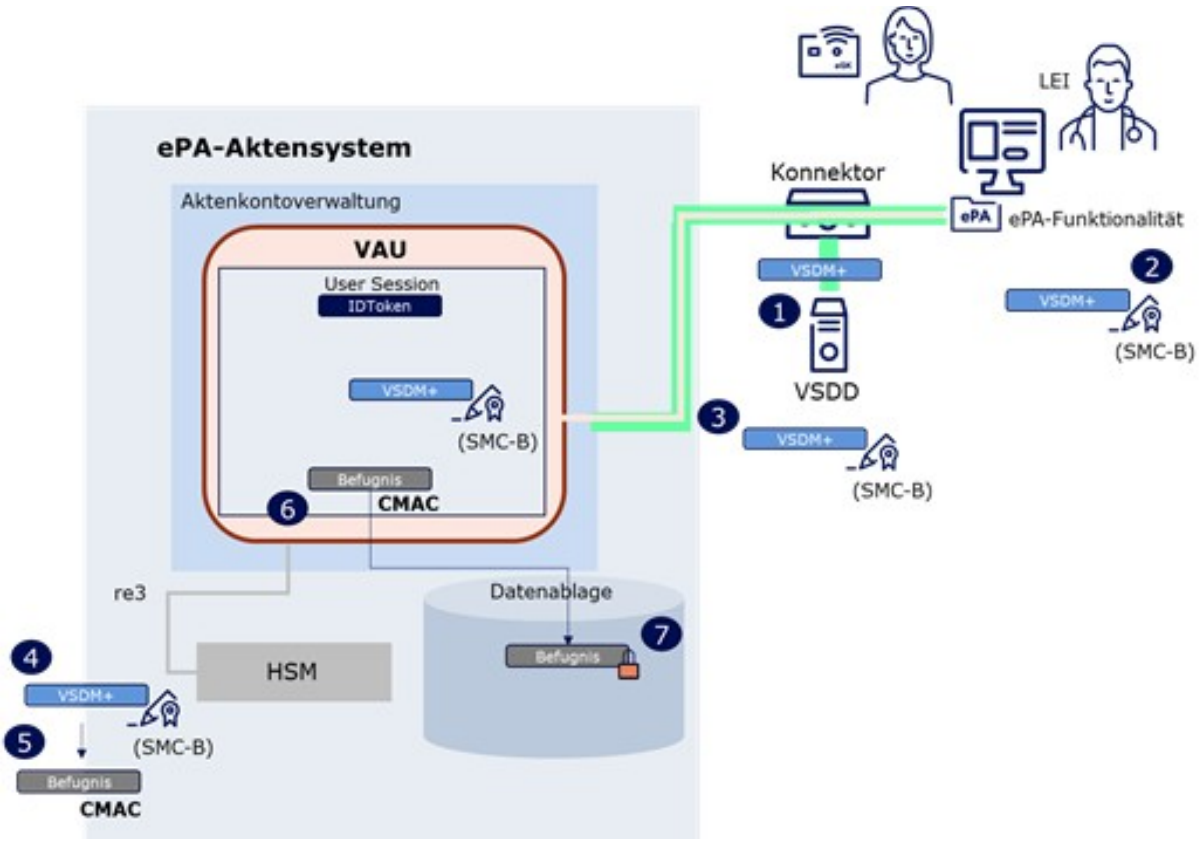


Abbildung 14: Ablauf Erstellung einer Befugnis mittels VSDM

Der Auslöser zur Erstellung einer Befugnis ist das etablierte Lesen der eGK mit Onlineprüfung (d.h.mit den Parametern `PerformOnlineCheck=true` und `ReadOnlineReceipt=true`) 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 E-Rezeptes mit eGK in der Apotheke durchgeführt.

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 Onlineprüfung (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.

Durch den beschriebenen Ablauf wird sichergestellt, dass der erste Besuch im Quartal im Allgemeinen zum Einstellen einer Befugnis führt. Für weitere Besuche in einer Leistungserbringer-Institution wird empfohlen, dass das PS versucht, direkt auf die Akte des Versicherten zuzugreifen. Falls kein Zugriff auf die Akte möglich ist (Akte ist vorhanden) und dieser gewünscht wird, sind folgende Schritte notwendig:

- eGK in KT stecken
- Button/Menüpunkt: Erstellen der Befugnis wiederholen (löst ein ReadVSD mit Onlinprüfung aus und erstellt danach das Entitlement)

3.9.2.1 Umsetzung

Die Aktivitäten des Anwendungsfalles *Erstellen einer Befugnis mittels VSDM* sind:

Vorbedingung:

- Ermittelter `Service-Endpunkt` zum Aktenkonto
- erfolgreiches ReadVSD mit Onlineprüfung

Auslöser:

- Erhalt einer Prüfziffer durch Lesen der eGK mit erfolgreicher Onlineprüfung (Prüfnachweis 1 oder 2)
- manuelle Auslösung
- Nachfrage bei uploadpflichtigen PS-Aktionen und fehlender Befugnis

Aktivitäten:

- Auswahl KVNR
- Auswahl des `Service-Endpunkts` zum Aktenkonto
- Auswahl der Prüfziffer des Versicherten und
- Bildung des Hash Check Value (hcv)gemäß A_27352* [gemSpec_Krypt]: Die Werte für die Berechnung des hcv-Wertes werden aus`UC_AllgemeineVersicherungsdatenXML.Versicherter.Versicherungsschutz.Beginn (VB)` und `UC_PersoenlicheVersichertendatenXML.Versicherter.Person.StrassenAdresse.Strasse (SAS)`der ReadVSDResponse entnommen. Die Daten sind dort in der Zeichenkodierung ISO-8859-15 (Latin 9) kodiert. Diese Kodierung ist auch bei der Berechnung des hcv-Wertes zu verwenden.
- Der berechnete hcv-Wert MUSS base64 kodiert werden.
- Die Prüfziffer des Versicherten MUSS base64 kodiert werden.
- Bildung eines JWS mit Prüfziffer und Zertifikat der SMC-B gemäß [gemSpec_Aktensystem_ePAfueralle#A_24590-*]
- JWS signieren mit SMC-B
- signiertes 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 gesetzlich für diese Operation erlaubten Berufsrollen (professionOID) gehört oder wenn die konkrete LEI vom Versicherten geblockt wurde.
- Die Antwort enthält im Erfolgsfall mit dem *validTo* das Enddatum der Befugnisdauer. Das PS kann die Befugnisdauer persistieren.

3.9.2.2 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_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_24540-01 -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.**[<=]**

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.

A_27402 -Kodierung der Daten zur Berechnung von hcv
Das PS MUSS bei der Erstellung einer Befugnis den hcv gemäßA_27352 ermitteln und dabei sicherstellen, dass VB und SAS aus ReadVSDResponse ohne Änderung und Umkodierung für die Erzeugung des hcv verwendet werden.**[<=]**

Hinweis: Die Versichertendaten werden nach Spezifikation VSDM [gemSpec_eGK_Fach_VSDM], in ISO-8859-15 (Latin-9) vom eGK-Personalisierer und vom VSDM-FD kodiert eingebracht. Der verwendete Zeichensatz für die fachlichen Inhalte ist ISO8859-15.

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 von Medikationsdaten über einen 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 10: 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 Operation getConsentDecisionInformation 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 Beitrag der ePA zum digital gestützten Medikationsprozess (dgMP) wird über den Medication Service umgesetzt, dessen Daten als elektronische Medikationsliste (eML) und als elektronischer Medikationsplan (eMP) vom Leistungserbringer über das Primärsystem abgerufen und angezeigt werden können.

Der FHIR Implementation Guide [gemIG_ePA_Medication] beschreibt Anforderungen an das Primärsystem zur Umsetzung der dgMP-Prozessabläufe.

3.11 Dokumentenmanagement

Für das Dokumentenmanagement in der ePA werden aktuell zwei verschiedene Schnittstellen angeboten, die in diesem Abschnitt näher beschrieben werden: XDS und MHD.

Während XDS seit der ePA 3.0 im Einsatz ist, wurde MHD mit der Version 3.1.3 in der ePA eingeführt, zunächst begrenzt auf das Suchen von Dokumenten inklusiven den Möglichkeiten einer Volltextsuche. Mit Start der ePA 27 wurde dann der ePA MHD Service um andere typische Dokumentenmanagement-Features wie das Einstellen, Aktualisieren und Löschen von Dokumenten ergänzt. Mit dieser Erweiterung wird auch gleichzeitig damit begonnen, den XDS Document Service zurückzubauen. Bereits in ePA 27 sind nicht mehr alle Operationen auf allen Dokumenten mit XDS möglich; einige Altdaten jedoch können weiterhin ausschließlich mit XDS und nicht mit MHD verwaltet werden.

Die folgenden Abschnitte stellen den aktuellen Stand dar. Weitere Anforderungen finden sich in [gemSpec_Aktensystem_ePAfueralle] und [gemIG_ePA_MHD].

Sofern nicht explizit anders gekennzeichnet, beziehen sich alle Anforderungen im Kapitel 3.11 zum Dokumentenmanagement auf den XDS Service.

3.11.1 Grundlegende Anforderungen für XDS

Die traditionelle Schnittstelle für das Dokumentenmanagement durch PS nutzt eine Profilierung der IHE-Spezifikationen rund um das Kernprofil `XDS.b` (Cross-Enterprise Document Sharing):

Tabelle 11: 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_24661-04 -Nutzung der Dokumentenmanagement-Schnittstelle I_Document_Management
Das PS KANN die Aktensystemschnittstelle`I_Document_Management` gemäß [gemSpec_Aktensystem_ePAfueralle] 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-TF2#3.39.5] mit Verweis auf [IHE-ITI-TF2#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.**[<=]**

Duplikat-Handling

XDS Document Service und ePA MHD Service liefern mit den Dokumentenmetadaten (`DocumentEntry.hash` in XDS und `DocumentReference.attachment.hash` in MHD) die Prüfsumme des Dokuments. Mithilfe dieser Prüfsumme kann ein PS lokal prüfen, ob ein einzustellendes Dokument bereits im Aktensystem vorliegt, um nicht unnötig zu versuchen, Duplikate von Dokumenten in die ePA einzustellen oder auch Dokumente mehrfach herunterzuladen.

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

Ab ePA 3.1.3 Umsetzungsphase 2 gibt das Aktensystem im `codeContext`-Attribut des zurückgegebenen`rs:RegistryError`-Elements gemäßA_24988* an:
1. Ursache des Fehlers mit `"errorText='Cannot register document: Duplicate already exists'"`

2. die Liste der UUIDs (DocumentEntry.entryUUID), der in der Akte identifizierten bereits vorhanden Dokumente mit:
"`entryUUID=`<entryUUID von document_1>`;entryUUID=`<entryUUID von document_2>`;...;entryUUID=`<entryUUID von document_n>"

Weitere Erläuterungen hierzu gibt es in Kapitel 7.2.2- Erweiterte Angaben des Aktensystems zum Fehler in codeContext .

In MHD hingegen werden Duplikate standardmäßig akzeptiert, sofern der masterIdentifier des Dokuments und der Hash identisch sind. **TODO: Weitere Fälle aufführen.**

Ordner

Ordner können über XDS auf Basis der XDS-Option `Folder Management` (PS als 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` und `diga`) 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 gelöscht werden, werden dadurch auch Dokumente gelöscht, die mit ihnen über Assoziationen verbunden sind.

Weitere übergreifende 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.

Im Rahmen von MHD können gar keine eigenen Ordner angelegt werden, da die statischen Ordner zur Verwaltung von Kategorien bereits vorhanden sind und dynamische Dokumentensammlungen über MHD nicht verwaltet werden können. In MHD werden FHIR List-Ressourcen verwendet, um sowohl Folder als auch SubmissionSets abzubilden.

3.11.2 Anforderungen für MHD

Die Anforderungen an Primärsysteme für die Umsetzung der MHD-Schnittstelle finden sich vornehmlich entsprechenden FHIR IG[gemIG_ePA_MHD].

A_30405 -Nutzung der Dokumentenmanagement-Schnittstellen des ePA MHD Service
Das PS MUSS die Anforderungen an die `ePA-Schnittstelle eines PS` gemäß [gemIG_ePA_MHD] implementieren.
[<=]

Nur an wenigen Stellen beschreibt der vorliegende Leitfaden informative Ergänzungen zum MHD IG, insbesondere dann, wenn es um die Abgrenzung zum traditionellen XDS Document Service geht.

3.11.3 Dokumente einstellen [ITI-41]

Dokumente, SubmissionSets und Folder

Pro Upload-Anfrage an das Aktensystem können ein oder mehrere Dokumente eingestellt werden. Alle Dokumente in einer Anfrage werden entweder ganz oder gar nicht vom Aktensystem akzeptiert. Zu jedem Dokument müssen entsprechende Metadaten (in einem "DocumentEntry" genannten Objekt) mit hochgeladen werden. Das Bündel gemeinsam eingestellter Dokumente (sozusagen der "Briefumschlag", in dem diese Dokumente geliefert werden) heißt "SubmissionSet", in dem ebenfalls einige Metadaten (wie z. B. die einstellende Praxis) hinterlegt werden müssen. Das SubmissionSet wird neben den Dokumenten mit ihren DocumentEntries vom Aktensystem gespeichert. Die Beziehung zwischen SubmissionSet und DocumentEntries (d.h. also, welche Dokumente gemeinsam und mit welchem "Briefumschlag") eingestellt wurden, wird ebenfalls beim Einstellen jeweils über eine sogenannte Association mitgeliefert und vom Aktensystem mit persistiert.

Das Aktensystem ist in Datenkategorien organisiert, die über sogenannte "Folder" (Ordner) umgesetzt werden. Um ein Dokument beim Einstellen einem bestimmten Ordner zuzuordnen, wird ebenfalls über einen bestimmten Typ "Association" zurückgegriffen, der ein Dokument (bzw. dessen DocumentEntry) dem Ordnerobjekt im Aktensystem zuordnet. Einige Ordner sind fest hinterlegt im Aktensystem (diese werden nie direkt adressiert beim Einstellen), andere werden beim Bedarf vom Primärsystem selbst angelegt; im letzteren Fall liefert das Primärsystem ein Folder-Objekt im SubmissionSet mit, welches ebenfalls einige Metadaten wie einen Ordnertitel enthält. Die verschiedenen Objekte im Aktensystem (DocumentEntries, SubmissionSets, Folder) und ihre Beziehungen ("Associations") untereinander können später über die Suche (siehe Dokumente Suchen [ITI-18] bzw. teilweise auch [ITI-67]) gefunden und so nachträglich nachvollzogen werden.

Weitere Details zum Datenmodell finden sich generell im IHE XDS-Integrationsprofil und speziell in [IHE-ITI-TF3].

Neben dem Einstellen von Dokumenten und dazugehörigen SubmissionSets sowie allfälligen Ordnerzuweisungen erlaubt die ePA auch die Nutzung zweier besondere IHE XDS-Features: Das Ersetzen von Dokumenten und die Verwendung von Dokumentenanhängen. Beide Mechanismen und ihre Anwendung in ePA werden im Folgenden kurz erläutert.

Ersetzen von Dokumenten ("Replacement , "RPLC"): Grundsätzliche Funktionsweise

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 "SubmissionSet") 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 können jedoch über Restricted Update Document Set geändert werden.

Ersetzen von Dokumenten ("Replacement , "RPLC"): Aktuelle Ausgestaltung

Der Ersetzungsmechanismus darf nur in ausgewählten Anwendungsfällen verwendet werden. Ab ePA 3.1.3 ist in XDS nur das Ersetzen der folgenden Dokumentenarten in der ePA erlaubt:

1. NFD: Notfalldatensatz
2. DPE: Datensatz Persönliche Erklärung
3. DiGA: Daten der Digitalen Gesundheitsanwendungen
4. (Ordner "technical": Dokumente für den internen Gebrauch der Aktensysteme / FdVs, nicht relevant für Primärsysteme)

Für NFD und DPE liegt der Grund darin, dass fachlich nur ein einziges aktives Dokument dieser Art jeweils existieren darf. Da alte Versionen sonst nicht aufbewahrt werden könnten, ist ein Ersetzen alter Versionen möglich, die bei einer Ersetzung wie oben beschrieben in den inaktiven Status ("Deprecated") wechseln. Bei DiGA-Daten ist das Ersetzen von Dokumentenversionen seit längerem etabliert, so dass dies auch weiterhin ermöglicht werden soll.

Das Ersetzen vonAbrechnungsdaten ("receipt") durch Kostenträger (KTR) sowie das Ersetzen von von Notizen zum Kinderuntersuchungsheft (durch das FdV) fallen in ePA 27 weg. Diese Daten können weiterhin über den Ersetzungsmechanismus in MHD ersetzt werden. Zudem ist der Ersetzungsmechanismus in MHD auch offen für weitere Dokumententypen (früher auch in XDS, weshalb entsprechende Altdaten vorliegen können).

Falls versucht wird, in XDS ein Dokument eines Typs zu ersetzen, für den Ersetzungen nicht erlaubt sind, gibt das Aktensystem den Fehler `XDSReplacementForbidden` zurück.

Dokumentenanhänge: Grundsätzliche Funktionsweise

Sowohl das verwendete IHE XDS-Framework als auch der ePA MHD Service erlauben optional in ePA die Verwendung von Dokumentenanhängen in der Patientenakte. Um ein Dokument ("Kinddokument") an ein anderes Dokument ("Elterndokument") anzuhängen, wird eine Verbindung (in IHE XDS: "append Association", in MHD entsprechende getypte DocumentReference.relatesTo-Referenz) zwischen beiden eingestellt.

Das Hochladen eines Kinddokuments und die dazugehörige Verknüpfung mit dem Elterndokument kann nachträglich erfolgen;. Bei XDS wird zuerst das Elterndokument hochgeladen werden und später dann das Kinddokument und die passende Verknüpfung. Auch das Einstellen von Eltern- und Kinddokument gleichzeitig (inklusive der Verknüpfung) ist möglich. In MHD ist es im Gegensatz zu XDS sogar machbar, zuerst Kind- und dann Elterndokument hochzuladen und die Verknüpfung nachträglich vorzunehmen.

Ein Elterndokument kann mehrere Kinddokumente besitzen. Auch können "Anhangsketten" erstellt werden, in dem ein Kinddokument wiederum selbst über einen oder mehrere Anhänge verfügt. Es ist in IHE XDS derzeit nicht möglich (jedoch in MHD), dasselbe Dokument als Kinddokument an zwei verschiedene Elterndokumente anzuhängen.

Dokumentenanhänge: Aktuelle Ausgestaltung

Das Aktensystem setzt in XDS einige weitere Einschränkungen bei Dokumentenanhängen durch, z. B. ist ein Anhängen an Dokumente in "Sammlungen" ist nicht möglich (das betrifft viele MIO-Dokumente) und auch nicht an Dokumente, die Teil von RPLC-Ketten (s.o.) sein können. Details finden sich in

[gemSpec_Aktensystem_ePAfueralle#A_27763] (RPLC-fähige Dokumente) und A_27764 (Sammlungen).

In MHD sind das Anhängen flexibler ausgestaltet.

3.11.3.1 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.

3.11.3.2 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] befüllen.**[<=]**

Das Feld DocumentEntry.homeCommunityId wird ab ePA 3.x nicht mehr benötigt und ggf. vom Aktensystem gelöscht.

A_26443 -Pflicht zur Verwendung des Implementation Guides für strukturierte Dokumente
Bei der Metadatenbelegung von strukturierten Dokumenten MUSS das PS den Vorgaben aus [gemSpec_IG_ePA] folgen.
[<=]

A_26444 -Empfehlung zur Verwendung des Implementation Guides für medizinische Bilder
Bei der Metadatenbelegung von medizinischen Bildern SOLL das PS den Vorgaben aus [gemSpec_IG_ePA] folgen.**[<=]**

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 [gemIG_TI_Terminology],
- 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_14932-02 -Bildung und Verwendung einer uniqueId für Dokumente
Das PS MUSS eine `DocumentEntry.uniqueID` gemäß [ITI-TF-3#4.2.3.2.26] und [gemSpec_Aktensystem_ePAfueralle#A_14760-*] erstellen. Für den XDS Document Service im ePA-Aktensystem wird die `DocumentEntry.uniqueID` in die Metadaten der IHE-Nachrichten eingestellt:

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

[<=]

Für die meisten Dokumente ist es völlig ausreichend, eine OID (wie bspw. "2.25.164078681790433400182932576131269019576") oder eine UUID (mit Präfix anzugeben, bspw. "urn:uuid:9c330bd0-0fcc-4866-a668-7b6d8bc9032f") zu generieren und als Wert zu verwenden. Nur in besonderen Fällen (HL7 CDA) oder Einstellen eines eArztbriefs (siehe auchAbschnitt zum eArztbrief) ist es sinnvoll oder wie beim eArztbrief sogar gefordert, davon abzuweichen. Die in A_14932-* angegebenen Literaturreferenzen enthalten noch weitere Informationen zum Thema.

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`

Es können keine Dokumenten-Dubletten in die ePA eingestellt werden; das Aktensystem lehnt Dokumente ab, die über denselben Fingerabdruck (Hash) verfügen. Auch die DocumentEntry.entryUUID und die DocumentEntry.uniqueId eines Dokuments sind eindeutig werden vom Aktensystem abgelehnt, wenn versucht wird, ein zweites Dokument mit denselben Werten hochzuladen. Beide Kennungen (sofern sie auch beim Primärsystem mitgespeichert werden) eignen sich gut dazu, festzustellen, ob ein lokales Dokument bereits in der ePA vorhanden ist oder nicht.

Falls es eine neuere Version eines Dokumentes gibt, kann die alte Dokumentenversion gelöscht und neu eingestellt werden, oder die neu Version "daneben" gelegt werden. Die Entscheidung, wann ein Löschen sinnvoll ist, liegt im Ermessen des Primärsystems oder des Anwenders.

Einige Dokumententypen können auch einen Ersetzungsmechanismus ("Replace") mit einer neuen Version aktualisiert werden. Das geänderte Dokument wird dabei hochgeladen und über eine RPLC-Association mit dem alten Dokument verknüpft. Das veraltete Dokumente wird vom Aktensystem automatisch alsveraltet ("Depracted") markiert. Siehe auch Erläuterungen zu Ersetzungen weiter oben.

Versicherte können am FdV einzelne Dokumente und Dokumentenkategorien verbergen. Dieses kann dazu führen, dass Dokumente, die ein Leistungserbringer erstellt hat, für ihn selbst nicht mehr sichtbar sind. 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.

A_27745-01 -Von der RPLC-Option unterstützte Dokumententypen
Das Primärsystem DARF NICHT Dokumente per "RPLC"-Mechanismus ersetzen, außer es handelt sich um die folgenden Dokumententypen gemäß [gemSpec_IG_ePA]:

- Notfalldatensatz (formatCode:`urn:gematik:ig:Notfalldatensatz:r3.1`)
- Datensatz Persönliche Erklärung (`urn:gematik:ig:DatensatzPersoenlicheErklaerungen:r3.1`)
- KTR-Abrechnungsdaten (Dokumente der Kategorie "receipt" (d.h. Dokumente im Ordner mit Folder.codeList=`b878db05-49e4-4f74-a329-b3bcdd8082c4`)
- DiGA: Daten der Digitalen Gesundheitsanwendungen (formatCode:`urn:gematik:ig:diga:v1.1`)

[<=]

A_27745-02 -Von der RPLC-Option unterstützte Dokumententypen
Das Primärsystem DARF NICHT Dokumente per "RPLC"-Mechanismus ersetzen, außer es handelt sich um die folgenden Dokumententypen gemäß [gemSpec_IG_ePA]:

- Notfalldatensatz (formatCode:`urn:gematik:ig:Notfalldatensatz:r3.1`)
- Datensatz Persönliche Erklärung (`urn:gematik:ig:DatensatzPersoenlicheErklaerungen:r3.1`)
- DiGA: Daten der Digitalen Gesundheitsanwendungen (formatCode:`urn:gematik:ig:diga:v1.1`)

[<=]

In ePA-Versionen vor ePA 3.1.2 war das Ersetzen weiterer Dokumententypen erlaubt, weshalb entsprechende "Ersetzungsketten" auch für andere Dokumententypen in Altdaten existieren können.

A_27748-01 -Kein Anhängen an Dokumente in RPLC-Ketten
Das Primärsystem DARF NICHT für ein Dokument eine Anhangsbeziehung (Elterndokument, Kinddokument) zu einem Dokument eines Typs einstellen, der für die Verwendung von RPLC-Ketten vorgesehen ist (siehe [gemSpec_Aktensystem_ePAfueralle#A_27763*]).
[<=]

Aktuell sind die RPLC-fähigen Dokumente, an die gemäß [gemSpec_Aktensystem_ePAfueralle#A_27763*] in XDS nicht angehängt werden darf:

Dokument	codeSystem	code
eMP	1.3.6.1.4.1.19376.3.276.1.5.6	urn:gematik:ig:Medikationsplan:r3.1
NFD	1.3.6.1.4.1.19376.3.276.1.5.6	urn:gematik:ig:Notfalldatensatz:r3.1
DPE	1.3.6.1.4.1.19376.3.276.1.5.6	urn:gematik:ig:DatensatzPersoenlicheErklaerungen:r3.1
DiGA	1.3.6.1.4.1.19376.3.27	urn:gematik:ig:diga:v1.1

	6.1.5.6	
Notizen Kinderuntersuchungsheft	1.3.6.1.4.1.19376.3.276.1.5.6	urn:gematik:ig:KinderuntersuchungsheftNotizen:v1.0.0 oder urn:gematik:ig:KinderuntersuchungsheftNotizen:v1.0.1

Zudem darf nicht an Dokumente in diesen Ordnern angehängt werden:

Ordner-Kategorie	Folder.entryUUID
receipt	91420e5e-e055-4c7d-b14e-96239e8f0d6d
technical	f88dc706-d2df-4ca0-a850-491cfaab2d31 (nicht relevant für PS)

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_24967-02 -Konvertieren von PDF nach PDF/A

Das PS MUSS eigene 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 Konvertierung von Dokumenten aus Drittsystemen, z. B. aus einem separaten Radiologieinformationssystem (RIS), nimmt das an die ePA angebundene Primärsystem, z. B. das führende KIS (Krankenhausinformationssystem), grundsätzlich nicht vor. Wenngleich das Krankenhaus eine durchgängige Anwendung des PDF/A-Standards für in die ePA einzustellende Dokumente sicherstellen sollte, besteht keine explizite gesetzliche Pflicht zur Konvertierung. Liegen in die ePA einzustellende Dokumente zum Zeitpunkt der Datenübermittlung nur als einfache PDF-Dokumente vor, können diese ohne Konvertierung nicht in der ePA gespeichert werden. Dasselbe gilt im ambulanten Bereich: Für Dokumente aus Drittsystemen gibt es keine Konvertierungspflicht. Natürlich ist eine Bereitstellung in der ePA jedoch aus Anwendersicht wünschenswert und sollte umgesetzt werden.

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

Die Unterstützung für das Ersetzen von Dokumenten durch neue Fassungen (ohne das alte Dokument dabei zu löschen) im Aktensystem ermöglicht, dass Dokumente durch eine neue Version des gleichen Dokuments ersetzt werden können. Das alte Dokument wird dabei vom Aktensystem als veraltet markiert.

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.**[<=]**

A_28239 -Einstellen von Dokumentenanhängen
Das PS SOLL es ermöglichen, Anhänge zu einem Dokument zusammen mit dem Elterndokument direkt im selben Arbeitsgang einzustellen ohne Dokumente nachträglich erst hinzufügen zu müssen.
[<=]

3.11.4 Dokumente suchen

Das Aktensystem verfügt über zwei Suchschnittstellen, die unterschiedliche Fähigkeiten besitzen.

Mit der Metadatensuche über [ITI-18] (sogenannte "Stored Query") kann eine SOAP-basierte Suchnachricht an das Aktensystem gesendet werden, mit der die Metadaten der Dokumente, SubmissionSets, Folders (Ordnern) und Asssociations zwischen ihnen durchsucht werden können.

Die zweite Suchschnittstelle (über [ITI-67], auch MHD-Suche genannt), die mit der ePA 3.1.2 eingeführt wurde, erlaubt ebenfalls eine Metadaten-basierte Suche, ergänzt jedoch zusätzlich die Möglichkeit, auch Dokumenteninhalten zu durchsuchen. Die MHD-Suche erlaubt zwar nur das Filtern auf den Metadaten der DocumentEntries, bietet jedoch auch ausgefeilte Suchmethoden für die Dokumenteninhalte (wie UND/ODER-Verknüpfungen von Suchbegriffen oder der Angabe von "Phrasen"). Die MHD-basierte Suche ist REST-basiert und wird in der Regel daher als etwas "leichtgewichtiger" in der Umsetzung angesehen.

In ePA 27 kommt zusätzlich in MHD die Suche Find Document Lists [ITI-66] hinzu, die das Suchen und Listen (im Falle von XDS-Dokumenten: XDS Folders und SubmissionSets) unterstützt.

Im Folgenden finden sich Detail zur traditionellen XDS Stored Query [ITI-18].

3.11.4.1 Dokumente suchen [ITI-18]

Das Suchen nach Dokumenten über die Registry Stored Query-Schnitstelle [ITI-18] erfolgt auf den Metadaten des Dokumentes, nicht auf den Inhalten des Dokumentes selbst (für letzteres siehe 3.11.4.2- Dokumente suchen [ITI-67]). 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 (d.h. alle Dokumente)
- Zeitintervall
- Dokumentenkategorie
- 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 Suchen mittels einer Suchmaske.

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].

3.11.4.1.1 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)

3.11.4.1.2 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_17198-04 -Nutzung des um XDSDocumentEntryTitle erweiterten Registry Stored Query FindDocuments
Das PS DARF 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 Query`FindDocuments` gemäß [IHE-ITI-TF2#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_25187-03 -Nutzung des um XDSDocumentEntryComment erweiterten Registry Stored Query FindDocuments
Das PS DARF 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-TF2#3.38] in Verbindung mit den zusätzlich zu [ITI-38] eingeführten Suchparametern$XDSDocumentEntryComments oder $XDSDocumentEntryComment (deprecated) nutzen können. Der zusätzliche Parameter$XDSDocumentEntryComments oder $XDSDocumentEntryComment ist verpflichtend und filtert die Suchergebnismenge über das Attribut DocumentEntry.comments.**[<=]**

Tabelle 12: 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.**[<=]**

A_27578 -Kennzeichnung des Einstellers
Das PS SOLL Dokumente in Übersichten oder Listendarstellungen dahingehend kennzeichnen, dass es für den Benutzer erkennbar ist, ob der Versicherte selbst oder eine bestimmte Art von Organisation das Dokument eingestellt hat. Dazu SOLL das PS insbesondere aus dem zum Dokument gehörenden SubmissionSet das Feld SubmissionSet.authorRole (siehe gemSpec_Aktensystem_ePAfueralle#A_14760-*) auswerten.
[<=]

Damit soll insbesondere das folgende Problem adressiert werden: Der Autor eines Dokuments ist (z. B. am ePA-FdV) häufig frei wählbar. Das heißt, ein Versicherter kann bspw. ein altes Dokument (aus der "Vor-ePA-Zeit") am ePA-FdV einscannen und als DocumentEntry.author einen Arzt hinterlegen. Das ePA-FdV und auch das ePA-Aktensystem können nicht prüfen, ob es sich um eine valide Angabe handelt. Eine Dokumentenliste, die bspw. nach der Suche die einzelnen Treffer mit Dokumententitel

und weiteren Details wie eben auch DocumentEntry.author anzeigt, kann deshalb leicht den Eindruck erwecken, dass es sich um "geprüfte" Angaben im DocumentEntry.author-Feld handelt ("Prof. Dr. Dr. Augustus Futrelle"). Es sollte jedoch für den Benutzer zweifelsfrei erkennbar sein, ob das Dokument aus einer vertrauenswürdigen Quelle stammt. Das heißt, der Einsteller, nicht der Autor des Dokuments, spielt bei der Beurteilung des Dokuments ebenfalls eine wichtige Rolle. Die obige Anforderung ist in diesem Sinne zu interpretieren.

Die Anforderung befindet sich im Kapitel zur Dokumentensuche, die einen wesentlichen Anwendungsfall für sie darstellt, geht aber insgesamt darüber hinaus; bspw. wäre auch die Anzeige eines ePA-Dokuments betroffen, dass in einer "lokalen" Dokumentenübersicht angezeigt wird.

Die Art der Kennzeichnung selbst ist der Implementierung des PS überlassen (Symbol, "Mouse-Over", Farbkodierung, etc.).

Es ist selbstverständlich dem PS freigestellt, auch in anderen Ansichten (ohne DocumentEntry.author) den Einsteller bzw. die Einstellerkategorie sinnvoll hervorzuheben.

Neben der Kennzeichnung des Herstellers kann es auch sinnvoll sein, in einer Listen- oder Dokumentenansicht hervorzuheben, dass ein Dokument Teil einer Anhangskette ist. Dies ist direkt aus den Dokumentenmetadaten ablesbar und erfordert demnach keine zusätzliche Suchoperation.

A_28238 -Hervorheben von Anhängen und automatisches Herunterladen
Das PS SOLL Dokumente in Übersichten oder Listendarstellungen kennzeichnen, ob das Dokumente Anhänge besitzt oder selbst als Anhang eines anderen Dokuments dient. Wenn ein Dokument zum Herunterladen ausgewählt wird, SOLL das PS anbieten, auch gleich in Anhangsbeziehung stehende Eltern- oder Kinddokumente mit herunterzuladen. Das PS SOLL es auch per Konfiguration ermöglichen, Eltern- und Kinddokumente automatisch ohne besondere Nutzeraktion mit herunterzuladen.
[<=]

A_28240 -Anzeige der letzten Version eines Dokuments
Das PS SOLL bei Dokumenten, die Teil von RPLC-Ketten sind, immer die letzte Dokumentenversion anzeigen oder eindeutig kennzeichnen. Vorgängerversionen dieses Dokuments SOLL das PS bei Bedarf auflisten und ebenfalls zum Herunterladen anbieten können.
[<=]

3.11.4.2 Dokumente suchen [ITI-67]

Alternativ zu den Suchmöglichkeiten der IHE-Transaktion [ITI-18] muss ein Primärsystem eine FHIR-basierte Suche nach [ITI-67], wie in [gemIG_ePA_MHD] spezifiziert, durchführen können. Darüber hinaus bietet diese Transaktion die Möglichkeit, eine Volltextsuche durchzuführen. Die "MHD"-basierte Suche erlaubt es auch, metadatenbasierte Suche und Volltextsuche direkt miteinander zu kombinieren.

Bei der Nutzung der Schnittstelle zur Durchführung einer Volltextsuche sollte, sowohl was die Formulierung der Anfragen als auch die Anfragehäufigkeit betrifft, Sorgfalt angewendet werden. Dies reduziert die Last am MHD Service und kann verhindern, dass die Suchanfragen nicht im erwarteten Zeithorizont beantwortet werden können. Der MHD Service darf eingehende Anfragen auch "throttlen" und gibt dann einen entsprechenden Fehler-Code zurück (siehe Schnittstelle "Find Document References" in [gemIG_ePA_MHD].

3.11.5 Dokumente laden

3.11.5.1 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.

3.11.5.1.1 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
- 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

3.11.5.1.2 Nutzung

Die RetrieveDocumentSetRequest 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.

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 ePA 3.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.

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_21503-03 -Daten digitaler Gesundheitsanwendungen auslesen
Das Primärsystem MUSS DiGA-Daten, deren Formatvorgabe als Medizinisches Informationsobjekt gemäß [gemSpec_IG_ePA] definiert sind, bei vorliegender Befugnis aus dem ePA-Aktensystem des Versicherten auslesen können.**[<=]**

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

3.11.5.2 Dokumente laden [ITI-68]

Alternativ zum Laden eines Dokuments per IHE-Transaktion [ITI-43] muss ein Primärsystem nach einer FHIR-basierten Suche nach [ITI-67], wie in [gemIG_ePA_MHD] spezifiziert, aus der Suchergebnisseite, Dokumente direkt herunterladen können.

3.11.6 Dokumente löschen [ITI-62]

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

A_27746 -Löschen von Dokumenten mit Anhängen
Das Primärsystem MUSS es dem Nutzer ermöglichen, zu erkennen, dass ein zu löschendes Dokument Anhänge besitzt oder selbst als Anhang einem Dokument zugeordnet ist (Elterndokument, Kinddokument). Wenn dies der Fall ist, MUSS dem Nutzer die Möglichkeit gegeben werden, auch weitere Dokumente in dieser Anhangskette zum Löschen auszuwählen.**[<=]**

Das Primärsystem muss dabei beachten, dass es für einige wenige Dokumente zwar Leserechte, das Dokument also suchen und anzeigen kann, aber nicht über entsprechende Löschrechte verfügt. Die Rechte können in der Legal Policy in [gemSpec_Aktensystem_ePAfueralle#19303*] nachgeschlagen werden.

Falls Dokumente aus RPLC-Ketten (Ersetzungen) gelöscht werden, löscht das Aktensystem automatisch alle Dokumente in der Kette. Es kann sinnvoll sein, auf dem Primärsystem eine entsprechenden Warnung auszugeben.

3.11.6.1 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 jedes gelöschten Dokuments gelöscht werden, falls sie zuvor persistent gespeichert wurde.

3.11.6.2 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.

Beim Löschen von Dokumenten, die über Anhangsbeziehungen mit anderen Dokumenten verbunden sind, wird nur das oder die ausgewählten Dokumente gelöscht, nicht die gesamte Anhangskette.

Beim Löschen von Dokumenten, die über RPLC-Beziehungen (Dokumentenersetzungen) miteinander verbunden sind werden hingegen alle Dokumente in der Ersetzungskette gelöscht.

3.11.7 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 Befugnis des Nutzers erlaubt. Ein Herunterladen des Dokumentes, auf die sich die Metadaten beziehen, ist zum Editieren der Metadaten nicht erforderlich.

3.11.7.1 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.

3.11.7.2 Nutzung

A_24386-02 -Aktualisierbare Metadaten
Das PS MUSS sich beim Anwendungsfall Aktualisieren von Metadaten des DocumentEntry mittels RestrictedUpdateDocumentSet auf das Ändern der folgenden Dokumentmetadatenfelder beschränken:

- author
- classCode
- comments
- confidentialityCode
- creationTime
- 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.**[<=]**

3.11.8 Artefakte

3.11.8.1 Namensräume

Tabelle 13: 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

3.11.8.2 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.

3.11.9 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_24505-01 -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. Liegt dem PS hingegen keine Informationsgrundlage für die Auswahl eines Metadatums vor, ist eine Vorbelegung von Metadaten zu vermeiden. Wertebereiche (Value Sets) für ePA-Dokumente sind je nach Festlegung von [gemIG_TI_Terminology] zu benutzen.**[<=]**

Das heißt auch, dass Werte, die für das jeweilige Metadatenfeld nicht ausdrücklich in [gemIG_TI_Terminology] vorgesehen sind, nicht verwendet werden dürfen.

Für die Wertebereiche der Metadaten gelten die Vorgaben von A_14760-*.

A_23556-05 -Einheitliche Metadaten-Vorgaben für unstrukturierte Dokumente ohne ImplementationGuide
Das PS MUSS bei der Vergabe von Metadaten für die fachliche Klassifizierung eines Dokuments, darunter mindestens Dokumentenklasse (classCode) und Dokumententyp (typeCode), die folgende Strategie umsetzen, sofern kein IG [gemSpec_IG_ePA] dafür vorliegt:

- PS-seitige Prüfung, ob für das Dokument ein KDL-Code (eventCodeList) vergeben werden kann; wenn ja, ist dieser zu übernehmen und classCode und TypeCode gemäß des aktuellsten KDL-IHE-Mapping [KDL-ILF] vorzuschlagen. Falls [KDF-ILF] auf den classCode oder typeCode "UNK" (Unbekannt - kein offizieller IHE-D Code) abbildet, kann kein IHE Code auf Basis des Mappings vorgeschlagen werden.
- Falls kein KDL-Code inkl. Mapping vergeben werden kann: PS-seitige Prüfung, ob für das Dokument eine Dokumentenklasse (classCode) und ein Dokumententyp (typeCode) vergeben werden kann; wenn ja, sind diese zu übernehmen.
- Falls keine Vorbelegung stattfinden kann, muss das PS dem Benutzer die manuelle Auswahl von classCode und typeCode möglichst nutzerfreundlich ermöglichen.

[<=]

Falls möglich, kann die Zuweisung der Metadaten auch völlig ohne Nutzerinteraktion stattfinden (siehe auch A_24505*).

Die Auswahl der Dokumentenart erfolgt zweistufig: Zunächst wird die Dokumentenklasse als classCode (grobe Einordnung), anschließend der Dokumententyp als typeCode (spezifischere Einordnung) bestimmt. Die manuelle Auswahl des richtigen classCode und typeCode kann durch eine Umsetzung in dieser Zweistufigkeit und eine priorisierte Anzeige besonders häufig vorkommender Auswahlmöglichkeiten unterstützt werden:

1. Auswahl eines classCHode aus einer reduzierten Auswahlliste, basierend auf besonders häufigen/verpflichtend in die ePA zu übertragenden Dokumentenklassen
2. Auswahl eines typeCodes aus einer reduzierten Auswahlliste, basierend auf dem ausgewählten classCode

Eine mögliche Priorisierung ist in der untenstehenden Tabelle dargestellt. Die Auswahl der genannten Dokumentenklassen orientiert sich an den Behandlungsdaten, welche gemäß § 347 und § 348 SGB V in die ePA übertragen werden müssen, sowie an Umsetzungshinweisen der DKG und einer Umfrage unter ärztlichen Fachgesellschaften durch die KBV. Die ausgewählten Dokumententypen treten gemäßKDL-IHE-Mapping [KDL-ILF] in Kombination mit der entsprechenden Dokumentenklasse auf. Die beispielhaften Arten von Dokumenten entsprechen Dokumenten der Klinischen Dokumentenklassenliste (KDL), die gemäßKDL-IHE-Mapping [KDL-ILF] die entsprechende Kombination an classCode und typeCode aufweisen (exkl. "Bilddaten Sonographie"). Die Auswahl der Liste erhebt keinen Anspruch auf Vollständigkeit. Eine mögliche Umsetzung im Primärsystem ist darunterstehend abgebildet.

Tabelle 14: Tab_ILF_ePA_Metadaten-Zuweisung

Dokumentenklasse	classCode	Dokumententyp	typeCode	Beispielhafte Arten von Dokumenten
Befundbericht	BEF	Ergebnisse Diagnostik	BEFU	Ärztlicher Befundbericht
		Ergebnisse bildgebender Diagnostik	BILD	Röntgenbefund
		Ergebnisse Funktionsdiagnostik	FUNK	EKG-Auswertung
		Pathologiebefundberichte	PATH	Histologiebefund
		Wunddokumentation	WUND	Wunddokumentationsbogen
Bilddaten	BIL	Ergebnisse bildgebender Diagnostik	BILD	Bilddaten Sonographie
		Fotodokumentation	FOTO	Fotodokumentation Diagnostik
		OP-Dokumente	OPDK	Fotodokumentation Operation
		Wunddokumentation	WUND	Fotodokumentation Wunden
Brief	BRI	Arztberichte	BERI	Krankenhaus-Entlassbrief
		Medikamentöse Therapien*	MEDI*	Apotheke Entlassbericht
		Pflegedokumentation*	PFLG*	Überleitungsbogen
		Schwangerschafts- und Geburtendokumentation*	GEBU*	Datenblatt für den Pädiater*
		Therapiedokumentation	FPRO	eDMP
Durchführungsprotokoll*	DUR	OP-Dokumente*	OPDK*	OP-Bericht

		Ergebnisse bildgebender Diagnostik*	BILD*	Herzkatheterprotokoll
Medizinischer Ausweis	AUS	Patienteneigene Dokumente	PATD	Allergiepass
		Schwangerschafts- und Geburtendokumentation	GEBU	Mutterpass
Planungsdokument	PLA	Medikamentöse Therapien	MEDI	Medikationsplan

* Nur in bestimmten Sektoren relevant, bspw.: Apotheke, pflegerische Einrichtungen oder Krankenhäuser.

Für Laborergebnisse wurde bis Einführung der ePA27 folgende Belegung empfohlen:

Dokumentenklasse	**classCode**	**Dokumententyp**	**typeCode**	**Beispielhafte Arten von Dokumenten**
Laborergebnisse	LAB	Ergebnisse Diagnostik	BEFU	Laborbefund
		Ergebnisse Immunologie	IMMU	Befund über positive Infektionsmarker
		Ergebnisse Mikrobiologie	MKRO	Blutkulturenbefund
		Ergebnisse Virologie	VIRO	Virologiebefund
		Transfusionsdokumente	TRFU	Herstellungs- und Prüfprotokoll von Blut und Blutprodukten

Ab ePA 27 werden Laborbefunde- und ergebnisse ausschließlich strukturiert über den ePA MHD Service [gemIG_ePA_MHD] eingestellt. Die fachlichen Vorgaben zum dazugehörigen FHIR-Format finden sich in [gemIG_ePA_Laboratory].

Eine Vorauswahl mit reduzierter Auswahlliste könnte wie folgt aussehen:

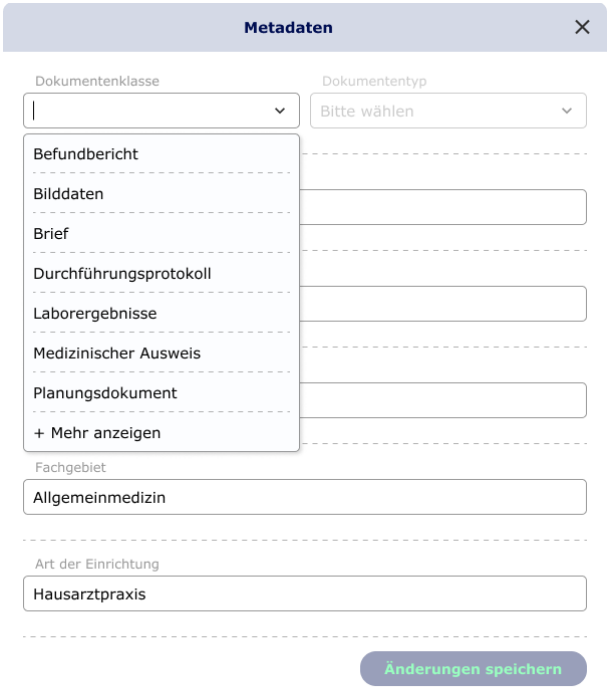


Abbildung 15: Beispiel für die Auswahl einer Dokumentenklasse aus einer reduzierten Auswahlliste

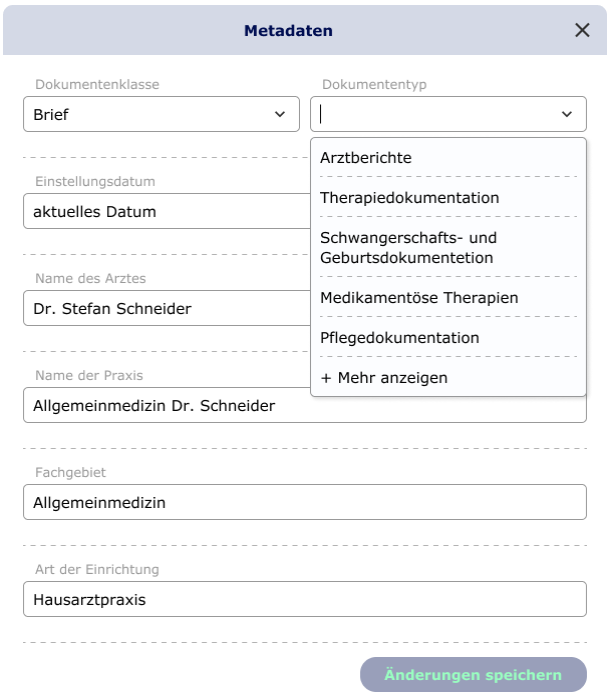


Abbildung 16: Beispiel für die Auswahl eines Dokumententyps aus einer reduzierten Auswahlliste (auf Basis der ausgewählten Dokumentenklasse)

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_27635-02 -Metadatenbelegung für Vorlagen
Das PS SOLL für häufig erstellte Dokumente - insbesondere von Dokumententypen der Tabelle Tab_ILF_ePA_Metadaten-Vorbelegung - spezifische Vorlagen bereitstellen, die mit den passenden Metadaten (insbesondere practiceSettingCode, classCode, typeCode und sowie sofern verfügbar/relevant KDL-Code in der eventCodeList) vorzubelegen sind. **[<=]**

Tabelle 15: Tab_ILF_ePA_Metadaten-Vorbelegung

Dokumententyp	classCode	typeCode	eventCodeList	Anzeigename
Arztbrief (nicht eArztbriefe gemäß [Richtlinie eArztbrief])	BRI	BERI	-	Arztbericht /Arztbrief
Krankenhausentlassungsbericht	BRI	BERI	AD010104	Krankenhausentlassungsbericht
Befund/Vorbefund/ Altbefund	BEF	BEFU	-	Ergebnisse Diagnostik
Röntgenbefund	BEF	BILD	DG020110	Ergebnisse bildgebender Diagnostik (Radiologie)
Sonographiebefund	BEF	BILD	DG020111	Ergebnisse bildgebender Diagnostik (Sonographie)
EKG-Auswertung	BEF	FUNK	DG060111	Ergebnisse Funktionsdiagnostik

				(EKG)
Histologiebefund	BEF	PATH	PT080102	Pathologiebefundberichte
Lungenfunktionstest	BEF	FUNK	DG060108	Ergebnisse Funktionsdiagnostik (Lunge)
Bilddaten	BIL	BILD	-	Ergebnisse bildgebender Diagnostik
Foto	BIL	FOTO	-	Fotodokumentation
OP-Bericht	DUR	OPDK	OP150103	OP-Dokumente (OP-Bericht)
OP-Plan/OP-Vorbereitung	DUR	OPDK	-	OP-Dokumente (OP-Vorbereitung)
Dialyseprotokoll	DUR	FPRO	VL040202	Therapiedokumentation (Dialyse)
Überweisung	VER	AUFN	AU050102	Überweisung (Überweisunsgschein)
Krankenhauseinweisung	VER	AUFN	AU050101	Verordnung von Krankenhausbehandlung
Anamnese	DUR	AUFN	-	Anamnese
Anamnesebogen	DUR	AUFN	AU010101	Anamnesebogen
Therapievorschlag/ Therapiebedarf	ANF	FPRO	-	Therapiedokumentation
Histologieanforderung	ANF	PATH	PT080101	Histologieanforderung
Kontaktdaten Angehörige	ADM	PATD	-	Kontaktdaten Angehörige
Neugeborenensceening	BEF	GEBU	SD070104	Neugeborenenscreening

Die Idee ist, dass ein über eine spezifische Vorlage erstelltes Dokument automatisch die passenden bekannten Metadaten erhält, um den Aufwand für die manuelle Eingabe möglichst gering zu halten. Wenn für die Vorlage bereits ein KDL-Code vergeben werden kann, können auch via KDL-Mapping (vgl.A_23556-*) typeCode und classCode automatisch vergeben werden. Wenn die Vorlage jedoch allgemeinerer Natur ist, kann classCode "Befundbericht" bspw. schon vorab gesetzt werden, um zumindest später weniger Metadaten manuell vergeben zu müssen.

A_28207 -Verwaltung individualisierter Vorlagen zur Belegung von Metadaten
Ein PS SOLL dem Nutzer anbieten, individualisierte Dokumentenvorlagen zu erstellen, deren Metadaten er mit Hilfe des Primärsystems passend zum Nutzungszweck der jeweiligen Vorlage vorbelegen kann. Die entsprechenden Vorlagen SOLLEN dem Nutzer dann beim Erstellen von Dokumenten oder beim Zuweisen der Metadaten zur Auswahl angeboten werden.
[<=]

Es kann sich bspw. auch um reine Metadatenvorlagen handeln, also einen Satz an Metadaten, der später gemeinsam mit einem Klick (oder eine ähnliche Aktion) für die Metadatenbelegung eines Dokuments ausgewählt werden kann.

A_27650-01 -Weitere technische Unterstützungsmöglichkeiten zur Belegung von Metadaten
Ein PS KANN folgende Möglichkeiten nutzen, um die Vergabe von Metadaten für Dokumente zu vereinfachen:

1. Priorisierung einzelner Codes in der Auswahl angebotenen Metadaten anhand der durch den Leistungserbringer häufig verwendeten Metadaten (werden z.B. sehr häufig EKG-Befunde geschrieben, kann der typeCode "FUNK - Ergebnisse Funktionsdiagnostik" bevorzugt vorgeschlagen werden). Das PS KANN also "mitlernen", welche Codes häufig vergeben werden.
2. Vorschläge von Metadaten anhand bekannten Kontextes oder bestehender bekannter Metadaten wie practiceSettingCode (ist bspw. der angemeldete Nutzer Teil der Intensivmedizin, kann für practiceSettingCode automatisch "INTM" und für classCode der Code für "DUR" für "Durchführungsprotokoll" in der näheren Auswahl stehen).
3. Vorschläge von Metadaten anhand von Dokumenteninhalten (z. B. Titel = "Ergometrieergebnisse" erlaubt Vorauswahl von KDL-Code für "Ergometriebefund" für eventCodeList sowie entsprechenden Vorschlägen für classCode und typeCode gemäß KDL-IHE-Mapping).
4. Aufnahme der Beschreibungstexte für zu vergebende Codes in das Primärsystem, um in der Code-Auswahl unsicherere Benutzer auf Wunsch zu unterstützen, sich für den korrekten Code zu entscheiden. Die KDL (aber auch andere Code Systeme) enthalten häufig für jeden Code eine Definition, welche Dokumente genau unter diesen Code fallen.

[<=]

A_27643 -Eindeutigkeit von KDL- und DMP-Code in der eventCodeList
Ein PS MUSS bei der Belegung von DocumentEntry.eventCodeList sicherstellen, dass jeweils höchstens ein KDL-Code ("Klinische Dokumentenklassen-Liste") und höchstens ein DMP-Code ("Disease Management Programm") verwendet werden. Das Hinzufügen von Codes aus anderen Value Sets ist davon nicht berührt und ist ohne Einschränkungen (abgesehen von generellen ValueSet-Vorgaben für das Feld eventCodeLIst) möglich.
[<=]

Frühere Versionen der ePA für Alle haben das Einstellen von mehreren KDL- bzw. DMP-Codes in die eventCodeList nicht unterbunden. Deshalb kann es Altdaten geben, die noch mehr als einen Code der entsprechenden Code Systeme in der eventCodeList enthalten.

ConfidentialityCode

DocumentEntry.confidentialityCode wurde im Rahmen von ePA 2.x genutzt, um Dokumenten im Rahmen des Befugnissystems bestimmte Vertraulichkeitsstufen zuzuordnen. Die entsprechenden Codes wurden beim Einstellen persistiert, vom Aktensystem zur Durchsetzung der vom Patienten vergebenen Befugnissen genutzt, und konnten auch so auch von Primärsystemen (sofern auf das jeweilige Dokument berechtigt) wieder mit den DocumentEntries heruntergeladen werden.

In der ePA für alle spielt das Metadatum confidentialityCode für das Primärsystem keine Rolle mehr. Der Code "CON" darf beim Einstellen von Dokumenten nicht verwendet werden. Andere Werte des Value Sets EPAXDSConfidentialityCodeVS für Confidentiality Code aus [gemIG_TI_Terminology] können vom Primärsystem beim Einstellen verwendet werden, jedoch ist ePA-seitig damit keine Semantik verbunden: Das Aktensystem ignoriert sie und Primärsysteme anderer Hersteller vermutlich ebenfalls.

[gemIG_TI_Terminology] enthält auch einige Codes, die als "deprecated" (veraltet) deklariert sind. Es ist angeraten, insbesondere diese Codes nicht mehr zu verwenden.

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.

A_28160 -Keine Verwendung von Codes im Status "inactive"
Das PS DARF beim Einstellen oder Aktualisieren von Metadaten für DocumentEntries, Folder und SubmissionSets NICHT Codes im Status "inactive" verwenden.

Falls ein inaktiver Code geschickt wird, gibt das Aktensystem den Fehler`XDSInactiveCode` zurück und listet den problematischen Code im `codeContext`-Attribut des zurückgegebenen`rs:RegistryError`-Elements.

Eine Ausnahme ist das Aktualisieren eines bestehende Codes mittels RMU-Operation oder das Ersetzen eines Dokuments über "RPLC"; wird der Code in in diesen Fällen mitgeschickt, weil er bereits auch an dieser Stelle im zu aktualisierenden/zu ersetzenden Objekt vorhanden ist, führt dies nicht zu einem Fehler.
[<=]

Codes im Status "Deprecated" sind nicht betroffen, d.h. sie dürfen regulär verwendet werden. Jedoch können diese Codes in späteren ePA-Versionen abgekündigt werden (Status "inactive") und ein Primärsystem sollte beginnen, alternative Codes zu verwenden, sofern möglich.

3.12.2 Vorgaben für bestimmte Dokumententypen

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. Zudem gelten für einige Dokumententypen wie Arztbriefe besondere Vorgaben.

Es kann auch geschehen, dass einzelne strukturierte Dokumentenformate mit der Zeit abgekündigt werden. Wenn sie dann nur noch zum Lesen zur Verfügung stehen, aber nicht mehr neu eingestellt werden können, wird dies auch für den jeweiligen Dokumententyp in [gemSpec_IG_ePA] festgelegt. Die entsprechende JSON-Beschreibung enthält dann den Hinweis "clientReadOnlyFromDate": "<Datum>", das heißt, dass gemäß gemSpec_Aktensystem_ePAfueralle#A_17546-*] das dort hinterlegte Dokumentenformat ab dem gegebenen Datum nicht mehr eingestellt sondern nur noch gelesen werden darf. Für die eAU gibt es bspw. stattdessen eine neuere IG-Festlegung (weitere JSON-Datei mit einer neuen Versionsnummer), die dann auch eingestellt werden kann.

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 und DPE (eGK)

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.

Hinweis: In Kapitel1.8- Formate beim Einstellen von Dokumenten gibt es darüber hinaus Zeichensatzvorgaben für NFD- und DPE-Dokumente.

NFD und DPE können jeweils nur ein einziges mal als aktives Dokument in einem Aktenkonto vorliegen. Wenn eine neue Version hochgeladen werden soll, kann dies entweder ersetzt (RPLC), sofern die alten Version erhalten bleiben soll, oder kann gelöscht werden. Weitere Details zum Ersetzungsmechanismus finden sich im Abschnitt zum Einstellen von Dokumenten .

3.12.2.3 Elektronischer Arztbrief (eArztbrief) der KBV

Als KBV-eArztbrief wird der eArztbrief gemäß KBV-Richtlinie [Richtlinie eArztbrief] bezeichnet. Ein KBV-eArztbrief besteht dabei aus einem PDF/A-Dokument und einem dazugehörigen CDA-Dokument.

Ein ePA-Primärsystem ist aktuell nur dazu verpflichtet, den PDF/A-Anteil einzustellen, entsprechendeMetadatenvorgaben folgen weiter unten.

Das heißt auch, dass beim Einstellen eines KBV-eArztbriefs der CDA-Anteil verworfen werden kann. Dies ist in der Regel unproblematisch, da er in der Praxis fast immer bis auf einige minimale verpflichtende Header-Daten leer ist. Falls tatsächlich ein strukturierter CDA-Body mit wesentlichen strukturierten Daten vorhanden ist, kann der CDA-Teil als "unspezifisches" HL7-CDA-Dokument eingestellt werden.

A_28669-02 -Einstellen des KBV-eArztbriefs (PDF/A) über XDS oder MHD
Das PS MUSS das im KBV-eArztbrief enthaltene PDF/A-Dokument in die ePA einstellen und sofern dazu die Schnittstellen des XDS Document Service genutzt werden, dabei die

Metadatenbelegung gemäß A_27747-* beachten (u.a. Eintrag des Codes`ED110104` in die eventCodeList).
[<=]

Für das Einstellen über den ePA MHD Service sind die Anforderungen in [gemIG_ePA_MHD] zu beachten.

Der PDF/A-Anteil des KBV-eArztbriefes wird unverändert inklusive der eingebetteten PDF-Signatur in die ePA eingestellt. Die Signatur wird nicht vom Aktensystem geprüft. Falls eine PDF/A-Konvertierung (Konvertierung in gültiges PDF/A-1/2 gemäß ePA-Anforderungen) notwendig ist, muss das konvertierte PDF/A ggf. ohne Signatur eingestellt werden.

A_28672-03 -Einstellen des KBV-eArztbriefs (PDF/A) - Setzen der DocumentEntry.uniqueId (XDS)
Das PS MUSS beim Einstellen des PDF/A-Anteils des KBV-eArztbriefs gemäß A_28669* die DocumentEntry.uniqueId mit einem Wert nach der folgenden Bildungsregel, basierend auf Dokumenten-Id (`root` und `extension`) aus dem KBV-eArztbrief belegen:"`<root>^<extension>^pdf`", wobei das "pdf" am Ende immer in Kleinbuchstaben anzugeben ist.**[<=]**

Details zur Dokumenten-Id finden sich in den CDA-Vorgaben der VHitG-Leitfaden-Spezifikation (referenziert in [Richtlinie eArztbrief]). Lautet die Dokumenten-Id bspw.

```
<id extension="123456789" root="2.16.840.1.113883.2.6.15.3.2.1"/>
```

wird DocumentEntry.uniqueId auf den Wert "`2.16.840.1.113883.2.6.15.3.2.1^123456789^pdf`" gesetzt. Bis auf das angehängte "^pdf" entspricht die Dokumentenkennung den IHE-Empfehlungen(vgl. [IHE-ITI-TF3#4.2.3.2.26]) für CDA-Dokumente, weshalb hier künstlich das "^pdf" angehängt wird. Wenn das CDA mit eingestellt wird, sollte unbedingt auch der Wert root^extension (im Beispiel: "`2.16.840.1.113883.2.6.15.3.2.1^123456789`" verwendet werden)gemäß IHE-Empfehlung verwendet werden.

Dieses Verfahren zur Belegung der DocumentEntry.uniqueId stellt sicher, dass derselbe KBV-eArztbrief nicht wiederholt in die ePA hochgeladen wird, selbst wenn das daraus extrahierte PDF/A umkonvertiert wurde, um es in die ePA einzustellen. Zudem lässt sich auch der Zusammenhang zu einem lokal vorliegenden KBV-eArztbrief herstellen, in dem die Kennungen (lokales CDA vs. uniqueId des ePA-PDF/A) verglichen werden.

A_27685-05 -KBV-eArztbrief mit Anhängen gemeinsam einstellen (XDS)
Das PS MUSS den PDF/A-Anteil eines KBV-eArztbriefs gemäß A_28669 gemeinsam mit seinen Anhängen einstellen, sofern dazu die Schnittstellen des XDS Document Service genutzt werden. Dabei muss das PS, sofern technisch möglich, alle Anhänge über APND-Associations mit dem PDF/A-Hauptdokument verbinden. Das PS MUSS zudem sicherstellen, dass außer dem PDF/A und den Anhängen keine weiteren Dokumente in der Anfrage enthalten sind.
[<=]

Insbesondere die Kennzeichnung der Anhänge bei einem gemeinsamen Einstellen stellt sicher, dass die richtige Struktur (Arztbrief+Anhänge) sofort im Aktenkonto verfügbar ist und kein "Zwischenzustand" veröffentlicht wird, in dem nur ein Teil der Dokumente verfügbar ist oder die Dokumente nicht über Anhangsbeziehungen miteinander verbunden sind. Zudem wird so das gesamte Dokumentenbündel durch das SubmissionSet "geklammert".

Um sicherzustellen, dass die Dublettenprüfung des Aktensystems die Anfrage nicht ablehnt, da bereits eingestellte Dokumente darin enthalten sind, kann für XDS die Option zur Duplikatübernahme verwendet werden (siehe [gemSpec_Aktensystem_ePAfueralle]), die dafür sorgt, dass Duplikate "stillschweigend" akzeptiert werden.

Wenn ein Anhang versehentlich nicht mit eingestellt wurde, muss der eAB gelöscht und neu eingestellt werden. Auf Wunsch können die Anhänge entweder mitgelöscht und neu mit eingestellt werden, oder der eAB alleine wird gelöscht und unter Wiederverwendung der alten Anhänge zusammen mit dem neuen Anhang hochgeladen.

Beim Einstellen mit Anhängen ist es möglich, dass ein bestehendes Dokument in der Akte beim Einstellen des PDF/A-Anteils an letzteren angehängt werden soll, das anzuhängende Dokument jedoch schon an ein anderes Elterndokument in der ePA angehängt ist. In dem Fall ist es nicht möglich, den Anhang an das einzustellende PDF/A aus dem KBV-eArztbrief anzuhängen, da ePA (IHE XDS) nur ein Elterndokument pro Anhangsdokument ermöglicht.

A_27138-03 -Behandlung von nicht unterstützten Anhängen eines KBV-eArztbriefs
Falls beim Einstellen von KBV-eArztbriefen Anhänge desselben in die ePA eingestellt werden sollen(z. B. wegen Übernahme aus Nicht-ePA-Anwendungen wie KIM), deren Format beim Einstellen in die ePA gemäß A_24864-* nicht unterstützt werden, SOLL das PS den eArztbrief dennoch mit allen Anhängen einstellen, die von der ePA unterstützt werden, alle nicht unterstützten Anhänge auslassen und den Benutzer über nicht eingestellte Anhänge informieren.
[<=]

A_27138-05 -Behandlung von nicht unterstützten Anhängen eines KBV-eArztbriefs in XDS und MHD
Falls beim Einstellen von KBV-eArztbriefen Anhänge desselben in die ePA eingestellt werden sollen(z. B. wegen Übernahme aus Nicht-ePA-Anwendungen wie KIM), deren Format beim Einstellen in die ePA gemäß A_24864-* nicht unterstützt werden, SOLL das PS den eArztbrief dennoch mit allen Anhängen einstellen, die von der ePA unterstützt werden, alle nicht unterstützten Anhänge auslassen und den Benutzer über nicht eingestellte Anhänge informieren.
[<=]

Wenn möglich, kann das PS natürlich die Anhänge in PDF/A konvertieren (und auf diese Weise das Formatproblem umgehen).

Bei der Verarbeitung im empfangenden PS können Anhänge fehlen, wenn diese nicht eingestellt werden konnten. Diese können nur außerhalb der ePA übertragen werden.

Vor ePA in der Version 3.1.3-1 wurden KBV-eArztbrief im sogenannten DischargeLetterContainer-Format in die ePA eingestellt, das PDF/A- und CDA-Anteil des KBV-eArztbriefs erhält. Der folgende Abschnitt stellt den Aufbau des Container-Formats vor, um Altdaten verarbeiten zu können. Diese müssen auch weiterhin angezeigt werden können (sie nachfolgende Anforderungen).

eArztbrief DischargeLetterContainer-Format

Das unten aufgeführte DischargeLetterContainer-Format wird in der Spezifikation weiterhin aufgeführt, um vorhandene Altdaten verstehen und interpretieren zu können.

Das DischargeLetterContainer-Format hat gemäß [Richtlinie eArztbrief] die verpflichtenden Teile PDF/A-Dokument und CDA-XML (nur der CDA-Header ist verpflichtend). Um diesen KBV-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.

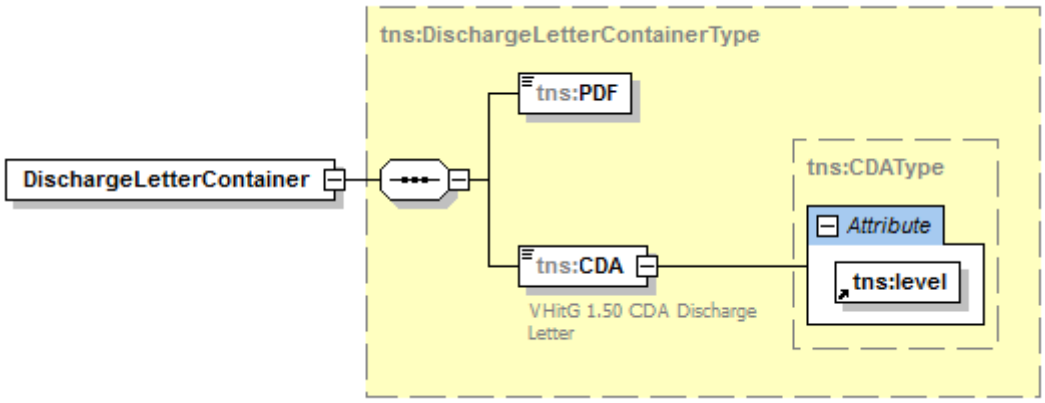


Abbildung 17: Abb_ILF_ePA_eAB-XML-Containerformat

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

Tabelle 16: XML-Struktur für Arztbrief im DischargeLetterContainer-Format

Element-, Attribut- oder Textknoten	Opt.	Nutzungsvorgabe
DischargeLetterContainer	R	
PDF	R	Base64-kodierter Arztbrief in PDF/A-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]

3.12.2.4 Arztbriefe und Krankenhausentlassbriefe

A_27747-02 -Metadatenbelegung für Arztbriefe und Krankenhausentlassbriefe über XDS

Das PS MUSS Arztbriefe und Krankenhausentlassbriefe gemäß den folgenden Metadatenvorgaben in `DocumentEntry.classCode`, `DocumentEntry.typeCode` und

DocumentEntry.eventCodeList kennzeichnen, sofern dazu die Schnittstellen des XDS Document Service genutzt werden,:

Tabelle 17 : Metadatenvorgaben für Arztbriefe und Krankenhausentlassbriefe

IHE-Metadaten	eventCodeList-Eintrag (KDL-Code)			
	Code	System inkl. Version	Display	Hinweis
classCode="BRI", typeCode="BERI"	ED110112	http://dvmd.de/fhir/CodeSystem/kdl| [2025]	KH-Entlassbrief	Aktuell: PDF/A
	ED110104	http://dvmd.de/fhir/CodeSystem/kdl| [2025]	eArztbrief	basierend auf entspr. KBV-Spezifikation
	"AD0101*" gemäß passendem KDL-Eintrag	http://dvmd.de/fhir/CodeSystem/kdl| [2025]	gemäß passendem KDL-Eintrag	Andere Arztberichte eingestellt als PDF/A

Wenn das Dokument vorläufig und nicht final ist, MUSS das PS zusätzlich den folgenden Code in die eventCodeList aufnehmen:

Tabelle 18 : Zusätzlicher Code für nicht finale Dokumente

Code	System	Display
H4	1.3.6.1.4.1.19376.3.276.1.5.15	vorläufiges Dokument

[<=]

AD0101 bezeichnet Codes die mit den Zeichen "AD0101" beginnen, z. B. "AD010112" für den "Kurzarztbrief". Der Code "AD0101" als Level 2-Code in KDL ist selbst nicht Teil des Value Sets für eventCodeList, das nur die konkreteren Level 3 Codes enthält.

Weitere Codes wie formatCode und mimeType müssen gemäß ePA-Spezifikation gewählt werden.

A_16246-03 -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/A-Anteil) aus der XML-Container-StrukturDischargeLetterContainer nach [PHR_Common.xsd] aus dem XDS Document Service herauslesen und als eArztbrief im DischargeLetterContainer-Format gemäß [Richtlinie eArztbrief] weiterverarbeiten und den PDF/A-Anteil zur Anzeige bringen können.**[<=]**

Hinweis: Ab ePA für Alle in der Version 3.0.5 wird für den elektronischen Arztbrief gefordert, den KDL-Code ED110104 in DocumentEntry.eventCodeList aufzunehmen. Siehe auch entsprechende Metadatenvorgaben in [gemSpec_IG_ePA].

A_28649 -Besondere Vorsicht beim Auslesen des eArztbriefs im DischargeLetterContainer-Format
Beim Auslesen des PDF/A- oder CDA-Anteils eines eArztbriefes mit formatCode="Code=urn:gematik:ig:Arztbrief:r3.1" (DischargeLetterContainer-Format) wie in A_16246-* beschrieben MUSS das PS besondere Vorsicht walten lassen, da das Aktensystem nicht gewährleistet, dass die jeweiligen Dokumente dem darunterliegenden Dateiformat (PDF/A, HL7 CDA) entsprechen.
[<=]

Hinweis 1: Insbesondere kann es sich bei den extrahierten vermeintlichen PDF/A- und CDA-Anteilen bspw. um Skripte oder auch binäre ausführbare Dateien handeln.

Hinweis 2: Seit ePA für Alle in der Version 3.1.3-1 können keine neuen eArztbriefe im DischargeLetterContainer-Format mehr eingestellt werden.

3.12.2.5 Laborergebnisse (inkl. Laborbefunde)

Ab ePA 27 werden Laborbefunde- und ergebnisse ausschließlich strukturiert über den ePA MHD Service [gemIG_ePA_MHD] eingestellt. Die fachlichen Vorgaben zum dazugehörigen FHIR-Format finden sich in [gemIG_ePA_Laboratory].

Für Altdaten gab es folgende Vorgaben für Primärsysteme:

- `DocumentEntry.eventCodeList`: passender KDL-Code (meist "LB*").
- `DocumentEntry.classCode`: Belegung "LAB"
- Kennzeichnung vorläufiger Ergebnisse/Befunde: Zusätzlicher KDL-Code "H4"

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 19: Tab_ILF_ePA_Datenfelder_Selbstauskunft

Vorkonfigurierbare Werte für DocumentEntry und SubmissionSet	Default-Konfiguration unter Beachtung von [gemSpec_Aktensystem_ePAfueralle] und [gemIG_TI_Terminology]
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

[<=]

Für einige Felder kann unter Umständen kein einzelner Wert hinterlegt werden oder nur eine sehr breite Vorauswahl getroffen werden, da sich in großen Organisationen (z. B. Krankenhäusern) der Wert je nach aktuellem Benutzer oder Dokument unterscheiden kann. So kann bspw. notwendig sein, die Fachrichtung im practiceSettingCode je nach Benutzer oder Dokument abweichend belegt werden müssen. Deshalb spricht die Anforderung auch nur davon, dass die Möglichkeit gegeben werden muss, eine Default-Konfiguration zu hinterlegen.

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.
Wird das Alltribut authorInstitution im SubmissionSet nicht gesetzt, so wird das Attribut zentral auf Basis der Authentisierungsinformationen gesetzt.

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.

3.12.4.1 Signaturen bei Medizinischen Informationsobjekten (MIOs)

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.**[<=]**

3.12.4.2 Signaturen bei PDF/A

A_28671 -PDF/A - QES-Signatur prüfen

Das PS KANN eine eingebettete QES-Signatur (PAdES) eines PDF/A-Dokuments durch die 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. Einige Dokumente müssen aber auch über den ePA MHD Service eingestellt werden.

Das Clientsystem des Kostenträgers kann die E-Mail-Adresse eines Versicherten verwalten.

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_19394-08 -Kennzeichnung eines Dokumentes als Kostenträgerinformation
Das Clientsystem des Kostenträgers MUSS beim Einstellen eines Dokuments über die Schnittstelle [I_Document_Management] 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 20: Tab_ILF_ePA_KTR_Metadatenkennzeichnungen

Dokumententyp	Metadaten
Dokumente der bei den Kostenträgern gespeicherten Daten über die in Anspruch genommenen Leistungen der	DocumentEntry.healthcareFacilityTypeCode=VER DocumentEntry.typeCode=ABRE DocumentEntry.authorRole=105 DocumentEntry.comment=Dokumente der bei den Kostenträgern gespeicherten Daten über die in Anspruch genommenen Leistungen der Versicherten gemäß § 305 SGB V

Versicherten	Submissionset.authorRole = 105
Eingescannte Dokumente	DocumentEntry.formatCode=urn:ihe:iti:xds-sd:pdf:2008 DocumentEntry.comment=Eingescannte medizinische Informationen gemäß § 350a SGB V Submissionset.authorRole = 105 SubmissionSet.contentType = 8
Medizinische Hinweise der Kostenträger	DocumentEntry.classcode=ASM DocumentEntry.typeCode=GRIS DocumentEntry.authorRole=105 DocumentEntry.mimeType=application/pdf DocumentEntry.comment=Ergebnisse datengestützter Auswertungen der Krankenkassen zu individuellen Gesundheitsrisiken gemäß § 25b SGB V. Submissionset.authorRole = 105

[<=]

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

Weitere Anforderungen an das Clientsystem des Kostenträgers sind im FHIR Implementation Guide für den Patient Service [gemIG_ePA_Basic] zu finden.

4.1.2 Ablauf eines betreiberübergreifenden Aktenumzugs (informativ)

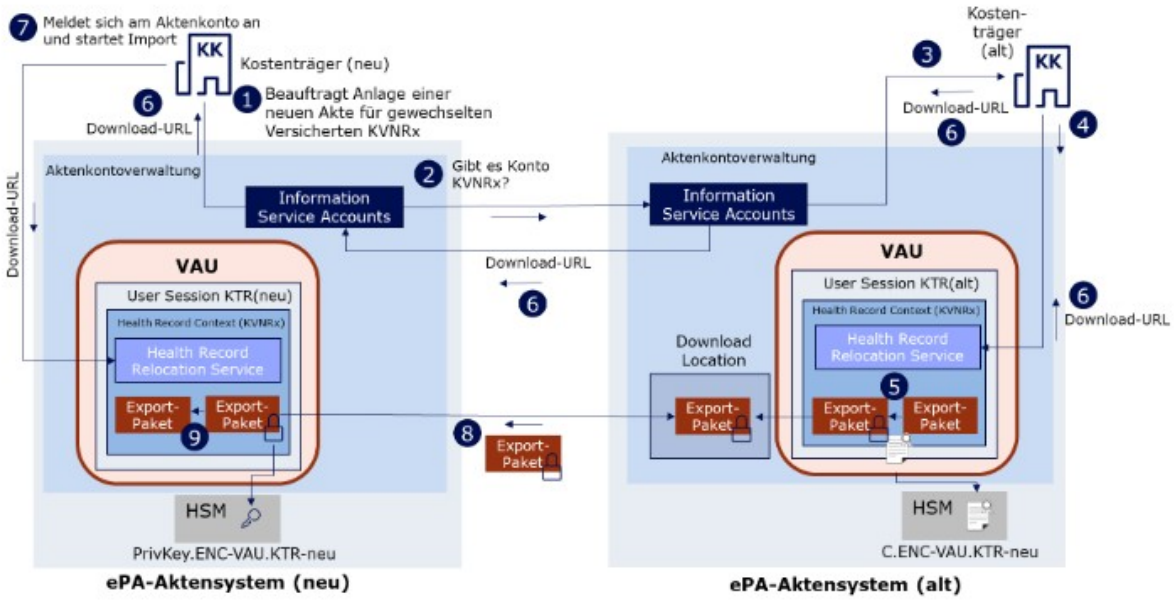


Abbildung 18: Ablauf eines betreiberübergreifenden Aktenumzugs

Anstoßen eines Aktentransfers
Der Kostenträger (neu) lässt im Aktensystem eine neue Akte anlegen (1). Das Aktensystem fragt am **Information Service Account** 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 Account** 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 Account** 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).

4.1.2.1 Erstellung des Exportpakets auf Seiten des alten Kostenträgers

Der **Information Service Account** 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 Exportpakets unter Verwendung des Verschlüsselungszertifikats.

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

Tabelle 21: 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 Account des Aktensystems senden. Das Format dieser Nachricht wird nicht von der gematik vorgegeben und ist betreiberspezifisch.

4.1.2.2 Einspielen des Exportpakets auf Seiten des neuen Kostenträgers

Der **Information Service Account** des neuen Aktensystems informiert das Clientsystem 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 22: 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].**[<=]**

4.1.2.3 Verhalten bei Scheitern des Imports

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

4.1.3 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.

Für einen Versicherten kann nur genau eine E-Mail-Adresse hinterlegt werden.

Folgende Anwendungsfälle werden ermöglicht:

- die beim Kostenträger Versicherten hinterlegte E-Mail-Adresse abrufen
- falls nicht vorhanden eine E-Mail-Adresse für den beim Kostenträger Versicherten hinterlegen

- die E-Mail-Adresse für den beim Kostenträger Versicherten aktualisieren

A_25446-02 -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 getEmailAddress und replaceEmailAddress 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 a) die Teilnahme am digitalen Medikationsprozess (medication) oder b) Einstellen von Verordnungsdaten und Dispensierinformation durch den E-Rezept-Fachdienst, und die Rücknahme dieser Widersprüche,
  - Widerspruch einlegen gegen dieÜbermittlung von pseudonymisierten medizinischen Daten an das Forschungsdatenzentrum Gesundheit (Sekundärdaten) und die Rücknahme dieses Widerspruchs,
  - Widersprüche zur Nutzung von Sekundärdaten
- 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 durch 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.

Die Verarbeitung von Dokumenten gehört nicht zum Funktionsumfang des Clientsystems der Ombudsstelle, das somit die Schnittstellen des XDS Document Service nicht nutzt.

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 Ombudsstelle ein search-access_token, welches das Clientsystem der Ombudsstelle am ePA-Aktensystem anfragt. Dies erfolgt durch Aufruf derOperation 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 23: 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 24: 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 25: 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 *getBlockedUserPolicyAssignments* gemäß [I_Entitlement_Management].**[<=]**

4.2.2 Widersprüche

Das Clientsystem der Ombudsstelle nutzt das **Consent Decision Management** des Aktensystems, um für einen Versicherten Widersprüche zu widerspruchsfähigen Funktionen der ePA einzustellen oder diese zu widerrufen.

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

Tabelle 26: 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 eines Widerspruchs gegen eine einzelne widerspruchsfähige Funktion aus.
`getContentDecisions`	Dieser Operation erlaubt es, den aktuellen Zustand aller Widersprüche über einen einzelnen Aufruf zu ermitteln.
getDateUsagePurposes	Diese Operation liest den aktuellen Zustand der Widersprüche gegen die verschiedenen Zwecke der Sekundärdatennutzung 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].**[<=]**

4.2.2.1 Widersprüche zum Medikationsprozess einstellen oder widerrufen

Das Clientsystem der Ombudsstelle nutzt das **Consent Decision Management** des Aktensystems, um Widersprüche gegen widerspruchsfähige Funktionen des Aktensystem einzulegen bzw. zurückzunehmen.

Es gibt zwei verschiedene Widersprüche:

Tabelle 27: Widersprüche im Rahmen des Medikationsprozesses

Art des Wider-spruchs	Folgen des Widerspruchs	Rücknahme des Widerspruchs
Medication	Die Zugriff auf die Daten der Datenkategorie "emp" im XDS Document Service und die Daten des "Medication Service" (FHIR) wird für alle LEI unterbunden. Bestehende Medikationsdaten	Die Rücknahme des Widerspruchs gegen Medication führt implizit zur Rücknahme des

	werden nicht gelöscht.	Widerspruchs gegen Erp-submission.
Erp-submission	Die Daten der Datenkategorie "emp" im XDS Document Service und die Daten des "Medication Service" (FHIR) werden gelöscht. Das Einstellen von Verordnungen und Dispensierdaten durch den Fachdienst wird abgelehnt. Ein Widerspruch gegen Erp-submission führt implizit auch zu einem Widerspruch gegen Medication.	Die Rücknahme des Widerspruchs gegen Erp-submission hat implizit keinerlei Auswirkung auf den Widerspruch zu Medication.

Es wird folgende Operation genutzt:

Tabelle 28: 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") jeweils 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].**[<=]**

4.2.2.2 Widersprüche zur Sekundärdatennutzung durch das FDZ einstellen oder widerrufen

Das Clientsystem der Ombudsstelle nutzt das **Consent Decision Management** des Aktensystems, um für einen Versicherten einen Widerspruch gegen die Sekundärdatennutzung durch das Forschungsdatenzentrum Gesundheit (FDZ) und Widersprüche gegendie Verwendung dieser Daten für bestimmte Sekundärnutzungszwecke einzustellen oder diese zu widerrufen.

Es gibt den grundsätzlichen Widerspruch gegen die Sekundärdatennutzung durch das FDZ:

Tabelle 29: Widerspruch Sekundärdatennutzung durch das FDZ

Art des Wider-spruchs	Folgen des Widerspruchs	Rücknahme des Widerspruchs
data-submission	Es werden keine Sekundärdaten des Aktenkontos an das FDZ weitergeleitet. Es erfolgt keine Sekundärnutzung von Daten des Aktenkontos durch das FDZ.	Es werden Sekundärdaten des Aktenkontos an das FDZ weitergeleitet. Eine Sekundärnutzung von Daten des Aktenkontos durch das

		FDZ ist möglich.

Tabelle 30: I_Consent_Decision_Management::updateConsentDecision

REST-Schnittstelle des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)	
I_Consent_Decision_Management	
`updateConsentDecision`	Diese Operation setzt für die Sekundärdatennutzung durch das FDZ (functionid "data-submission") eine Zustimmung ("permit") oder eine Ablehnung ("deny").

A_26455 -Entscheidung zur Sekundärdatennutzung setzen durch Ombudsstelle
Das Clientsystem der Ombudsstelle MUSS es dem Nutzer ermöglichen, den Widerspruch zur Sekundärdatennutzung durch das FDZ zu erteilen bzw. zurückzunehmen unter Verwendung der Operation `updateConsentDecision` gemäß [I_Consent_Decision_Management].**[<=]**

Ein Versicherter kann über die Ombudsstelle die einzelnen Sekundärnutzungszwecke zur Sekundärdatennutzung erteilen bzw. widerrufen. Das Management der Sekundärnutzungszwecke kann nur erfolgen, wenn kein Widerspruch gegen die Sekundärdatennutzung erteilt wurde.

Widersprüche zu folgenden Sekundärnutzungszweckengemäß § 303e SGB V Absatz 2 können erteilt oder widerrufen werden:

Tabelle 31: Sekundärnutzungszwecke

Sekundärnutzungszweckegemäß § 303e SGB V Absatz 2
1. Wahrnehmung von Steuerungsaufgaben durch die Kollektivvertragspartner
2.Verbesserung der Qualität der Versorgung sowie Verbesserung der Sicherheitsstandards der Prävention, Versorgung und Pflege
3.Planung von Leistungsressourcen, zum Beispiel Krankenhausplanung oder Pflegestrukturplanungsempfehlungen nach § 8a Absatz 4 des Elften Buches
4.wissenschaftliche Forschung zu Fragestellungen aus den Bereichen Gesundheit und Pflege, Analysen des Versorgungsgeschehens, sowie Grundlagenforschung im Bereich der Lebenswissenschaften
5.Unterstützung politischer Entscheidungsprozesse zur Weiterentwicklung der gesetzlichen Kranken- und Pflegeversicherung
6.Analysen zur Wirksamkeit sektorenübergreifender Versorgungsformen sowie zur Wirksamkeit von Einzelverträgen der Kranken- und Pflegekassen
7.Wahrnehmung von Aufgaben der Gesundheitsberichterstattung, anderer Berichtspflichten des Bundes nach diesem oder dem Elften Buch und der amtlichen Statistik sowie Berichtspflichten der Länder
8.Wahrnehmung gesetzlicher Aufgaben in den Bereichen öffentliche Gesundheit und

Epidemiologie
9.Entwicklung, Weiterentwicklung und Überwachung der Sicherheit von Arzneimitteln, Medizinprodukten, Untersuchungs- und Behandlungsmethoden, Hilfs- und Heilmitteln, digitalen Gesundheits- und Pflegeanwendungen sowie Systemen der Künstlichen Intelligenz im Gesundheitswesen einschließlich des Trainings, der Validierung und des Testens dieser Systeme der Künstlichen Intelligenz
10.Nutzenbewertung von Arzneimitteln, Medizinprodukten, Untersuchungs- und Behandlungsmethoden, Hilfs- und Heilmitteln sowie digitalen Gesundheits- und Pflegeanwendungen, Verhandlung von Vergütungsbeträgen oder Festlegung von Höchstbeträgen und Schwellenwerten nach § 134 sowie Vereinbarung oder Festsetzung von Erstattungsbeträgen von Arzneimitteln nach § 130b

Tabelle 32: I_Consent_Decision_Management::updateDataUsagePurposes

REST-Schnittstelle des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)	
I_Consent_Decision_Management	
`updateDataUsagePurposes`	Diese Operation setzt für die Widersprüche zu Sekundärnutzungszwecken (functionid "data-submission") eine Zustimmung ("permit") oder eine Ablehnung ("deny").

A_26456 -Entscheidung zur Sekundärdatennutzung setzen durch Ombudsstelle
Falls kein Widerspruch gegen die Sekundärdatennutzung erteilt wurde MUSS das Clientsystem der Ombudsstelle dem Nutzer ermöglichen, Widersprüche zu Sekundärnutzungszwecken zu erteilen bzw. zurückzunehmen unter Verwendung der Operation `updateDataUsagePurposes` gemäß [I_Consent_Decision_Management].**[<=]**

Um den Zustand der Widersprüche zu Sekundärnutzungszwecken festzustellen, benutzt das Clientsystem folgende Operation:

Tabelle 33: I_Consent_Decision_Management::getDataUsagePurposes

REST-Schnittstelle des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)	
I_Consent_Decision_Management	
`getDataUsagePurposes`	Diese Operation den aktuellen Zustand der Widersprüche zu Sekundärnutzungszwecken für das Aktenkonto aus

A_26458 -Entscheidungen zu widerspruchsfähigen Funktionen abfragen
Falls kein Widerspruch gegen die Sekundärdatennutzung erteilt wurde MUSS das Clientsystem der Ombudsstelle dem Nutzer ermöglichen, den aktuellen Zustand der Widersprüche zu Sekundärnutzungszwecken abzufragen unter Verwendung der Operation `getDataUsagePurposes` 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 Schnittstellen des FHIR Implementation Guide für den Audit Event Service [gemIG_ePA_Basic].

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 34: Schnittstellen IG_Audit_Event_Service

REST-Schnittstelle des Aktensystems (Nutzung nur bei etabliertem VAU-Kanal)	
Query API: AuditEvent	
`listAuditEvents_AuditEventSvc`	Mit dieser Operation kann die Ombudsstelle über eine FHIR-basierte Abfrage unter Nutzung der entsprechenden Suchparameter die Protokolldaten eines Aktenkontos abrufen.
`getAuditEventById_AuditEventSvc`	Diese Operation ermöglicht der Ombudsstelle über eine FHIR-basierte Abfrage das Lesen einer AuditEvent Instanz.
Render API: PDF Audit	
`renderAuditEventsToPDF`	Mit dieser Operation kann die Ombudsstelle die Protokolldaten eines Aktenkontos als PDF/A Dokument abrufen.

Weitere Anforderungen sind im FHIR Implementation Guide für den Audit Event Service [gemIG_ePA_Basic] zu finden.

4.3 Funktionsumfang Clientsystem DiGA

Das Clientsystem eines DiGA-Herstellers kann DiGA-Daten in die ePA einstellen und aktualisieren. Für jede mit einer individuellen Telematik-ID ausgestatteten DiGA legt dazu das Aktensystem 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 eingestellten Dokumentes persistieren, falls er die Möglichkeit nutzen möchte, für dieses Dokument Updates durchzuführen. Hierzu ist es gemäß [IHE-ITI-TF2#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 35 : I_Information_Service::setUserExperienceResult

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

A_24685-01 -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 36: 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.
UX_MHD_Search_PS	Es wird der Zeitraum zwischen "Absenden der MHD Find Document References - Nachricht" bis zur "Anzeige der

	Ergebnisse" gemessen.
UX_MHD_Download_PS	Es wird der Zeitraum zwischen "Absenden der MHD Retrieve Document - Nachricht" bis zur "Information des Nutzers über den erfolgreichen Download" / "Anzeige des Dokumentes" gemessen

[<=]

A_24686-01 -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.**[<=]**

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.

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.

Ein Großteil des Kapitels beschreibt dabei das Dokumenten-Management über den traditionellen XDS Document Service. Ab ePA 27 ist dieser Dienst nur noch eingeschränkt verfügbar. Das heißt insbesondere:

- Das Aktualisieren von Metadaten ist nicht mehr über XDS möglich; die RMU-Schnittstelle wird abgeschaltet.
- Es ist nicht der vollständige Dokumentenhaushalt über XDS einsehbar: Alle über MHD eingestelle Dokumente sind nicht im XDS Document Service sichtbar.
- Strukturierte Laborbefunde (dgLP Laborbefund) können ausschließlich über MHD eingestellt werden.

Das heißt, für die meisten Clients ist eine (alleinige) Nutzung des XDS Document Service nicht mehr sinnvoll oder akzeptabel, abgesehen von Clients mit stark eingeschränkten Funktionsanforderungen (bspw. ausschließliches Einstellen von eArztbriefen).

Am Ende findet sich noch eine minimale Einordnung des MHD Service. Details finden sich jedoch (auch für Primärsysteme) in [gemIG_ePA_MHD].

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 *Voraussetzung für eine Befugniserzeugung*).

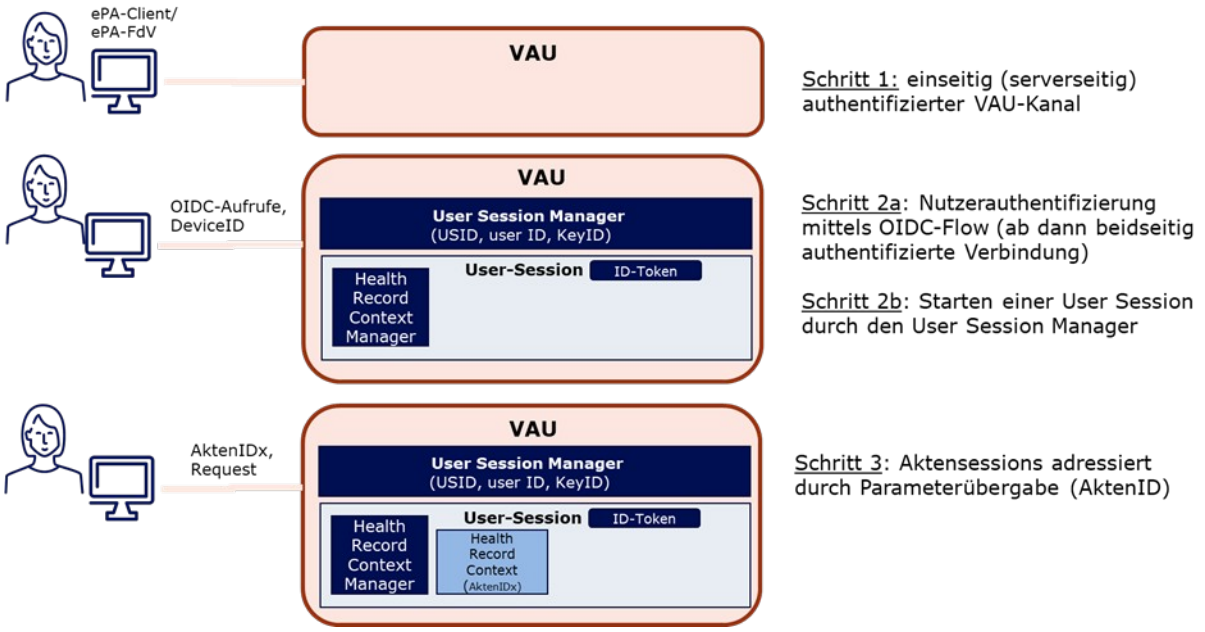


Abbildung 19: Voraussetzung für eine Befugniserzeugung

In allen Sektoren setzt die Benutzung der ePA voraus, dass ein technisch nachgewiesener Behandlungskontext vorliegt und eine Befugnis erzeugt wird. Dies geschieht, indem die eGK eingelesen, eine Prüfziffer vom VSDM erzeugt und dieser HMAC signiert in das ePA-Aktensystem eingestellt wird. Alternativ kann beim Einlesen der eGK oder durch Nutzung der GesundheitsID auch ein PoPP-Token vom PoPP Service bezogen werden und dieses in das ePA-Aktensystem eingestellt werden. Das Einstellen des VSDM-Prüfnachweises oder PoPP-Tokens 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.

Im Allgemeinen führt der erste Besuch im Quartal wegen des obligatorischen VSDM-Abrufs zum Einstellen einer Befugnis – Fehlersituationen können aber auch zu einem anderen Ergebnis führen. Für weitere Besuche in einer Leistungserbringer-Institution wird daher empfohlen, dass das PS unmittelbar beim Eintreffen des Versicherten versucht, auf dessen Akte zuzugreifen. Falls der Zugriff auf die vorhandene Akte aufgrund einer fehlenden Befugnis nicht möglich ist, sollte das PS hierüber informieren und empfehlen, die eGK erneut in das KT zu stecken. Bei erneutem Stecken der eGK wird das Einstellen der Befugnis vom PS angestoßen.

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 öffentlichen 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 Befugnis 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/ECC/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).

Um neu eingestellte Inhalte zu ermitteln, kann die RegistryStoredQuery *FindSubmissionSets* mit den Parametern $*XDSSubmissionSetSubmissionTimeFrom* und $*XDSSubmissionSetSubmissionTimeTo* verwendet werden, gefolgt von *GetSubmissionSetAndContents* zu jedem gefunden SubmissionSet, um die dazugehörigen Dokumenteinträge zu erhalten. 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 (FHIR)
- Bildbefund (PDF/A)
- Befundberichte aus invasiven oder chirurgischen sowie aus nicht-invasiven oder konservativen Maßnahmen (PDF/A)

Bei vorliegender Zustimmung eines Patienten kann diese Liste patientenindividuell um weitere Dokumente erweitert werden.

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 prüft zudem bei jedem jedem Hochladen anhand einer Hashwertbildung über das Dokument selbst, ob es sich um eine Dublette handelt. Bestehende Dokumente können auch ersetzt werden. Dabei entsteht ein Verweis zwischen beiden Versionen und die alte Fassung wird als veraltet markiert.

Für den Fall, dass dem Hochladen eines 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, auch um sicherzustellen, dass das Dokument nicht später versehentlich doch noch hochgeladen wird.

Im stationären Sektor bezieht sich ein Widerspruch gegen das Hochladen von Daten im aktuellen Behandlungskontext einheitlich auf sämtliche Daten dieses Behandlungskontexts. Es besteht kein Anspruch auf einen differenzierten Widerspruch. Ein vom Primärsystem erzeugter Protokolleintrag/Hinweisnotiz sollte sich entsprechend auf alle Daten im aktuellen Behandlungskontext beziehen. Eine Widerspruchsmöglichkeit auf Basis einzelner Dokumente kann ein Primärsystem im stationären Sektor darüber hinaus umsetzen.

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 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 diesem Fall 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.

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 eArztbrief abgewählt wurde, erzeugt das Primärsystem demnach standardmäßig einen Protokolleintrag in der Patientenübersicht oder eine Notiz

in der Karteikarte der Patient:in, dass diese:r dem Hochladen des eArztbriefs widersprochen hat. Im stationären Sektor bezieht sich ein Widerspruch im Behandlungskontext immer auf alle Daten des aktuellen Behandlungskontexts und sollte dementsprechend protokolliert werden. Der eArztbrief wird per KIM verschickt, jedoch nicht in das ePA-Aktenkonto hochgeladen.

Eine elektronische Arbeitsunfähigkeitsbescheinigung (eAU) ist nur auf Wunsch des Versicherten durch den Leistungserbringer in das ePA-Aktenkonto hochzuladen. Beim Versand einer eAU per KIM kann demnach analog verfahren werden, sofern der Versicherte dem Leistungserbringer gegenüber einen solchen Wunsch geäußert hat. Der Wunsch kann auch als generelle Zustimmung für alle folgenden eAUs geäußert werden; das Primärsystem darf das Hochladen anschließend als Standard beim Versand von eAUs per KIM einstellen. Gleichermaßen kann auch mit anderen Dokumententypen verfahren werden, die regelmäßig durch den Leistungserbringer in die ePA eingestellt werden. Nähere Festlegungen zur eAU werden im Abschnitt 6.1.6 getroffen.

6.1.6 Vorgaben für eAU

Nachfolgend sind die Festlegungen von KBV und GKV-SV aufgeführt:

Einstellen einer eAU

1. Das Primärsystem bietet dem Anwender Möglichkeiten, die Einwilligung des Versicherten zur Einstellung von eAUs zu dokumentieren. Hierbei können einmal hinterlegte Angaben wieder angepasst werden. Eine Anpassung der Entscheidung des Versicherten zum Einstellen in die ePA gilt nicht rückwirkend für bereits an die Krankenkasse versandte eAUs. Es ist möglich, für einzelne eAUs das Einstellen in die ePA abzuwählen (z. B. bei Vorliegen stigmatisierender Diagnosen).
2. Sofern die Einwilligung des Versicherten zur Einstellung der eAU vorliegt und der Arzt die notwendigen Berechtigungen besitzt, stellt die Software bei Versicherten, die über eine ePA verfügen, automatisch mit dem Versand der eAU an die Krankenkassen die an die Krankenkasse versandte eAU (als PKCS7-Datei gemäß den Anforderung P310-14 und P4-01 der Technischen Anlage eAU [KBV_eAU]) in die ePA des Versicherten..
3. Die Software dokumentiert, ob grundsätzlich oder im Einzelfall der Wunsch auf Einstellen einer eAU in die ePA vorlag oder nicht und somit eine eAU in die ePA eingestellt wurde oder nicht.
4. Die Metadaten sind nach den Vorgaben aus [gemSpec_IG_ePA] gemäßA_26443 zu belegen.
5. Die Software weist den Anwender im Bedarfsfall mit aussagekräftigen Hinweisen auf Fehler/Probleme im Rahmen der Einstellung der eAU in die ePA hin.

Stornieren einer eAU

1. Sofern im Primärsystem eine versendete eAU storniert wird, löscht das Primärsystem die eingestellte eAU aus der ePA (sofern alle Voraussetzungen vorliegen).
2. Wenn vom Anwender eine neue eAU ausgestellt wird, so wird Punkt 2 von „Einstellen einer eAU“ durchgeführt.

Fehler im Rahmen des Versandes einer eAU

1. Sofern ein Anwender im Primärsystem zu einer versendeten eAU eine Fehlermeldung der Krankenkasse erhält, bietet das Primärsystem dem Anwender die Möglichkeit, die eingestellte eAU aus der ePA zu löschen (sofern alle Voraussetzungen vorliegen).
2. Wenn vom Anwender eine neue eAU ausgestellt wird, so wird Punkt 2 von "Einstellen einer eAU" durchgeführt.

6.1.7 Hochladen in ein ePA-Aktenkonto als Standard für NFDM (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) dieser standardmäßig in das dazugehörige ePA-Aktenkonto der Patient:in hochgeladen wird. 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.

Der Master-Datenträger für NFDM ist die eGK.

6.1.8 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.

6.1.9 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.

6.1.10 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 (eArztbrief und weitere Dokumente auf Wunsch des Versicherten)

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 20). Eine weitere Möglichkeit ist, dass die Dokumente des ePA-Aktenkontos in der Dokumentenverwaltung integriert und dort zur Anzeige gebracht werden (siehe Abbildung 21).

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 37: 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

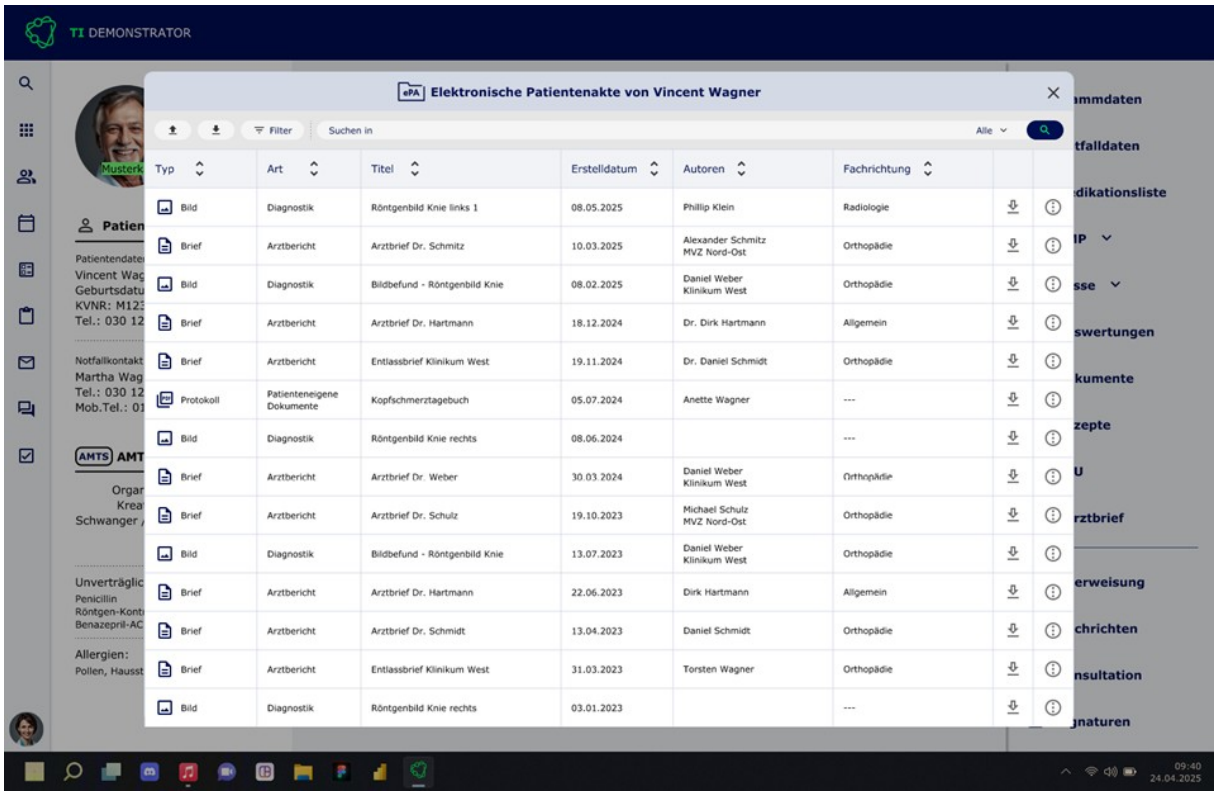


Abbildung 20: Anzeige der ePA-Dokumentenübersicht als separate Ansicht aus einer Karteikarte heraus

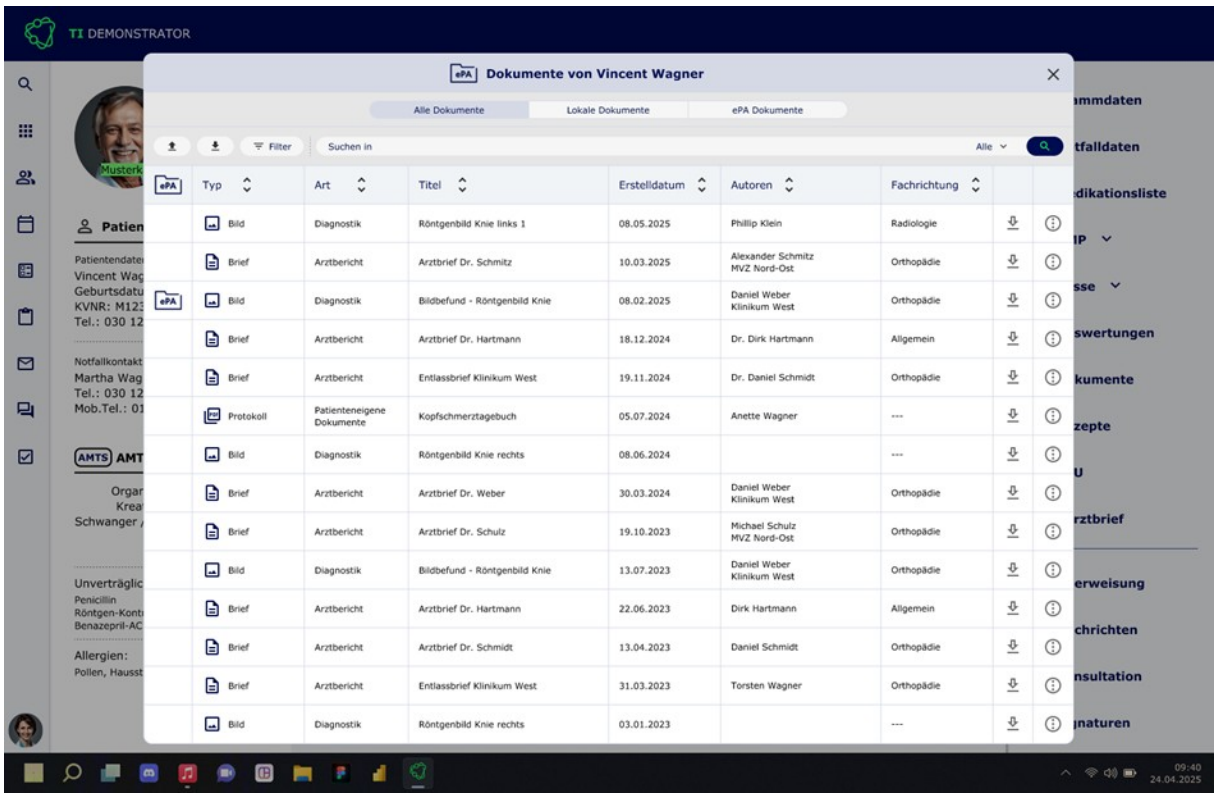


Abbildung 21: Anzeige von ePA-Dokumenten als Teil einer integrierten Dokumentenübersicht in der lokalen Dokumentenverwaltung

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. Zusätzlich gibt es die Möglichkeit, auch Dokumenteninhalte (aktuell PDF/A und Textdokumente) zu durchsuchen. Siehe auchentsprechender Abschnitt im Kapitel Dokumentenmanagement , der die Hauptcharakteristika und Unterschiede beider Suchen beschreibt. Auch die Volltextsuche soll vom Primärsystem unterstützt werden, da sie ein nützliches Hilfsmittel bei der Sichtung größerer Dokumentensammlungen bietet.

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 eventCodeList 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.

Das Einstelldatum von Dokumenten wird über die sogenannten SubmissionSets festgelegt (nur über Suchschnittstelle ITI-18, nicht ITI-67 durchführbar), mir denen jeweils ein oder mehrere Dokumente in die Akte eingestellt werden. Die SubmissionSets werden in der ePA gespeichert und verfügen neben anderen Metadaten auch über das Einstelldatum (SubmissionSet.submissionTime), nach dem auch in der Suche gefiltert werden kann. Eine mögliche Suchstrategie, mit der sich die Suche "Neu eingestellte Dokumente ab einem bestimmten Datum" mithilfe der "Registry Stored Query"-Suchen des Aktensystems umgesetzt werden kann, wird im Folgenden gezeigt:

- FindSubmissionSets (Suche nach SubmissionSets mit Filter auf SubmissionSet.submissionTime für Suche ab einem bestimmten Datum)
- GetAssociations (Einmal pro gefundener Association: Herunterladen aller Verlinkungen, die mit dem SubmissionSet eingestellt wurden; die Associations verlinken jeweils auf der einen Seite das SubmissionSet und auf der anderen Seite ein damit eingestelltes Dokument)
- GetDocuments (Herunterladen der DocumentEntries, der eigentlichen Dokumentenmetadaten, anhand der verlinkten Dokumente aus dem vorhergehenden Schritt)

Die DocumentEntries spiegeln am Ende alle seit einem bestimmten Termin neu eingestellte Dokumente wieder. Ein oder mehrere Dokumente können anschließend gezielt heruntergeladen werden.

Eine andere Strategie, insbesondere dann, wenn viele neue Dokumente erwartet werden, ist es, beim Aufruf von FindSubmissionSets zunächst nur leichtgewichtige Referenzen (returnType="ObjectRef") zu suchen. Damit lassen sich dieselben Schritte wie oben durchführen, nur dass bei der ersten Suche keine SubmissionSet-Metadatenobjekte zurückkommen, sondern nur deren eindeutige Kennungen. Damit lässt sich ein Client-seitiges "Paging" (ein gestaffelter, "seitenweiser" Zugriff) durchführen, der vom Server nicht direkt unterstützt wird. Damit erhält das Primärsystem zunächst sehr schnell alle relevanten SubmissionSets und kann dann gestaffelt über GetAssociations() jeweils für eine gewünscht Anzahl von SubmissionSets (z. B. 20) die dazugehörigen Verlinkungen holen. Falls die Informationen (wie einstellende Einrichtung, exaktes Einstellungsdatum etc.) aus den SubmissionSet-Objekten ebenfalls benötigt werden, müssen sie allerdings früher oder später ebenfalls noch via GetSubmissionSets() heruntergeladen werden.

Falls lokal noch keine oder fast keine Informationen zu Dokumenten in der Akte vorliegen, kann auch der Aufruf der "Stored Query" GetAll sinnvoll sein. Falls jedoch regelmäßig Dokumente abgeglichen werden, ist diese Variante für Clients unnötig langwierig und erzeugen auf den Aktensysteme auch unnötige Last.

In einigen Fällen kann es gewünscht sein, neben den beschriebenen Filtermöglichkeiten in den Metadaten auch im Volltext der Dokumente zu suchen, um festzustellen, ob sie für eine bestimmte Fragestellung von Relevanz sind. Häufig ist vermutlich eine Kombination beider Suchansätze relevant ("Zeige alle Dokumente, die Arztbriefe sind und nach dem

1.1.2020 eingestellt wurden und das Wort 'Blutdruck' enthalten"). Diese Suche sucht über Metadaten von DocumentEntries und SubmissionSets (benötigt also die ITI-18-Suche) als auch über Dokumenteninhalte ("Blutdruck"). Dem Primärsystem ist es überlassen, wie eine entsprechende Suchmaske dem Nutzer dargeboten wird. Es ist in vielen Fällen wahrscheinlich sinnvoll, beide*technisch getrennten* Suchen unter einer gemeinsame *logische* Eingabemaske abzubilden. Je nach Eingabe entscheidet das Primärsystem, welches Suchverfahren und welche Suche im Detail zum Einsatz kommen.

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 22 und Abbildung 23 entnommen werden.

Tabelle 38: 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

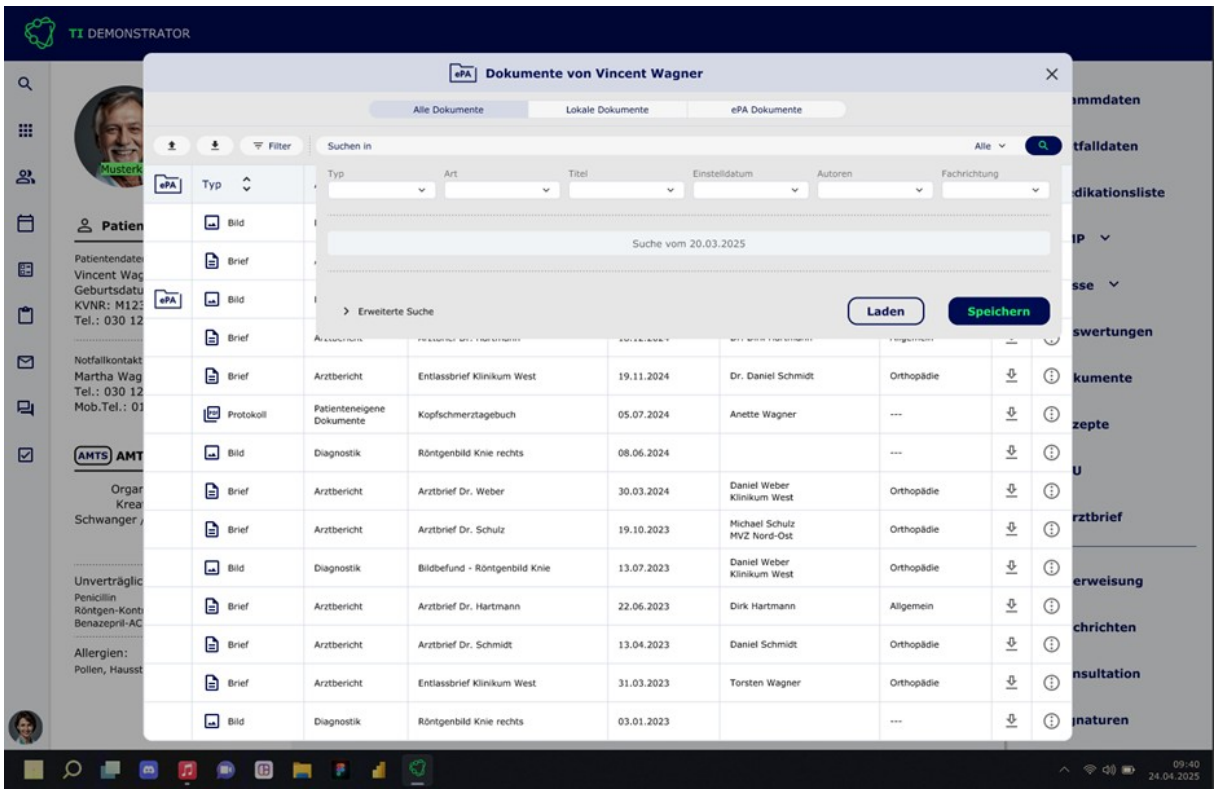


Abbildung 22: Funktion im Primärsystem, um zu suchen, filtern und sortieren von Dokumenten in einem ePA-Aktenkonto

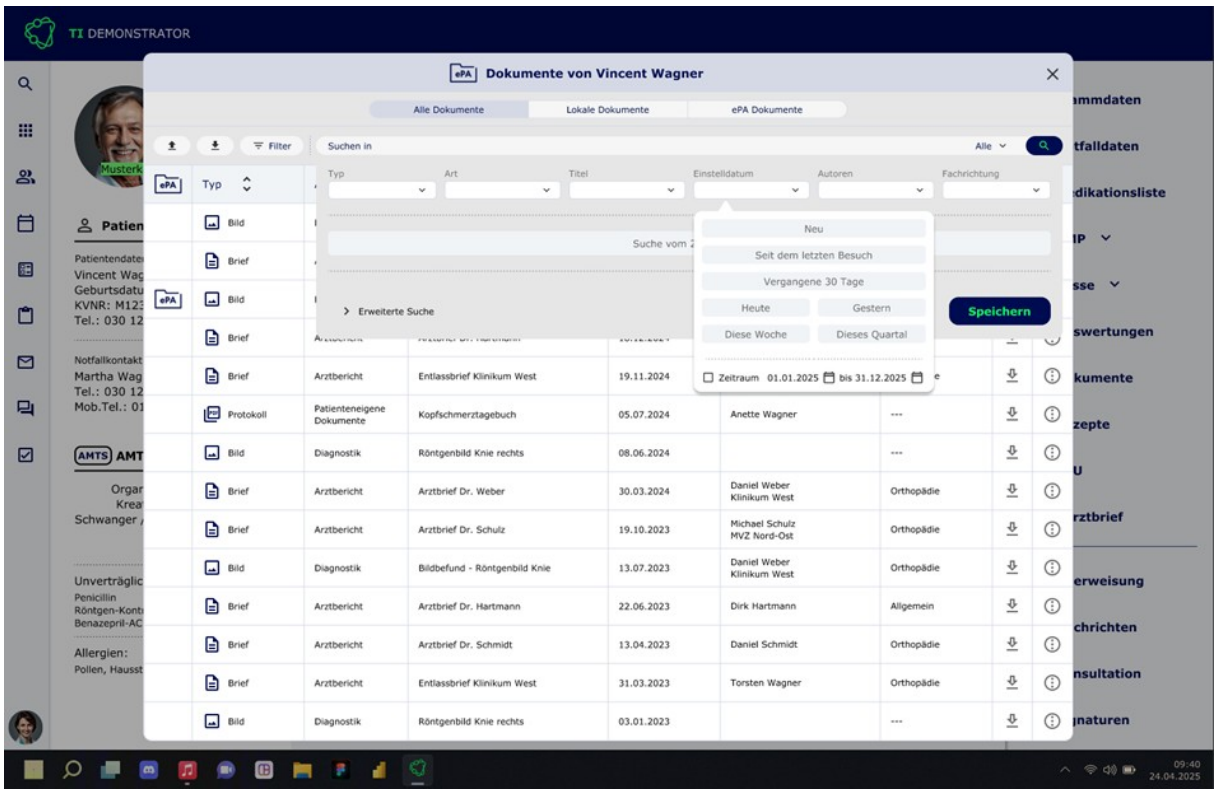


Abbildung 23: Funktion im Primärsystem, um zu suchen, filtern und sortieren von Dokumenten in einem ePA-Aktenkonto

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 und muss im Hintergrund laufen. Ein sog. "Freezing" des Systems, welches verhindert, dass der Nutzer während des Herunterladens des Dokuments weitere Aktivitäten ausführen kann, ist zu vermeiden. 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 21 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.*
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.*
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 39: 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

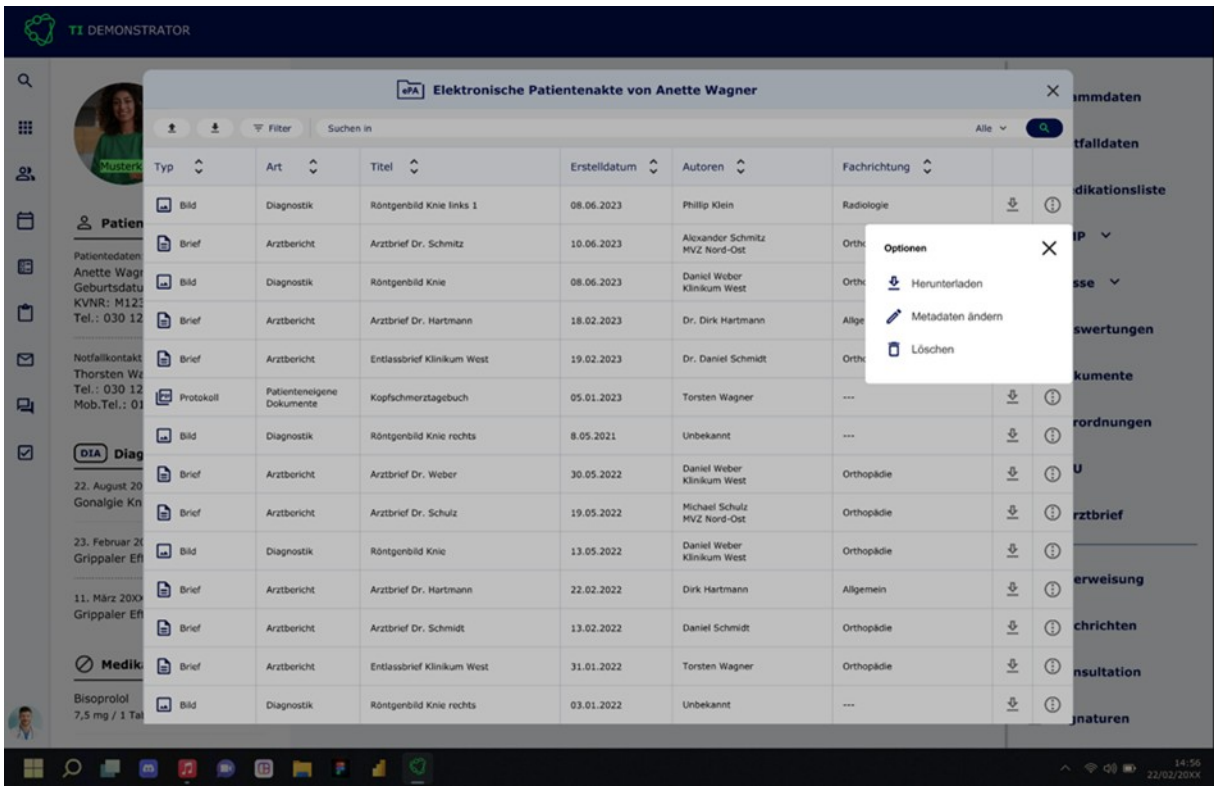


Abbildung 24: Anzeige eines Kontextmenüs für ein ausgewähltes Dokument, um dieses zu bearbeiten (am rechten Bildrand ist der Menüpunkt zu finden)

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 25 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 40: 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.

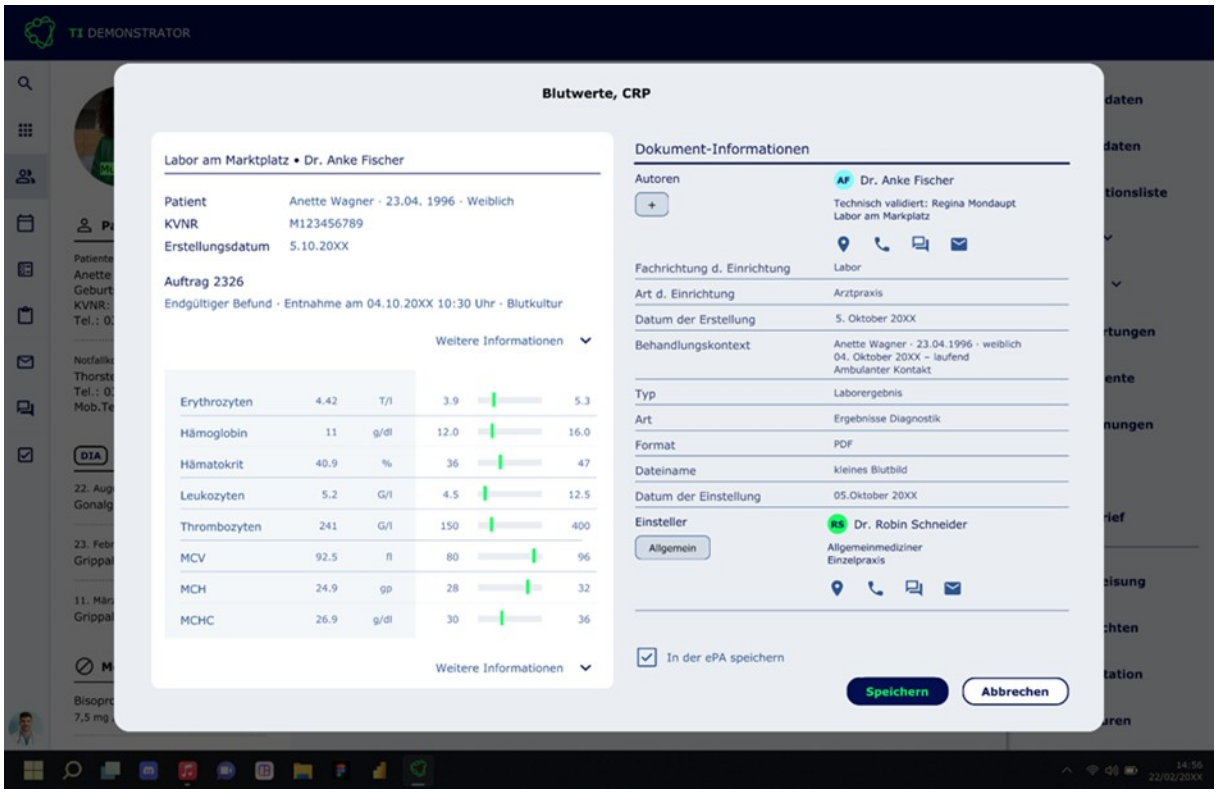


Abbildung 25: Eingabemaske mit der vorausgefüllten Einstellung, dass ein Dokument (am unteren Bildrand ist der Menüpunkt zu finden)

6.2.5 Dokument hochladen aus KIM-Workflow

Um eines 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 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.

Für weitere Dokumente, darunter die eAU, soll dies ebenfalls beim Versand von KIM anwählbar sein oder patientenindividuell als Standard festgelegt werden können. Bei diesen Dokumenten ist die Zustimmung des Versicherten einzuholen und lokal zu dokumentieren. Dies kann auch einmalig für alle Dokumente desselben Typs erfolgen.

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 beispielhaft am eArztbrief der Abbildung 26 entnommen werden.

Tabelle 41: Dokument hochladen aus KIM-Workflow - UX Optimaler Klickpfad

Titel	**ePA_DMS_5 - Dokument hochladen aus KIM-Workflow**
Zielstellung	Der Nutzer verschickt einen eArztbrief 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. • 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 eArztbrief. 2. Es wird eine KIM-Nachricht erstellt mit dem eArztbrief 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.

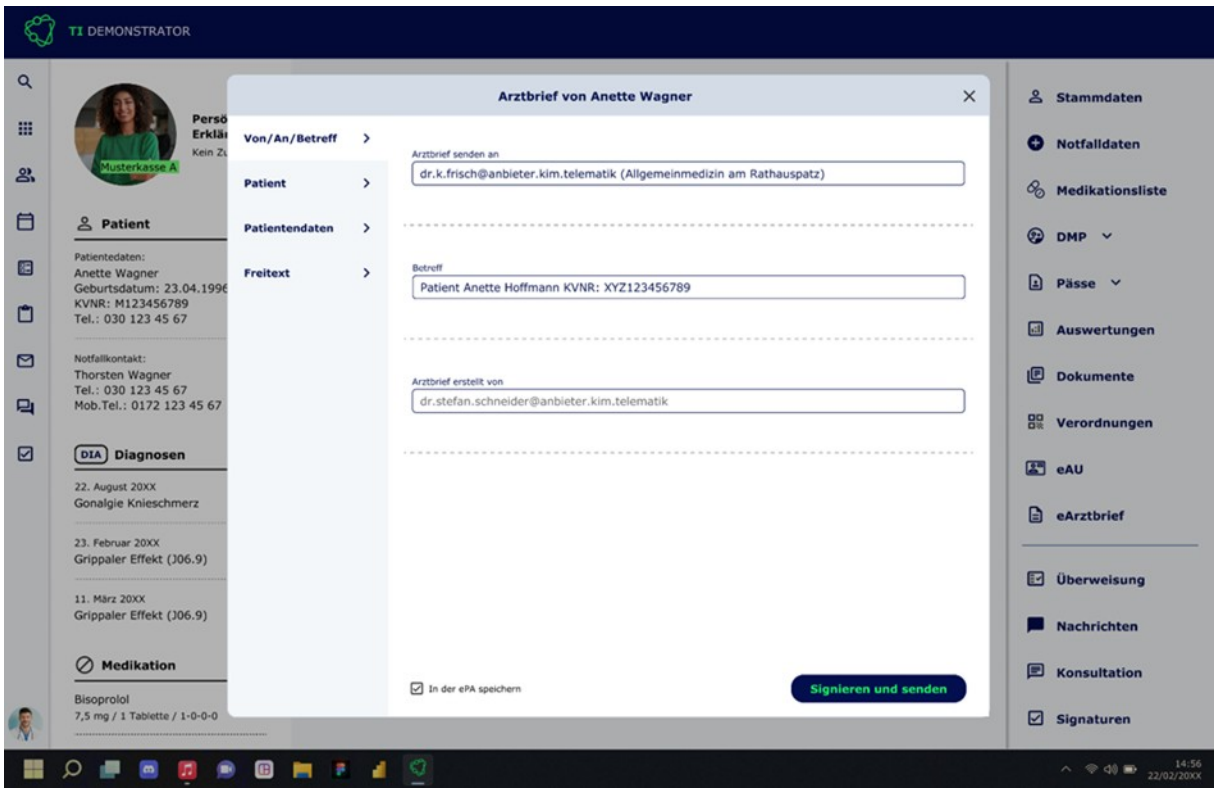


Abbildung 26: Option zum Hochladen eines Dokuments im Falle des Versands eines eArztbriefs im Rahmen des KIM-Workflows ist standardmäßig ausgewählt

6.2.6 ePA MHD Service

Zusätzlich zu den oben beschriebenen Suchfunktionalitäten des XDS Document Service steht den Primärsystemen auch der MHD Service zur Verfügung, der eine tendenziell leichtgewichtigere Suche über FHIR-Schnittstellen ermöglicht. Ab ePA 27 ist es zudem möglich, auch alle anderen typischen Dokumenten-Management-Funktionen (Löschen, Aktualisieren, Einstellen) über den MHD Service abzuwickeln. Zudem erlaubt es der MHD Service seit ePA 3.1.3 auch, den Volltext der Dokumente in einem Aktenkonto zu durchsuchen. Alle Details zum ePA MHD Service finden sich in [gemIG_ePA_MHD].

7 Fehlerbehandlung

Auftretende Fehlertypen unterscheiden sich je nach Architekturebene:

- http-Fehler auf Transportebene
- Fehler an REST-Schnittstellen
- Fehler auf Ebene des Dokumentenmanagements

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 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 42: 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	403	notEntitled	Die Leistungserbringerinstitution ist

no valid entitlement			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 does not exist	404	noHealthRecord	Das Aktenkonto existiert nicht (mehr).
Health record is not in state ACTIVATED	409	statusMismatch	Das Aktenkonto befindet sich im Umzug, ca. 24 Stunden 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.

7.2 Fehlerbehandlung im XDS Document Service

Der Zugriff auf die IHE-Schnittstellen des XDS Document Service erfolgt durch das Primärsystem über [SOAP].

IHE-Fehler werden werden ausschließlich im IHE-Protokoll übertragen, d.h. auch wenn in der IHE-Response ein IHE-Fehler enthalten ist, wird der http-Statuscode 200 zurückgeben.

Ab ePA 3.1.3-1 Umsetzungsphase 2 gilt:

Eine konkreteFehlerprüfung im Aktensystem erfolgt für alle im Request enthaltenen Dokumente (gemäß gemSpec_Aktensystem_ePAfueralle#A_28657*), d.h. in der IHE-Fehlermeldung sind alle Dokumente aus dem Request enthalten, die diesen Fehler verursacht haben. Falls beispielsweise in einem Request zwei Dokumente eingestellt werden sollen, die bereits in der Akte vorhanden sind, führt dieser Aufruf zu einem Fehler. Die IHE-Response enthält eine Fehlerliste (`RegistryErrorList`), die zwei Einträge (`RegistryError`) enthält. Der Fehler in diesen beiden Einträgen ist XDSDuplicateDocument (`errorCode`).

7.2.1 IHE-Error

In der Response der IHE-Schnittstellen-Aufrufe können verschiedene Fehler auftreten. Sie lassen sich grundsätzlich gemäß ihres ResponseStatusType in drei Kategorien (Erfolg, Teilerfolg und Fehler) unterteilen. Die folgende Tabelle stellt die verschiedenen Statuskategorien dar. Der Status wird dabei im Attribut rs:RegistryResponse/@status Attribut zurückgegeben:

Tabelle 43: Tab_ILF_ePA_IHE_Success_and_Error_Reporting

Wert in rs:RegistryResponse/@status	Beschreibung	Erläuterung	Beispiel Anzeigetext
urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success	[IHE-ITT-TF3]#4.2.4	Die ausgeführte Transaktion konnte ohne Fehler durchgeführt werden.	Transaktion erfolgreich.
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.

Im Falle von einem oder mehreren Fehlern oder auch Warnungen wird eine Liste (RegistryErrorList) zurückgeschickt, welche die Probleme mit der Anfrage auflistet. Falls die ErrorList nur Warnings enthält (RegistryError-Elemente severity=warning im

Gegensatz zu severity=error), kann die Verarbeitung als vollständig 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.

7.2.2 Erweiterte Angaben des Aktensystems zum Fehler in codeContext

Zusätzlich zu den Vorgaben aus [ITI TF Vol 3#4.2.4] "Success and Error Reporting" gibt es Vorgaben für das Aktensystem, wie`codeContext` mit weiteren Angaben zum Fehler zu befüllen ist.

Ab ePA 3.1.3-1 Umsetzungsphase 2 gilt:

Die Formatvorgabe für `codeContext` ist in A_28655* beschrieben. Lässt sich der Fehler auf ein SubmissionSet, DocumentEntry oder Folder zurückführen lässt, und dessen uniqueId bekannt ist, so wird in `codeContext` die entsprechende uniqueId wie folgt enthalten sein: "`uniqueId='<DocumentEntry.uniqueId>'`" (gemäß [gemSpec_Aktensystem_ePAfueralle#A_28654*).

Im XDS Document Service sind zahlreiche Fehlersituationen in Anforderungen beschrieben, die dann auch weitere Inhalte zum Fehler in `codeContext` fordern.

Beispiel - Validierung der Metadaten aus ITI Document Sharing-Profilen gemäßA_14938*:

RegistryError mit:

errorCode = `XDSRepositoryMetadataError`
codeContext =
`"uniqueId='2.25.269167723254896828623';errorText='Cannot register document: Metadata do not match A_14760';metadata='authorPerson';metadata='authorRole'"`

Informationen aus codeContext:

1. Bei welchem Dokument/SubmissionSet tritt der Fehler auf ->`uniqueId`, d.h. Dokument 2.25.269167723254896828623 hat den Fehler verursacht. Wenn die uniqueId diejenige des SubmissionSet wäre, würde sich der Fehler auf die Metadaten des SubmissionSet beziehen.
2. Was ist das für ein Fehler ->`errorText: "Cannot register document: Metadata do not match A_14760"`, d.h. die Validierung der Metadaten ist fehlgeschlagen
3. Welche Metadaten sind fehlerhaft ->`metadata: authorPerson, authorRole`, d.h. die Metadaten `authorPerson` und `authorRole` genügen nicht den Vorgaben des Aktensystems

Zusätzlich zur uniqueId und sonstigen Vorgaben können mit`errorDetail` (gemäß A_28656) optional in `codeContext` weiterführende Informationen zum Fehler übertragen werden.

Beispiel:

RegistryError mit:

errorCode = `InvalidDocumentContent`
codeContext =
`"uniqueId='2.25.269167723254896828623';errorDetail='Fehlerhafter Aufrufparameter [PDF service encountered an unacceptable document format for validatePDF'"`

Informationen aus codeContext:

1. Bei welchem Dokument/SubmissionSet tritt der Fehler auf ->`uniqueId`, d.h. Dokument`2.25.269167723254896828623` hat den Fehler verursacht.
2. Das PDF-Dokument ist kein erlaubtes PDF-Format

Wie sich aus den Beispielen ablesen lässt, wird der codeContext mit "Key:Value"-Paaren befüllt; die generische Struktur soll das Auslesen der Details erleichtern.

7.2.3 Fehlermeldungen aus dem XDS Document Service

Das Aktensystem kann unter anderem die Fehler (`errorCode`) der Tabelle Tab_ILF_ePA_IHE-Fehlermeldungen_Aktensystem zurückliefern. Weitere mögliche Fehler werden in [IHE-ITI-TF3#Table 4.2.4.1-2] gelistet. Die in der Tabelle und bei IHE beschriebenen Fehler Codes können unvollständig sein.

Tabelle 44: Tab_ILF_ePA_IHE-Fehlermeldungen_Aktensystem

errorCode	Mögliche Gründe	Referenz
InvalidDocumentContent	Es wird versucht, ein Notfalldokument mehrmals einzustellen.	[gemSpec_Aktensystem_ePAfueralle#A_24456*] [gemSpec_Aktensystem_ePAfueralle#A_25137*] [IHE-ITI-TF3#4.2.4]
LegalPolicyViolation	Zugriffsunterbindungsregeln wurden verletzt	[gemSpec_Aktensystem_ePAfueralle#A_24509*]
UnresolvedReferenceException	Versuch, ein Dokument in einen dynamischen Ordner zu schreiben, der entweder verborgen ist oder nicht existiert.	[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]
XDSDuplicateDocument	Dokument existiert bereits in der Akte	[gemSpec_Aktensystem_ePAfueralle#A_24988*]
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.]

XDSInactiveCode	Die übermittelten Daten enthalten einen Code im Status "inactive", der nicht mehr verwendet werden darf. codeContext enthält den Code-Wert.	[gemSpec_Aktensystem_ePAfueralle#A_28159*]
XDSFolderAccessDenied	Der Zugriff auf einen Ordner ist nicht erlaubt. Dieser Fehler wird zurückgegeben, wenn versucht wird in eine Kategorie einzustellen, die vor dem LEI verborgen wurde.	[gemSpec_Aktensystem_ePAfueralle#A_28858*]

7.3 Anforderungen an das Primärsystem bei IHE-Fehlern

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.**[<=]**

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.**[<=]**

7.4 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 29). Der UHD verantwortet demnach die Behebung von Störungen, die von Nutzern gemeldet werden.

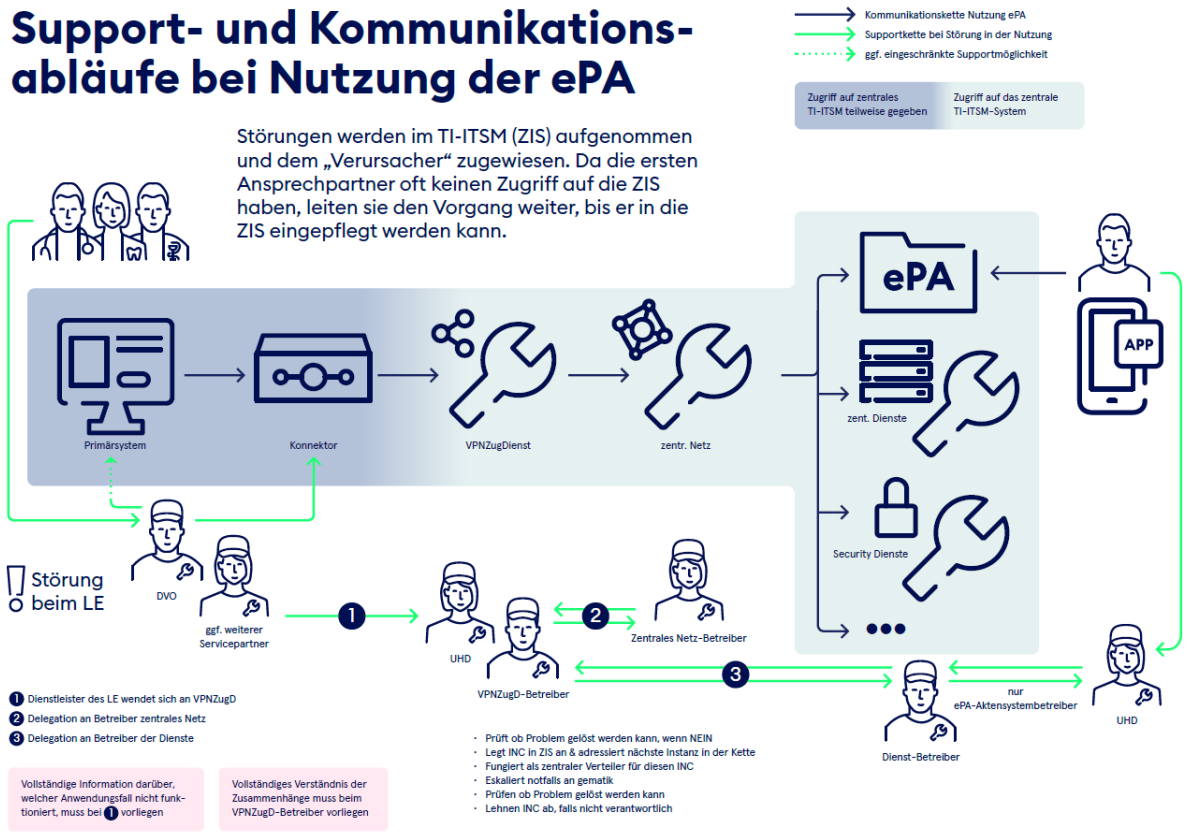


Abbildung 27: Support- und Kommunikationsabläufe bei Nutzung der ePA

8 Anhang A – Verzeichnisse

8.1 Abkürzungen

Kürzel	Erläuterung
AS	Aktensystem
AVS	Apothekenverwaltungssystem
BAG	Berufsausübungsgemeinschaft
CS	Clientsystem
DPE	Datensatz Persönliche Erklärungen
dgMP	Digital gestützter Medikationsprozess
DTBS	Data To Be Signed – zu signierende Daten
DTBSR	Data to be Signed Representation – maschinenlesbare Repräsentation der zu signierenden Daten
E-Rezept	elektronisches Rezept
eAB/eArztbrief	elektronischer Arztbrief
eGK	elektronische Gesundheitskarte
eML	elektronische Medikationsliste
eMP	elektronischer Medikationsplan
ePA	elektronische Patientenakte
FdV	Frontend des Versicherten gemäß gemSpec_ePA_FdV
FDZ	Forschungsdatenzentrum Gesundheit
FHIR	Fast Healthcare Interoperability Resources
HL7 CDA	HL7 Clinical Document Architecture – XML-basierter Datenstandard
IDP	Identity Provider
IHE	Integrating the Healthcare Enterprise
JSON	JavaScript Object Notation
KAS	Klinisches Arbeitsplatzsystem

KBV	Kassenärztliche Bundesvereinigung
KIS	Krankenhausinformationssystem
KT	Kartenterminal
KVNR	Krankenversicherungsnummer
LEI	Leistungserbringerinstitution
MHD	Mobile access to Health Documents (FHIR-Service im Aktensystem u.a. für Volltextsuche)
MIO	Medizinisches Informationsobjekt
MTOM	Message Transmission Optimization Mechanism
NFD	Notfalldatensatz
OAuth2	Open Authorization 2.0
OIDC	OpenID Connect
OH KIS	Orientierungshilfe KIS (Datenschutzkonferenz)
OWASP	Open Web Application Security Project
PDMS	Patientendatenmanagementsystem
PKCE	Proof Key for Code Exchange
PKV	Private Krankenversicherung
PS	Primärsystem
PTSB	Produkttypsteckbrief
PZN	Pharmazentralnummer
REST	Representational State Transfer
SGB V	Sozialgesetzbuch – Fünftes Buch
SMC-B	Security Module Card– Typ B
SOAP	Simple Object Access Protocol
TI	Telematikinfrastruktur
TLS	Transport Layer security
Versicherten-ID	10-stelliger unveränderlicher Teil der 30-stelligen Krankenversicherungsnummer

VAU	Vertrauenswürdige Ausführungsumgebung
WSDL	Web Services Description Language
XDS	Cross-Enterprise Document Sharing
XML	Extensible Markup Language
XOP	XML-binary Optimized Packaging

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

Abbildung 1: Überblick ePA für alle....13

Abbildung 2: Schematisches Prozessmodell zur ePA für Arztpraxen, Zahnarztpraxen und psychotherapeutische Praxen....17

Abbildung 3: Schematisches Prozessmodell zur ePA für Apotheken.....19
Abbildung 4: Schematisches Prozessmodell zur ePA für Krankenhäuser - ambulant.....21
Abbildung 5: Schematisches Prozessmodell zur ePA für Krankenhäuser - zentrale Notaufnahme.....21
Abbildung 6: Schematisches Prozessmodell zur ePA für Krankenhäuser - stationär.....21
Abbildung 7: Schematisches Prozessmodell zur ePA für die Pflege.....26
Abbildung 8: Schematisches Prozessmodell zur ePA bei Heilmittelerbringern.....27
Abbildung 9: Überblick über Aufbau VAU, User Session und Aktensession.....34
Abbildung 10: Überblick über Nutzerauthentifizierung.....35
Abbildung 11: Detaillierter Nachrichten-Flow für die Nutzerauthentifizierung mit dem IDP-Dienst.....36
Abbildung 12: ILF_ePA_Element_Context.....47
Abbildung 13: Ablauf Erstellung einer Befugnis mittels PoPP.....49
Abbildung 14: Ablauf Erstellung einer Befugnis mittels VSDM.....51
Abbildung 15: Beispiel für die Auswahl einer Dokumentenklasse aus einer reduzierten Auswahlliste.....79
Abbildung 16: Beispiel für die Auswahl eines Dokumententyps aus einer reduzierten Auswahlliste (auf Basis der ausgewählten Dokumentenklasse).....79
Abbildung 17: Abb_ILF_ePA_eAB-XML-Containerformat.....87
Abbildung 18: Ablauf eines betreiberübergreifenden Aktenumzugs.....95
Abbildung 19: Voraussetzung für eine Befugniserzeugung.....109
Abbildung 20: Anzeige der ePA-Dokumentenübersicht als separate Ansicht aus einer Karteikarte heraus.....117
Abbildung 21: Anzeige von ePA-Dokumenten als Teil einer integrierten Dokumentenübersicht in der lokalen Dokumentenverwaltung.....117
Abbildung 22: Funktion im Primärsystem, um zu suchen, filtern und sortieren von Dokumenten in einem ePA-Aktenkonto.....121
Abbildung 23: Funktion im Primärsystem, um zu suchen, filtern und sortieren von Dokumenten in einem ePA-Aktenkonto.....122
Abbildung 24: Anzeige eines Kontextmenüs für ein ausgewähltes Dokument, um dieses zu bearbeiten (am rechten Bildrand ist der Menüpunkt zu finden).....125
Abbildung 25: Eingabemaske mit der vorausgefüllten Einstellung, dass ein Dokument (am unteren Bildrand ist der Menüpunkt zu finden).....127
Abbildung 26: Option zum Hochladen eines Dokuments im Falle des Versands eines eArztbriefs im Rahmen des KIM-Workflows ist standardmäßig ausgewählt.....129
Abbildung 27: Support- und Kommunikationsabläufe bei Nutzung der ePA.....138

8.4 Tabellenverzeichnis

Tabelle 1: TabILF_Kurzübersicht_PS-CS-Typen.....28

Tabelle 2: I_Authorization_Service::getNonce....36
Tabelle 3: I_Authorization_Service::send_Authorization_Request_SC....38
Tabelle 4: I_Authorization_Service::sendAuthCode....40
Tabelle 5: I_Information_Service::getRecordStatus....41
Tabelle 6: I_Information_Service::getRecordStatusV2....41
Tabelle 7: TAB_ILF_Zertifikate....43
Tabelle 8 : Parameter der TI-Zertifikate....44
Tabelle 9: I_Entitlement_Management::setEntitlementPs....49
Tabelle 10: I_Information_Service::getConsentDecisionInformation....54
Tabelle 11: Tab_ILF_ePA_Profilierung....55
Tabelle 12: Tab_ILF_ePA_Fehlerbehandlung_Dokumente_Suchen....67
Tabelle 13: Tab_ILF_ePA_Namensräume....74
Tabelle 14: Tab_ILF_ePA_Metadaten-Zuweisung....76
Tabelle 15: Tab_ILF_ePA_Metadaten-Vorbelegung....80
Tabelle 16: XML-Struktur für Arztbrief im DischargeLetterContainer-Format....87
Tabelle 17 : Metadatenvorgaben für Arztbriefe und Krankenhausentlassbriefe....88
Tabelle 18 : Zusätzlicher Code für nicht finale Dokumente....88
Tabelle 19: Tab_ILF_ePA_Datenfelder_Selbstauskunft....90
Tabelle 20: Tab_ILF_ePA_KTR_Metadatenkennzeichnungen....93
Tabelle 21: I_Health_Record_Relocation_Service::startPackageCreation....95
Tabelle 22: I_Health_Record_Relocation_Service::startPackageImport....96
Tabelle 23: I_Entitlement_Management::setBlockedUserPolicyAssignment....98
Tabelle 24: I_Entitlement_Management::deleteBlockedUserPolicyAssignment....98
Tabelle 25: I_Entitlement_Management::getBlockedUserPolicyAssignment....99
Tabelle 26: I_Consent_Decision_Management::getConsentDecision....99
Tabelle 27: Widersprüche im Rahmen des Medikationsprozesses....100
Tabelle 28: I_Consent_Decision_Management::updateConsentDecision....100
Tabelle 29: Widerspruch Sekundärdatennutzung durch das FDZ....101
Tabelle 30: I_Consent_Decision_Management::updateConsentDecision....101
Tabelle 31: Sekundärnutzungszwecke....101
Tabelle 32: I_Consent_Decision_Management::updateDataUsagePurposes....102
Tabelle 33: I_Consent_Decision_Management::getDataUsagePurposes....103
Tabelle 34: Schnittstellen IG_Audit_Event_Service....103
Tabelle 35 : I_Information_Service::setUserExperienceResult....105
Tabelle 36: Tab_UX_KPI_Messung_ePA_PS....105
Tabelle 37: Dokumentenübersicht anzeigen - UX Optimaler Klickpfad....116
Tabelle 38: Dokumente suchen, filtern und sortieren - UX Optimaler Klickpfad....119

Tabelle 39: Dokumente herunterladen, aktualisieren oder löschen - UX Optimaler Klickpfad.....123
Tabelle 40: Dokument hochladen aus Karteikarte - UX Optimaler Klickpfad.....126
Tabelle 41: Dokument hochladen aus KIM-Workflow - UX Optimaler Klickpfad.....128
Tabelle 42: Tab_ILF_ePA- Beispiele für REST-Fehlermeldungen.....130
Tabelle 43: Tab_ILF_ePA_IHE_Success_and_Error_Reporting.....132
Tabelle 44: Tab_ILF_ePA_IHE-Fehlermeldungen_Aktensystem.....134

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.

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur
[gemKPT_FK_ePAfueralle]	gematik: Fachkonzept elektronische Patientenakte für alle
[gem_KPT_GK_ePAfueralle]	gematik: Grobkonzept "ePA für Alle" https://github.com/gematik/ePA-Basic/blob/ePA-3.1.3/concept/concept.adoc
[gem_KPT_GK_XDS]	Grobkonzept "ePA für Alle": XDS Document Service https://github.com/gematik/ePA-XDS-Document/blob/ePA-3.1.3/concept/concept.adoc
[gemSpec_Aktensystem_ePAfueralle]	gematik: Spezifikation gemSpec_Aktensystem_ePAfueralle
[gemSpec_Krypt]	gematik: Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[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

[ePA_XDS_Document]	gematik: GitHub Repository "ePA-xds-document" https://github.com/gematik/ePA-XDS-Document/
[gemSpec_IG_ePA]	gematik: Implementation Guides für strukturierte Dokumente siehe [ePA_XDS_Document] Path: src/implementation_guides
[gemIG_ePA_Laboratory]	gematik: "ePA Laboratory Report Implementation Guide" https://gemspec.gematik.de/ig/fhir/epa-laboratory/1.0.0/index.html
[ePA_Basic]	gematik: GitHub Repository "ePA-Basic" https://github.com/gematik/ePA-Basic
[I_Information_Service]	gematik: I_Information_Service REST-Schnittstelle zum Abruf Informationen zu einem Aktenkonto siehe [ePA_Basic] Path: src/openapi/I_Information_Service.yaml
[I_Ehr_Information_Service]	gematik: I_Ehr_Information_Service REST-Schnittstelle zum Abruf Informationen zu einem Aktenkonto siehe [ePA_Basic] Path: src/openapi/I_Ehr_Information_Service.yaml
[I_Authorization_Service]	gematik: I_Authorization_Service REST-Schnittstelle zur Nutzerauthentifizierung siehe [ePA_Basic] Path: src/openapi/I_Authorization_Service.yaml
[I_Entitlement_Management]	gematik: I_Entitlement_Management REST-Schnittstelle zur Verwaltung von Befugnissen und Befugnisausschlüssen siehe [ePA_Basic] Path: src/openapi/I_Entitlement_Management.yaml
[I_Health_Record_Relocation_Service]	gematik: I_Health_Record_Relocation_Service REST-Schnittstelle zum Aktenumzug siehe [ePA_Basic] Path: src/openapi/I_Health_Record_Relocation_Service.yaml
[I_Consent_Decision_Management]	gematik: I_Consent_Decision_Management REST-Schnittstelle zum Management der Widersprüche zu Versorgungsprozessen siehe [ePA_Basic] Path: src/openapi/I_Consent_Decision_Management.yaml
[I_Email_Management]	gematik: I_Email_Management REST-Schnittstelle zum Management von email-Adressen eines Versicherten siehe [ePA_Basic] Path: src/openapi/I_Email_Management.yaml

[gemIG_ePA_Basic]	gematik: FHIR Implementation Guide "ePA Basisfunktionalitäten" https://gematik.de/fhir/epa/ImplementationGuide/de.gematik.epa
[gemIG_ePA_Medication]	gematik: FHIR Implementation Guide "ePA Medication Service" https://gematik.de/fhir/epa-medication/ImplementationGuide/de.gematik.epa.medication
[gemIG_ePA_MHD]	gematik: FHIR Implementation Guide "ePA MHD Service" https://gematik.de/fhir/epa-mhd/ImplementationGuide/de.gematik.epa.mhd
[gemIG_TI_Terminology]	gematik: Implementation Guide "TITerminology" https://gemspec.gematik.de/ig/fhir/terminology/
[KBV_eAU]	KBV: Technische Anlage zur eAU https://update.kbv.de/ita-update/DigitaleMuster/eAU/KBV_ITA_VGEX_Technische_Anlage_eAU.pdf
[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

8.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[BasicProfile 1.2]	Basic Profile Version 1.2 http://www.ws-i.org/Profiles/BasicProfile-1.2-2010-11-09.html
[BasicProfile 2.0]	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-TF2]	IHE International (2025): IHE IT Infrastructure (ITI) Technical Framework, Volume 2 (ITI TF-2) – Transaction definitions and constraints, Revision 20.2, https://profiles.ihe.net/ITI/TF/Volume2/
[IHE-ITI-TF3]	IHE International (2025): IHE IT Infrastructure (ITI) Technical Framework, Volume 3 (ITI TF-3) – Cross-Document Sharing Metadata and Content Profiles, Revision 20.2, https://profiles.ihe.net/ITI/TF/Volume3/

[KBV Portal]	Portal der Kassenärztliche Bundesvereinigung https://kbv.de
[KDL-ILF]	DVMD: KDL Implementierungsleitfaden https://simplifier.net/guide/kdl-implementierungsleitfaden-2025?version=2025 und https://simplifier.net/guide/kdl-implementierungsleitfaden-2025/Hauptseite/ConceptMap-2024/MappingvonKDLnachIHETypeCode-2024?version=2025 und https://simplifier.net/guide/kdl-implementierungsleitfaden-2025/Hauptseite/ConceptMap-2024/MappingvonKDLnachIHEClassCode-2024?version=2025
[MTOM]	W3C (2005): SOAP Message Transmission Optimization Mechanism, https://www.w3.org/TR/soap12-mtom/
[Richtlinie eArztbrief]	Kassenärztliche Bundesvereinigung (2024): Richtlinie über die Übermittlung elektronischer Briefe in der vertragsärztlichen Versorgung gemäß § 383 SGB V, Richtlinie Elektronischer Brief https://www.kbv.de/documents/infothek/rechtsquellen/weitere-vertraege/praxen/telemedizin/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
[RFC 7518]	https://datatracker.ietf.org/doc/html/rfc7518
[BSI-TR-03111]	https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03111/BSI-TR-03111_V-2-1_pdf.pdf?__blob=publicationFile&v=1

4223