

**Elektronische Gesundheitskarte und Telematikinfrastruktur**

# **Implementierungsleitfaden Primärsysteme - Elektronische Patientenakte (ePA)**

Version:	1.8.0
Revision:	370293
Stand:	02.06.2021
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemILF_PS_ePA

---

## Dokumentinformationen

---

### 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
1.0.0	18.12.18		initiale Erstellung des Dokuments	gematik
1.1.0	15.05.19		Einarbeitung P 18.1	gematik
1.2.0	28.06.19		Einarbeitung P 19.1	gematik
1.3.0	02.10.19		Einarbeitung P 20.1/2	gematik
1.4.0	02.03.20		Einarbeitung P 21.1	gematik
1.5.0	30.06.20		Anpassungen gemäß Änderungsliste P22.1 und Scope-Themen aus Systemdesign R4.0.0	gematik
1.6.0	12.10.20		Einarbeitung P22.2	gematik
1.7.0	19.02.21		Einarbeitung Änderungsliste P22.5	gematik
1.8.0	02.06.21		Einarbeitung ePA_Maintenance_21.1	gematik

---

## Inhaltsverzeichnis

---

<b>1 Einordnung des Dokumentes .....</b>	<b>6</b>
1.1 Zielsetzung .....	6
1.2 Zielgruppe .....	6
1.3 Geltungsbereich .....	6
1.4 Abgrenzungen .....	7
1.5 Methodik .....	7
<b>2 Systemüberblick .....</b>	<b>8</b>
2.1 Relevante Integrationsprofile.....	8
<b>3 Systemkontext.....</b>	<b>9</b>
3.1 Akteure und Rollen .....	9
3.2 Nachbarsysteme .....	9
<b>4 Übergreifende Festlegungen .....</b>	<b>11</b>
4.1 Webservice-Kommunikation .....	11
4.2 Dienstverzeichnisdienst.....	12
4.3 Ereignisdienst.....	12
4.4 Zugriffssteuerung .....	13
4.4.1 Aufrufkontext .....	13
4.4.2 RecordIdentifier .....	15
4.4.3 Status Aktenzugriff.....	16
<b>5 Funktionsmerkmale .....</b>	<b>19</b>
<b>5.1 ePA-Administration .....</b>	<b>21</b>
5.1.1 Aktenanbieter ermitteln .....	22
5.1.1.1 Schnittstelle .....	23
5.1.1.2 Umsetzung .....	24
5.1.1.3 Nutzung .....	25
5.1.2 Aktenkonto aktivieren.....	26
5.1.2.1 Schnittstelle .....	27
5.1.2.2 Umsetzung .....	28
5.1.2.3 Nutzung .....	28
5.1.3 Ad-hoc-Berechtigung erteilen .....	29
5.1.3.1 Schnittstelle .....	31
5.1.3.2 Umsetzung .....	33
5.1.3.3 Nutzung .....	35
<b>5.2 Dokumentenmanagement .....</b>	<b>36</b>
5.2.1 Dokumente einstellen .....	39
5.2.1.1 Schnittstelle .....	40
5.2.1.2 Umsetzung .....	42
5.2.1.3 Nutzung .....	49

5.2.2 Dokumente suchen .....	51
5.2.2.1 Schnittstelle .....	53
5.2.2.2 Umsetzung .....	55
5.2.2.3 Nutzung .....	55
5.2.3 Dokumente laden .....	60
5.2.3.1 Schnittstelle .....	61
5.2.3.2 Umsetzung .....	61
5.2.3.3 Nutzung .....	63
5.2.4 Dokumente löschen .....	64
5.2.4.1 Schnittstelle .....	65
5.2.4.2 Umsetzung .....	65
5.2.4.3 Nutzung .....	66
5.2.5 Artefakte .....	66
5.2.5.1 Namensräume .....	66
5.2.5.2 WSDLs und Schemata .....	67
5.2.6 Testunterstützung .....	67
<b>5.3 Protokolle und Benachrichtigungen .....</b>	<b>67</b>
5.3.1 Benachrichtigungen erhalten .....	67
5.3.1.1 Info-Quelle ePA-Administration .....	69
5.3.1.2 Info-Quelle Berechtigungs-Abfrage .....	70
5.3.1.3 Info-Quelle Dokumentensuche .....	71
5.3.1.4 Info-Quelle Systeminformationsdienst .....	72
5.3.1.5 Info-Quelle Fehlermeldung .....	72
5.3.1.6 Umsetzung .....	73
5.3.1.7 Nutzung .....	74
5.3.2 Übertragungsprotokolle speichern .....	75
<b>5.4 Status- und Fehlermeldungen .....</b>	<b>75</b>
5.4.1 Statusinformationen .....	75
5.4.2 Fehlerbehandlung .....	77
5.4.2.1 TelematikError .....	77
5.4.2.2 IHE-Error .....	78
5.4.3 Handlungs-Empfehlungen in Fehlerfällen .....	78
5.4.4 Übersicht möglicher Fehlermeldungen .....	80
5.4.4.1 Fehlermeldungen aus dem Fachmodul ePA .....	80
5.4.4.2 Fehlermeldungen aus dem Aktensystem ePA .....	82
<b>6 Informationsmodell .....</b>	<b>85</b>
<b>6.1 Metadaten .....</b>	<b>85</b>
<b>6.2 Wertebereiche .....</b>	<b>85</b>
<b>6.3 Dokumentenformate der ePA .....</b>	<b>87</b>
6.3.1 ContentProfile Notfalldatensatz und Datensatz Persönliche Erklärungen .....	88
6.3.2 ContentProfile elektronischer Medikationsplan .....	91
6.3.3 ContentProfile Arztbrief nach § 291f .....	92
6.3.4 Strukturierte Dokumente .....	95
6.3.4.1 Signatur für strukturierte Dokumentenformate der ePA .....	96
<b>7 Ergänzende Funktionalitäten .....</b>	<b>99</b>
<b>7.1 Empfehlung zur Archivierung .....</b>	<b>99</b>
<b>8 Anhang A – Verzeichnisse .....</b>	<b>100</b>

<b>8.1 Abkürzungen .....</b>	<b>100</b>
<b>8.2 Glossar .....</b>	<b>100</b>
<b>8.3 Abbildungsverzeichnis.....</b>	<b>100</b>
<b>8.4 Tabellenverzeichnis .....</b>	<b>101</b>
<b>8.5 Referenzierte Dokumente .....</b>	<b>102</b>
8.5.1 Dokumente der gematik.....	102
8.5.2 Weitere Dokumente.....	103

---

## **1 Einordnung des Dokumentes**

---

### **1.1 Zielsetzung**

Die vorliegende Spezifikation definiert Anforderungen zu Erstellung, Test und Betrieb derjenigen Anteile eines Primärsystems, die zur Nutzung der elektronischen Patientenakte erforderlich sind. Die gematik erstellt auch in Hinsicht auf die ePA eine Bestätigung über die Konformität des Primärsystems zur Konnektorschnittstelle aus. Bei Umsetzung der Anforderungen dieses Dokumentes erfüllt der PS-Hersteller die Anforderungen des Bestätigungsverfahrens.

Die Anforderungen des Dokumentes sind für Primärsystemhersteller, die keine Bestätigung auf Konformität der Konnektorschnittstelle durch die gematik benötigen informativ.

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 aus der Sicht der PS-Hersteller erläutert. Dabei werden nicht nur Anwendungsfälle der ePA erläutert, sondern auch praktische Umsetzungshinweise sowie Beispiele gegeben.

### **1.2 Zielgruppe**

Das Dokument ist maßgeblich für Hersteller von Primärsystemen, welche die Fachmodul-ePA-Schnittstelle des Konnektors nutzen.

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

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

### **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. Dokumentenlandkarte, Produkttypsteckbrief, Leistungsbeschreibung) fest-gelegt 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\_DM\_ePA] beschrieben sind;
- Rendering-Vorschriften zur Form, in der ePA-Dokumente zur Anzeige gebracht werden (ggf. wird auf externe Festlegungen referenziert).

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

## **1.5 Methodik**

Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID sowie die dem RFC 2119 [RFC2119] entsprechenden, in Großbuchstaben geschriebenen deutschen Schlüsselworte 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.

---

## 2 Systemüberblick

---

Einem Leistungserbringer als Nutzer seines Primärsystems bietet ein ePA-fähiger Konnektor den Zugang zur elektronischen Patientenakte des gesetzlich Versicherten an. Leistungserbringer und Primärsystem greifen in der ConsumerZone der TI primär auf die lokalen bzw. dezentralen TI-Komponenten der LE-Institution zu. Zugriffe auf elektronische Patientenakten erfolgen ausschließlich gekapselt über den Konnektor.

Zu diesem Zweck nutzt das Primärsystem IHE-Schnittstellen, die das Fachmodul ePA des Konnektors bereitstellt.

Eine Übersicht über die Fachanwendung ePA im Ganzen liefert [gemSysL\_ePA]. Einen Überblick über die ePA-Profilierung des Frameworks von IHE (Integrating the Healthcare Enterprise) liefert [gemSpec\_Dokumentenverwaltung].

Wenn von der "Akte" 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.

### 2.1 Relevante Integrationsprofile

Für das aktennutzende PS sind mehrere IHE-Integrationsprofile für das Primärsystem relevant:

**Tabelle 1: Tab\_ILF\_ePA\_IHE-TransaktionenProfile**

Kürzel	Dokument	Transaktion
[ITI-41]	[ITI TF-2b#3.41]	Provide and Register Document Set-b
[ITI-18]	[ITI TF-2a#3.18]	Registry Stored Query
[ITI-43]	[ITI TF-2b#3.43]	Retrieve Document Set
[ITI-62]	[IHE-ITI-RMD]	Remove Metadata



---

## **3 Systemkontext**

---

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 Berechtigungsvergabe 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 mit dem Fachmodul ePA, welches die Kommunikation mit dem ePA-Aktensystem ermöglicht. Mit dem Konnektor stehen auch die Komponenten der Basis-TI, die zentrale TI und der Fach- und Basisdienste der TI zur Verfügung, deren Nutzung durch das PS in [gemILF\_PS], [gemILF\_PS\_NFDM] und [gemILF\_PS\_AMTS] beschrieben sind.

### **3.1 Akteure und Rollen**

Leistungserbringer agieren in zwei ePA-Szenarien:

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

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

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

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

### **3.2 Nachbarsysteme**

Leistungserbringer erhalten über ihr ePA-fähiges Primärsystem Zugriff auf die ePA des Versicherten ausschließlich über den Konnektor. Der Konnektor macht zusätzlich die zentralen und dezentralen Komponenten der TI für das PS zugänglich, für Details siehe die Übersicht in [gemKPT\_Arch\_TIP]. Weitere Nachbarsysteme oder an das PS angebundene Softwaremodule werden in diesem Dokument nicht betrachtet.

Das vorliegende Dokument bezieht sich mit den referenzierten Konnektorschnittstellen auf den Leistungsumfang der ePA-Komponenten, die in der dazugehörigen Dokumentenlandkarte aufgelistet sind. Die hier beschriebene Funktionalität wird als ePA Stufe 2 (und höher) beschrieben, um zu kennzeichnen, dass die vorliegenden Primärsystemschnittstellen der ePA einige nur beschränkt abwärtskompatible

Änderungen zur ePA-Stufe 1 enthält. Das betrifft insbesondere die Erteilung von Berechtigungen. In ePA 1 erstellte Berechtigungen werden vom Aktensystem in Berechtigungen für ePA 2 transformiert. ePA 2 - Berechtigungen können jedoch nicht in ePA 1 - Berechtigungen zurück transformiert werden. Das Upgrade von ePA 1 auf ePA 2 kann nicht rückgängig gemacht werden. In einer früheren Version des vorliegenden Dokumentes ist die Nutzung der ePA Stufe 1 beschrieben, zuletzt für das Release 3.1.3.

Das Upgrade des Primärsystems auf Stufe 2 ist abhängig von der Verfügbarkeit des ePA 2 - Konnektorfachmoduls im Konnektor des Leistungserbringers. Falls der PS-Hersteller die Verfügbarkeit des Konnektor PTV5 (mit der ePA 2 - Funktionalität) bei den Leistungserbringern nicht durchgängig sicher stellen kann, kann es für das Ausrollen des ePA 2 - Primärsystems erforderlich sein, die Schnittstellenversion des Konnektors über den Dienstverzeichnisdienst zu ermitteln und die Inbetriebnahme des ePA 2 - Upgrades vom Vorliegen der passenden Schnittstellenversion im Dienstverzeichnisdienst abhängig zu machen (PHRService V2.x und PHRServiceManagement V2.x sind erreichbar). Dieses Feature ("Dualmode" des Primärsystems) unterstützt die Migration von ePA 1 nach ePA2 und darf nicht dazu verwendet werden zwischen den Interfaces von ePA 1 und ePA 2 beliebig zu wechseln. Dies würde dazu führen, dass bei manchen PS-Installation ePA 1 genutzt wird, bei anderen ePA 2, je nach Version des Konnektors in der konkreten LE-Institution. Dieser "Dualmode" erlaubt PS-Herstellern ein einheitliches Release-Management für unterschiedliche Praxiskonstellationen im Migrationszeitraum der ePA Stufe 1 auf die ePA Stufe 2.

---

## **4 Übergreifende Festlegungen**

---

Das Primärsystem verarbeitet die primäre Behandlungsdokumentation der Versicherten. Die ePA ist ein potentiell lebenslanger Speicherort für eine sekundäre Behandlungsdokumentation der Versicherten.

Die Anbindung und Nutzung dezentraler TI-Komponenten, die in [gemILF\_PS] beschrieben wird, ermöglicht unter anderem den Aufbau von Kartensitzungen, die an verschiedenen Stellen vorausgesetzt werden, insbesondere zur Nutzung der eGK des Versicherten.

Das Fachmodul ePA wird vom Konnektor ab Produkttyp Version 4 (PTV4) zur Verfügung gestellt.

Die Inbetriebnahme des Konnektors in die LE-Umgebung [gemILF\_PS#4.1] und die Unterstützung des VSDM durch das PS für eine Gültigkeitsprüfung der eGK [gemILF\_PS#4.3] MUSS erfolgt sein, um die ePA nutzen zu können.

Für die Anwendungsfälle der ePA MUSS eine SM-B in PS und Konnektor verwaltet werden und freigeschaltet sein [gemILF\_PS#4.2.3]. Das PIN-Handling von eGK und SM-B wird in [gemILF\_PS#4.1.5] beschrieben.

Das PS muss eine Arbeitsplatz-Konfiguration in der LE-Institution ermöglichen, in der Versicherte auf ein Kartenterminal zugreifen können, in dem sie ihre eGK freischalten können. Dazu gehört ein KT, dessen PIN-Pad dem Versicherten zur Eingabe seiner PIN.CH zugänglich ist. Die Konfiguration eines Arbeitsplatzes, an dem ein Kartenterminal für den Versicherten zur PIN-Eingabe zugänglich ist, insbesondere am Empfangstresen, wird in [gemILF\_PS#9.1] beschrieben.

### **4.1 Webservice-Kommunikation**

Die Webservice-Konnektorschnittstellen werden nachrichtenbasiert angesprochen über

- SOAP1.1 mit [BasicProfile1.2] für Webservices der Konnektor-Basisdienste und anderer Fachmodule und
- SOAP1.2 mit [BasicProfile2.0] für Webservices des Fachmoduls ePA.

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 Aufruf- und Aktenkontext zu erhalten (s. Kap. 4.4).

#### **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\_14511 - Leere oder fehlende SOAP-Header im Falle fehlender Parametern**

Das PS KANN einen leeren SOAP-Header an den Konnektor senden oder eine Nachricht ohne SOAP-Header versenden, wenn keine SOAP-Header-Parameter 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 - 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. Beispiel einer korrekten Angabe im http-Header: Content-Type: text/xml; charset=utf-8. [≤]

## **4.2 Dienstverzeichnisdienst**

**A\_15573 - Nutzung DVD zur Ermittlung der Webservice-Endpunkte der ePA am Konnektor**

Das PS MUSS ausschließlich den Dienstverzeichnisdienst des Konnektors nutzen, um die Webservice-Endpunkte für die ePA-Dienste des Fachmoduls zu ermitteln. Die URL des Webservice-Endpunktes, die aus WSDL-Abfragen wie GET `/ws/CertificateService?wsdl` ermittelt werden kann, ist nicht zu verwenden. [≤]

Das PS soll auch mit Konnektoren kompatibel sein, die eine Produkttypversion kleiner als PTV4 nutzen. Der PS-Hersteller kann es erreichen, dass sein Primärsystem mit Konnektoren unterschiedlicher Produkttypversion zusammen arbeitet, um darauf vorbereitet zu sein, dass seine Kunden Konnektoren älterer Produkttypversionen (kleiner PTV4) nutzen, indem er die Versionsinformationen des Dienstverzeichnisdienstes beachtet:

- Der Dienstverzeichnisdienst stellt dem PS die Information zur Verfügung, ob der Konnektor ePA-Dienste anbietet. Wenn kein ePA-Webservice angeboten wird, SOLL das PS die ePA-Funktionsmerkmale an der Nutzeroberfläche nicht zur Verfügung stellen.
- Der Dienstverzeichnisdienst stellt ihm die Information, in welcher Version der Konnektor seine Webservices anbietet, als eine dreistellige Versionsnummer mit Hauptversionsnummer (1. Stelle), Nebenversionsnummer (2. Stelle) und einer Revisionsnummer (3. Stelle) zur Verfügung.

Es kann vorkommen, dass PS und Konnektor vom selben Webservice unterschiedliche Dienstversionsnummern unterstützen. Der Umgang mit Abweichungen zwischen produktiven PS und Konnektor in Bezug auf unterstützte Dienstversionen wird in [gemILF\_PS#4.1.2] beschrieben.

## **4.3 Ereignisdienst**

Falls das PS den Eventservice des Konnektors abonniert, kann es Komfortfunktionen der Kartenverwaltung wie Benachrichtigungen über gesteckte und gezogene Karten und Informationen über den Betriebszustand des Konnektors nutzen.

**A\_15577 - Abonnierung von Ereignissen**

Das PS SOLL Benachrichtigung über Konnektor-Ereignisse gemäß [gemILF\_PS#4.1.4] Eventservice abonnieren, insbesondere FM\_EPA/POLICY\_LEI (Kap. 5.4.1) und FM\_EPA/ACTIVATE\_ACCOUNT/START (Kap. 5.1.2).[<=]

## **4.4 Zugriffssteuerung**

Der ePA-Client übergibt je nach Signatur der Operation eines ePA-Webservices Informationen über

1. sich selbst (bzw. den Arbeitsplatz, von dem aus der Clientaufruf erfolgt) in den Context-Parametern (im SOAP-Header oder im SOAP-Request) sowie
2. Identifikatoren zur Akte des Versicherten.

Viele Funktionsmerkmale erfordern die Kenntnis des Status der Zugriffsberechtigung auf die ePA eines Versicherten, um

- nicht auf unnötige Fehler zu laufen (insbesondere bei Operationen des Dokumentenmanagements) und
- Aufrufe vollständig umsetzen zu können.

### **A\_14413 - Primärdokumentation als Voraussetzung der ePA als Sekundärdokumentation**

Das PS MUSS für einen Versicherten Daten in seiner Primärdokumentation verwalten, falls er für ihn Funktionsmerkmale des ePA-Dokumentenmanagements zur Sekundärdokumentation nutzen will, und dort folgende Informationen hinterlegen können: RecordIdentifier inklusive Versicherten-ID (Die Versicherten-ID ist der 10-stellige unveränderliche Teil der 30-stelligen Krankenversicherungsnummer), Status Zugriffsberechtigung.[<=]

#### **4.4.1 Aufrufkontext**

Das Bilden des Aufrufkontextes erfolgt wie schon im PTV1-Konnektor. Die nur für den HBA verwendete User-ID muss im Rahmen der ePA nicht gesetzt werden, da der Zugriff auf die ePA mittels HBA in den Stufen 1 und 1.1 nicht möglich ist.

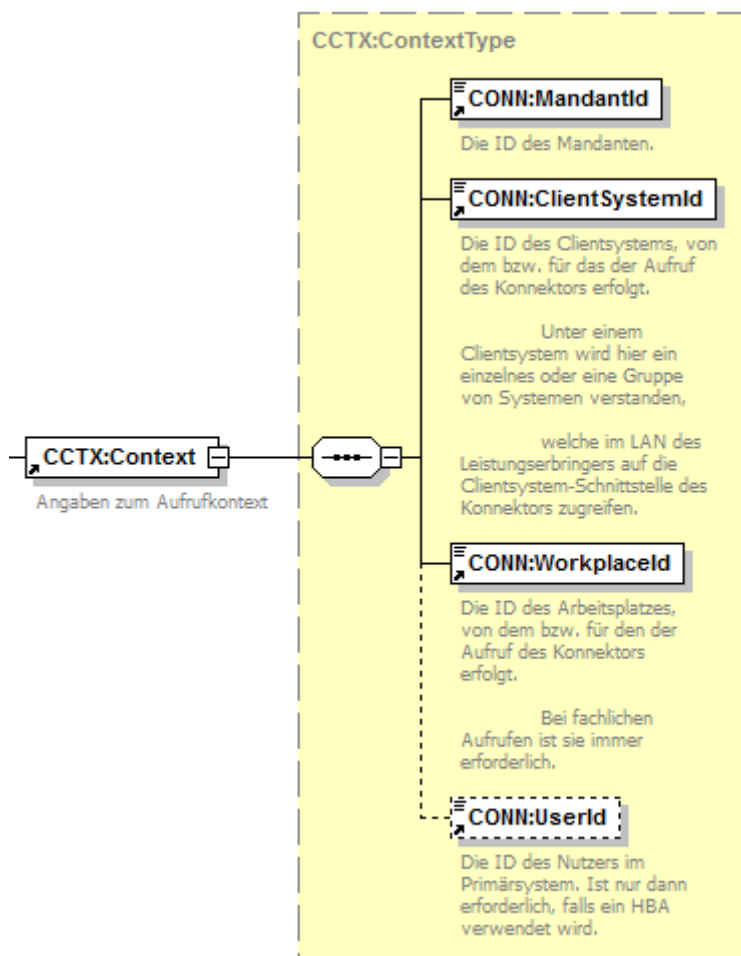


Abbildung 1: ILF\_ePA\_Element\_Context

Der Konnektor ermittelt unter Verwendung von Konfigurationsdaten am Konnektor und der Context-Informationen die zur Laufzeit verfügbaren SM-Bs, die für den Aktenzugriff vom Konnektor herangezogen werden können. Voraussetzung für die Nutzung vieler Funktionsmerkmale ist daher das Vorliegen mindestens einer freigeschalteten SM-B.

#### 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>
```

#### A\_14442 - Freischaltung von SM-Bs garantieren

Das PS MUSS mindestens einmal täglich den Sicherheitszustand aller SM-Bs prüfen, die in der LE-Institution verfügbar sind. Im Falle nicht freigeschalteter SM-Bs MUSS das PS den Nutzer auffordern, die Freischaltung der SM-Bs durchzuführen. [ < = ]

Die Liste der gesteckten SM-Bs liefert der Systeminformationsdienst (siehe [gemILF\_PS#4.1.4]). Der erhöhte Sicherheitszustand bzw. die Freischaltung einer SM-B ist mittels `GetPinStatus` am Rückgabewert `verified` erkennbar (siehe [gemILF\_PS#4.1.5.4]).

Eine Eins-zu-Eins-Beziehung zwischen MandantID und TelematikID wird von der gematik nicht anwendungsübergreifend festgeschrieben. Für die Anwendung ePA ist die 1:1-Beziehung zwischen MandantID und TelematikID jedoch fachlich erforderlich.

Das PS kann die 1:1-Beziehung zwischen MandantID und TelematikID technisch verifizieren, indem es (Schritt 1) potentiell mehrere SMC-B-Cardhandles der für die ePA im Kontext verwendeten MandantID ermittelt, (Schritt 2) für jede dieser CardHandle per `ReadCardCertificate` aus der SMC-B das C.HCI.AUT – Zertifikat ausliest, die Telematik-ID extrahiert und (Schritt 3) eine Fehlermeldung anzeigt, falls die ermittelten TelematikIDs pro MandantID nicht identisch sind.

## 4.4.2 RecordIdentifier

Für die ePA eines Versicherten werden identifizierende Merkmale in unterschiedlicher Form verwendet:

**Tabelle 2: Tab\_ILF\_ePA\_Identifizier\_für\_Versicherte\_und\_Akten**

Datentyp	Bestandteile	Format	Beschreibung
RecordIdentifier	InsurantId	Strukturierter Datentyp, s. Abb_ILF_ePA_RecordIdentifier mit der Versicherten-ID als @extension in Verbindung mit der OID für KVNRS als @root	Kennung des Versicherten, eindeutig über alle verfügbaren Aktensysteme (Verwendung im Kontext der ePA-Administration)
	HomeCommunityId	String, gebildet als OID mit 64 Zeichen nach [IHE-ITI-TF3#4.2.3.2.12] [gemSpec_DM_ePA#2.1.4.6]	Kennung des Aktenanbieters, eindeutig über alle verfügbaren Aktensysteme
patientID		String, gebildet aus Versicherten-ID und ihrer OID gemäß [gemSpec_DM_ePA#2.1.4.5]	Kennung des Versicherten, eindeutig über alle verfügbaren Aktensysteme (Verwendung im Kontext der Dokumentenverwaltung)

An den Konnektor-Schnittstellen werden jeweils entweder der `RecordIdentifier` oder seine Bestandteile verwendet.

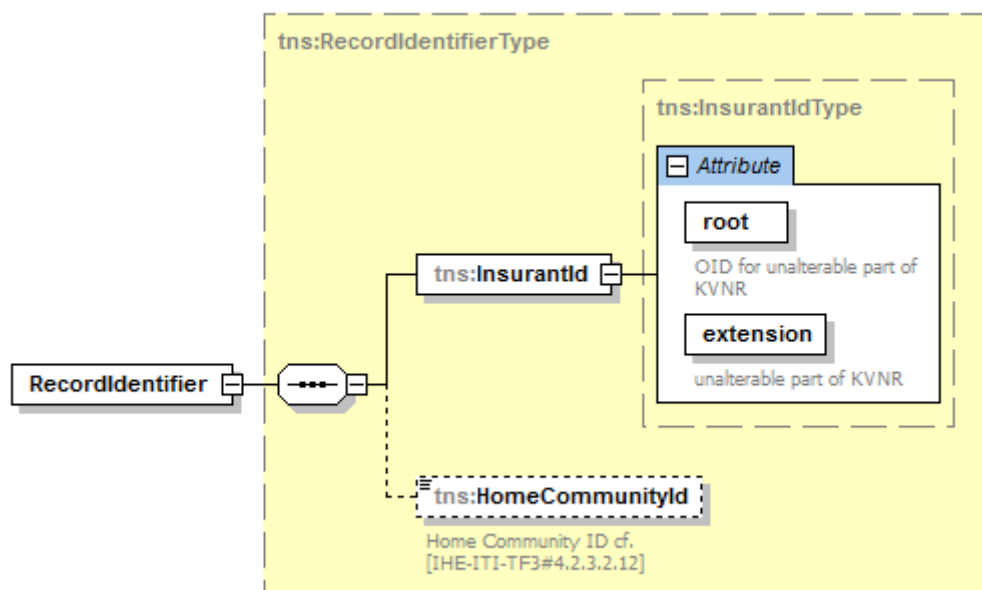


Abbildung 2: Abb\_ILF\_ePA\_RecordIdentifier

#### A\_15640 - Transformationen InsurantId und patientId

Das PS MUSS in der Lage sein, aus der Versicherten-ID gemäß [gemSpec\_DM\_ePA#2.1.4.5] eine InsurantId und eine patientId zu erzeugen, sowie die inhaltsgleichen InsurantId und patientId wechselseitig ineinander zu transformieren. [ $\leq$ ]

### 4.4.3 Status Aktenzugriff

Die LEI wird vom Primärsystem darin unterstützt, die Metadaten für die Aktenzugriffe mit möglichst wenig Pflegeaufwand zu befüllen, und zwar insbesondere durch die

- Persistierung von Statusinformationen der Zugriffsberechtigung einer LEI auf Akten;
- Verwendung von Default-Einstellungen
- Selbstauskunftsangaben und reduzierte Wertebereichsvorschlagslisten aus [gemSpec\_DM\_ePA] gemäß Kap. 6.2

Der lokal hinterlegbare Status des Aktenzugriffs umfasst für einzelne Versicherte in Tab\_ILF\_ePA\_Zugriffsberechtigungsstatus pro RecordIdentifier aufgeführte Informationen. Kap. 5.4.1 (Benachrichtigungen verwalten) beschreibt, wie sich diese Informationen akkumulieren und aktualisieren lassen.

Tabelle 3: Tab\_ILF\_ePA\_Zugriffsberechtigungsstatus pro RecordIdentifier

Information pro RecordIdentifier	Wert	Quellen für Aktualisierungen
----------------------------------	------	------------------------------



Kennung des Versicherten (Versicherten-ID)	RecordIdentifier/InsurantId/@extension	<ul style="list-style-type: none"> <li>Primärdokumentation des Versicherten</li> <li>Anwendungsfall VSD von eGK lesen, [gemILF_PS#4.3.3]</li> </ul>
Kennung des Aktenanbieters	HomeCommunityId	Anwendungsfall <i>Aktenanbieter ermitteln</i>
Vorliegen der Berechtigung, auf seine Akte zuzugreifen; Ablaufdatum Zugriffsberechtigung	ExpirationDate: Datum, an dem die Zugriffsberechtigung abläuft	Anwendungsfälle: <ul style="list-style-type: none"> <li><i>Ad-hoc-Berechtigung erteilen</i></li> <li><i>Benachrichtigung verwalten</i></li> </ul>
Dokumentenliste	<ul style="list-style-type: none"> <li>ObjektIdentifier (insbesondere XSDSDocumentEntry_uniqueId)</li> <li>Downloadstatus (Dokument oder Metadaten)</li> <li>Aktualisierungsdatum</li> </ul>	Anwendungsfälle Kapitel 5.2.6, 5.3.1
Zugriffsberechtigung (Typ der Dokumente im Zugriff)	Einer der Werte der Tabelle Tab_ILF_ePA_Zugriffsberechtigungen	Anwendungsfälle Kapitel 5.1.3

Die LEI erhält Zugriff auf ePA-Dokumente je nach erteilter Kombination von Zugriffsberechtigungen. Folgende einander ergänzende Zugriffsberechtigungen sind in der ePA möglich:

**Tabelle 4: Tab\_ILF\_ePA\_Zugriffsberechtigungen**

Technischer Identifier Zugriffsberechtigung	Anmerkung
DocumentCategory: Liste von Identifiern für Dokumentenkategorien gemäß [gemSpec_DM_ePA#Tab_DM_Dokumentenkategorien]	LEI erhält Zugriffsrecht auf alle aufgelisteten Dokumentenkategorien, soweit es der Festlegung in der AuthorizationConfidentiality, sowie den Zugriffsunterbindungsregeln aus A_19303 nicht widerspricht.

AuthorizationConfidentiality="N"	LEI erhält "Einfaches Zugriffsrecht", auf: Dokumente vom Typ ConfidentialityCode <code>normal</code> , falls es nicht den Zugriffsunterbindungsregeln aus A_19303 nicht widerspricht.
AuthorizationConfidentiality="R"	LEI erhält "Erweitertes Zugriffsrecht", auf: Dokumente vom Typ ConfidentialityCode <code>normal</code> und <code>restricted</code> , falls es nicht den Zugriffsunterbindungsregeln aus A_19303 nicht widerspricht. Die umfasst auch durch ihn selbst später in der Vertraulichkeitsstufe <code>restricted</code> ("vertraulich") eingestellte Dokumente.

---

## **5 Funktionsmerkmale**

---

Das Aktenkonto eines Versicherten kann sowohl beim LE, als auch am ePA-Frontend des Versicherten aktiviert werden (Kap. 5.2.1).

Das PS nutzt die Berechtigungsverwaltung des ePA-Aktensystems über seine Schnittstellen zum Fachmodul ePA.

Leistungserbringerinstitutionen haben zwei Möglichkeiten, vom Versicherten eine Berechtigung zum Aktenzugriff zu erhalten:

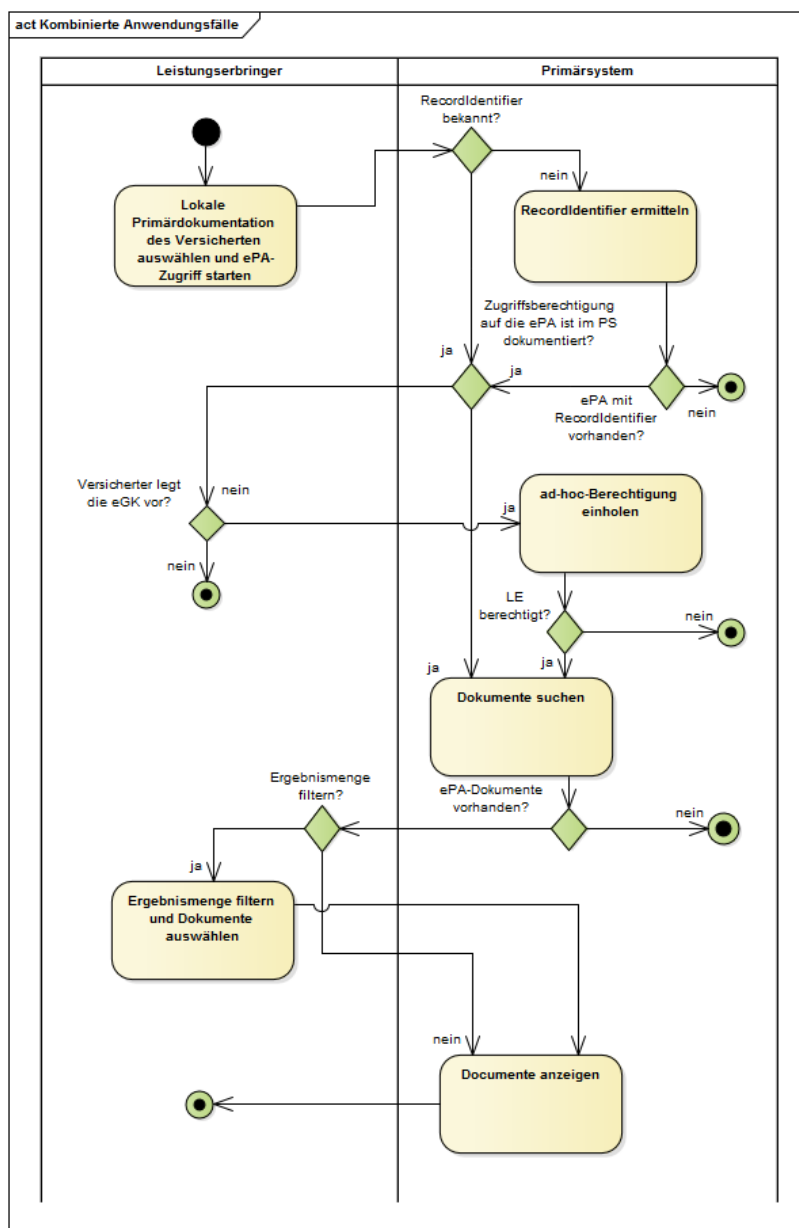
1. Der Versicherte erteilt eine Berechtigung für die LE-Institution am ePA-Frontend des Versicherten
2. In der LE-Institution erteilt der Versicherte eine Ad-hoc-Berechtigung (Kap. 5.1.4)

Die Berechtigung kann sowohl vom Versicherten selbst stammen, als auch vom Vertreter des Versicherten. Sie ist auf Leistungserbringer (inkl. deren berufsmäßigen Gehilfen oder zur Vorbereitung auf den Beruf Tätige, jedoch nicht die Gehilfen der nichtärztlichen Psychotherapeuten) eingeschränkt, s. [gemSpec\_PKI#Tab\_PKI\_254 Zugriffsprofile für eine Rollenauthentisierung] und [gemKPT\_Arch\_TIP#Tabelle Zugriffsberechtigter Personenkreis (PK) nach §291a SGB V].

Die Laufzeit von Zugriffsberechtigungen ist begrenzt. Falls eine Zugriffsberechtigung aufgrund in der Vergangenheit liegendem `expirationDate` oder Berechtigungsentzug am ePA-Frontend des Versicherten nicht mehr existiert, ist eine erneute Berechtigungsvergabe erforderlich, s. [gemSysL\_ePA#2.5.2].

Im Falle vorliegender Berechtigung kann das PS den `RecordIdentifier` des Versicherten ermitteln (Kap. 5.1.5).

Für ein bereits aktiviertes Aktenkonto kann sich eine Kombination der Anwendungsfälle bis hin zu einem lesenden Aktenzugriff beispielhaft folgendermaßen darstellen:



**Abbildung 3:**  
**Abb\_ILF\_ePA\_Kombinierte\_Anwendungsfälle\_für\_bereits\_aktiviertes\_Aktenkonto**

In technische Abläufe wird der Versicherte oder sein Vertreter über die PIN-Eingabe integriert.

**Tabelle 5: Tab\_ILF\_ePA\_Funktionsmerkmale\_Beteiligung\_Versicherter**

<b>Obligatorische Beteiligung des Versicherten oder seines Vertreters (eGK-Nutzung erforderlich)</b>	<b>Fakultative Beteiligung des Versicherten oder seines Vertreters (keine eGK-Nutzung)</b>
--	--

<i>Aktenkonto aktivieren</i> (Kap. 5.1.2) (Nur durch den Versicherten, nicht durch den Vertreter)	<i>Aktenanbieter</i> der Versicherten <i>ermitteln</i> (Kap. 5.1.1)
<i>Ad-hoc-Berechtigung erteilen</i> (Kap. 5.1.3)	Management von Dokumenten: <ul style="list-style-type: none"> <li>• <i>einstellen</i> (Kap. 5.2.1)</li> <li>• <i>suchen</i> (Kap. 5.2.2)</li> <li>• <i>laden/anzeigen</i> (Kap. 5.2.3)</li> <li>• <i>löschen</i> (Kap. 5.2.5)</li> </ul>
	<i>Benachrichtigungen über Änderungen innerhalb einer Akte erhalten</i> (Kap. 5.3.1)

Der Vertreter hat seine Vertretungsberechtigung am ePA-Frontend des Versicherten erhalten, wo auch die eGK des Vertreters der ePA des Vertretenen bekannt gemacht wurde. Im Gegensatz dazu benutzt der gesetzlich bevollmächtigte Vertreter die eGK desjenigen, den er vertritt.

Falls ein Vertreter das Aktenkonto aktivieren möchte, kann er dies nur dann tun, falls er ein gesetzlich bevollmächtigter Vertreter ist, der über eGK und PIN des Versicherten verfügt, den er vertritt. Für das Aktivieren des Aktenkontos kann der Vertreter seine eigene eGK nicht verwenden, anders als beim Erteilen der Ad-hoc-Berechtigung

Für die Durchführung der Aktenkonto-Aktivierung oder der Erteilung der Ad-hoc-Berechtigung durch einen gesetzlich bevollmächtigten Vertreter ist keine darüber hinaus gehende zusätzliche Implementierung am PS erforderlich.

Das komplette Berechtigungskonzept inklusive der Berechtigungsverwaltung am ePA-Frontend des Versicherten liefert [gemSysL\_ePA#3.6].

### **A\_15090 - Protokollierung Dokumententransfer im Übertragungsprotokoll**

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

## **5.1 ePA-Administration**

Das Aktenmanagement der Leistungserbringer (PHRManagementService) erfolgt weitgehend über das Fachmodul ePA und dort gekapselte Funktionalitäten.

**Tabelle 6: Tab\_ILF\_ePA\_PHRManagementService**

<b>Name</b>	<b>PHRManagementService [gemSpec_FM_ePA#7.2]</b>
<b>Version</b>	2.0
<b>Namensraum</b>	http://ws.gematik.de/conn/WSDL/PHRManagementService/v2.0
<b>Abkürzung Namensraum</b>	phr_management

Operationen	Name	Implementierungshinweise
	GetHomeCommunityID	[gemSpec_FM_ePA#7.2.1.4]
	ActivateAccount	[gemSpec_FM_ePA#7.2.1.1]
	RequestFacilityAuthorization	[gemSpec_FM_ePA#7.2.1.2]
<b>WSDL</b>	PHRManagementService.wsdl	
<b>XML-Schema</b>	PHRManagementService.xsd	

In `ActivateAccount` und `RequestFacilityAuthorization` werden eGK und SM-B im freigeschaltetem Zustand verwendet, in `GetHomeCommunityID` nur die SM-B.

### 5.1.1 Aktenanbieter ermitteln

*Frau Gundlach ist Patientin bei Herrn Dr. Weber und teilt ihm bei einem vergangenen Arzttermin mit, dass sie seit kurzem ein Aktenkonto bei einem ePA - Provider eingerichtet hat. Dr. Weber ermittelt daraufhin dessen Identifier über eine Funktion seines Primärsystems, und speichert den Identifier des Aktenanbieters von Frau Gundlach daraufhin persistent in der Primärdokumentation des Primärsystems ab.*

Zur Ermittlung der `HomeCommunityID` des Versicherten wird die Operation `GetHomeCommunityID` des `PHRManagementService` genutzt.

Für die Nutzung der ePA durch das Primärsystem ist das Vorliegen eines Identifikators für das Aktenkonto des Versicherten (`RecordIdentifier`) erforderlich.

Fachliche Grundlage der Aktenzuordnung ist die Versicherten-ID des Versicherten. Jeder Versicherte hat zur selben Zeit nur ein einzelnes Aktenkonto. Unterschiedliche Versicherte können bei jeweils unterschiedlichen Aktenanbietern ihre Patientenakte hosten lassen. Die Abfrage der verschiedenen möglichen Anbieter übernimmt das Fachmodul für das PS. Die `HomeCommunityId` kann pro Versicherten über das Fachmodul ePA ermittelt werden.

Jeder Versicherte verfügt über genau eine aktive Akte, auch während er ggf. den Aktenanbieter wechselt.

Wenn die Aktenzuordnung für einen Vertreter durchgeführt wird, muss der Vertreter der LEI hinreichend genau mitteilen, für welchen Versicherten er vertretungsberechtigt ist, damit für den Vertretenen der Aktenanbieter ermittelt werden kann. Aufgrund der vom Vertreter mitgeteilten Patientenidentifikationsmerkmale ermittelt die LEI die betroffene Primärakte und ermittelt den Aktenanbieter aus dieser Primärakte heraus. Durch das Starten des Anwendungsfalles aus dem Aktenkonto desjenigen heraus, der vertreten wird, wird dessen `KVNR` als `InsurantID` verwendet. Die Ermittlung desjenigen, der vertreten wird, kann nicht über die eGK des Vertreters erfolgen und muss vielmehr im Dialog mit dem Vertreter durchgeführt werden.

### A\_15581 - Anwendungsfall Aktenanbieter ermitteln

Das PS MUSS es dem Leistungserbringer ermöglichen, für einen Versicherten, über dessen Versicherten-ID er in der Primärdokumentation seines PS verfügt, mittels `GetHomeCommunityID` die `HomeCommunityId` des Aktenanbieters zu ermitteln. [ $\leq$ ]

Das Resultat von *Aktenanbieter ermitteln*, die `HomeCommunityId`, wird als Teil des `RecordIdentifiers` verwendet, sowie separat als Wert bestimmter Metadatenfelder. Aufgrund der vielfachen Verwendung ist eine persistente Speicherung in der Primärdokumentation des Versicherten erforderlich.

### 5.1.1.1 Schnittstelle

#### **A\_15582 - Identifikation des Versicherten mittels Versicherten-ID**

Das PS MUSS die Versicherten-ID benutzen, um den Versicherten in seiner Primärdokumentation seiner ePA durch Bildung eines `RecordIdentifiers` zuzuordnen. [ $\leq$ ]

**Tabelle 7: Tab\_ILF\_ePA\_Operation\_getHomeCommunityID**

Operationsname	GetHomeCommunityID [gemSpec_FM_ePA#7.2.1.1]	
Aufrufparameter	Name	Implementierung
	Context	Aufrufkontext gemäß [ConnectorContext.xsd], s. [gemILF_PS#3.3.1]
	InsurantID	InsurantIdType, s. Kap. 4.4.2
Rückgabeparameter	Name	Implementierung
	Status	Status nach [gemSpec_Kon#3.5.2] zur Information im PS
	HomeCommunityId	Anbieterkennung gemäß [gemSpec_DM_ePA#2.1.4.7]

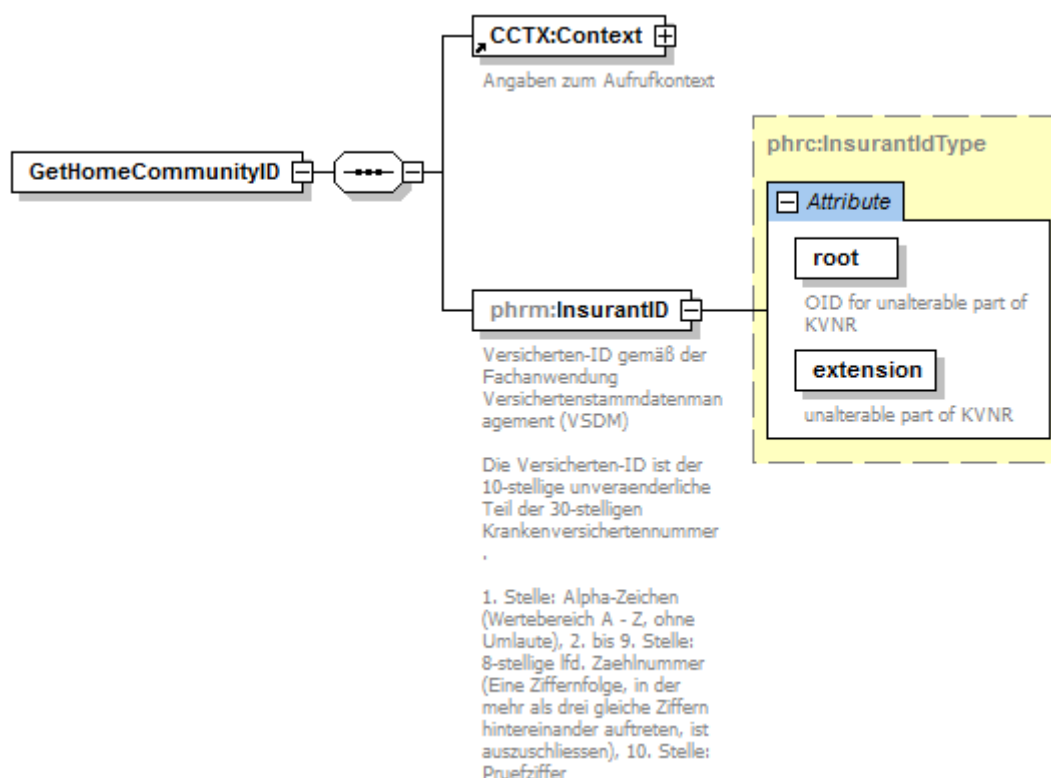


Abbildung 4: Abb\_ILF\_ePA\_getHomeCommunityRequest

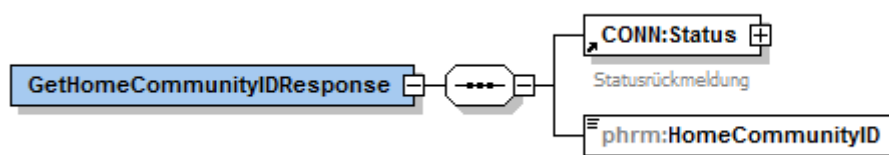


Abbildung 5: Abb\_ILF\_PS\_ePA\_getHomeCommunityResponse

### 5.1.1.2 Umsetzung

Die Aktivitäten des Anwendungsfalles *Aktenanbieter ermitteln* sind:

#### Vorbedingung:

- Dem Versicherten ist aktuell nach Auslesen der eGK oder bei einem vorangegangenen Arztbesuch eine Versicherten-ID im Primärsystem zugeordnet worden.
- Der Aufruf erfolgt aus der Primärdokumentation des Versicherten heraus

#### Auslöser:

- Die für einen Zugriff auf die Akte des Versicherten oder Verwaltung der Zugriffsberechtigung erforderliche `HomeCommunityId` liegt nicht vor.



- Bisher im PS bekannte `HomeCommunityId` hat sich als falsch herausgestellt, insbesondere aufgrund eines Anbieterwechsels des Versicherten.

**Aktivitäten:**

- Ermitteln der Versicherten-ID aus der Primärdokumentation des Versicherten

**Resultat:**

- Im Erfolgsfalle der Operation erhält der Nutzer eine `HomeCommunityId`, als Voraussetzung der Nutzung der ePA eines Versicherten.
- Die `HomeCommunityId` wird in der Primärdokumentation des Versicherten abgespeichert gemäß [A 14660](#).

### 5.1.1.3 Nutzung

Das erfolgreiche Ermitteln einer `HomeCommunityId` ist kein Beleg für das Vorliegen einer Zugriffsberechtigung auf die Akte des Versicherten. Daher ist die Nutzung der Operation `GetHomeCommunityID` vor allem im Kontext der Ad-hoc-Berechtigung sinnvoll, oder nach einer Kenntnisnahme davon, dass Leistungserbringer eine Berechtigung über das ePA-Frontend des Versicherten erhalten haben.

**Beispiel 2: Bsp\_ILF\_ePA\_Request\_getHomeCommunityID**

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope
xmlns:m1="http://ws.gematik.de/conn/ConnectorCommon/v5.0"
xmlns:m0="http://ws.gematik.de/conn/ConnectorContext/v2.0"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:SOAP-
ENC="http://www.w3.org/2003/05/soap-encoding" xmlns:SOAP-
ENV="http://www.w3.org/2003/05/soap-envelope">
<SOAP-ENV:Header>
<Action SOAP-ENV:mustunderstand="true"
xmlns="http://www.w3.org/2005/08/addressing">http://ws.gematik.de/co
nn/phrs/PHRManagementService/v1.3/GetHomeCommunityID</Action>
<To SOAP-ENV:mustunderstand="1"
xmlns="http://www.w3.org/2005/08/addressing">http://10.11.218.161:80
/fm/phrmanagementservice</To>
<MessageID SOAP-ENV:mustunderstand="true"
xmlns="http://www.w3.org/2005/08/addressing">5d3f0445-1c9c-4c0f-
a246-57816bc99cab</MessageID>
<ReplyTo SOAP-ENV:mustunderstand="1"
xmlns="http://www.w3.org/2005/08/addressing">
<Address>http://www.w3.org/2005/08/addressing/anonymous</Address
>
</ReplyTo>
</SOAP-ENV:Header>
<SOAP-ENV:Body>
<m:GetHomeCommunityID
xmlns:m="http://ws.gematik.de/conn/phrs/PHRManagementService/v1.3">
<m0:Context>
<m1:MandantId>Mandant1</m1:MandantId>
<m1:ClientSystemId>ClientID1</m1:ClientSystemId>
```

```
<m1:WorkplaceId>CATS</m1:WorkplaceId>
</m0:Context>
<m:InsurantID extension="X110411319" root="1.2.276.0.76.4.8"/>
</m:GetHomeCommunityID>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Wenn das Primärsystem durch eine VSDM-Prüfung von einem Wechsel der Haupt-IK-Nummer an den Daten des Versicherten informiert wird, soll im Falle einer bestehenden Zugriffsberechtigung auf eine Akte der Operation `GetHomeCommunityID` aufgerufen werden, da ein Wechsel des Aktenanbieters nicht unwahrscheinlich ist.

#### **A\_14660 - Eingeschränkte Speicherung der HomeCommunityId**

Das PS SOLL die `HomeCommunityId` nur im Falle festgestellter Zugriffsberechtigungen in die Primärdokumentation des Versicherten speichern:

- im Erfolgsfalle von *Ad-hoc-Berechtigung erteilen* ([A\\_14517](#))
- bei neu ermittelten Zugriffsberechtigungen im Rahmen der Benachrichtigungsverwaltung ([A\\_14659](#))
- im Rahmen des Dokumentenmanagements, falls die `HomeCommunityId` noch nicht in der Primärdokumentation gespeichert vorliegt.

[<=]

### **5.1.2 Aktenkonto aktivieren**

*Frau Gundlach hat bei einem Aktenanbieter einen Vertrag über die Nutzung einer elektronischen Patientenakte abgeschlossen. Sie bittet Dr. Weber darum, für sie das Aktenkonto zu aktivieren. Dr. Weber ermittelt den Aktenanbieter von Frau Gundlach durch Aufruf einer entsprechenden Funktion im PVS und aktiviert dort für Sie ihre Akte. Dabei gibt Frau Weber die PIN ihrer eGK ein.*

Zur Umsetzung des "Schritt 2 - Aktivierung in der Umgebung des Leistungserbringers" im Anwendungsfall *Aktenkonto einrichten* aus [gemSysL\_ePA#3.5.1, UC 2.1 - Aktenkonto einrichten, Schritt 2 - Aktivierung in der Umgebung des Leistungserbringers] wird die Operation `ActivateAccount` des `PHRManagementService` genutzt.

#### **A\_14191 - Anwendungsfall Aktivierung Aktenkonto des Versicherten**

Das PS MUSS es dem Leistungserbringer ermöglichen, mittels `ActivateAccount` das Aktenkonto des Versicherten zu aktivieren. [ $\leq$ ]

Das Aktivieren des Aktenkontos wird entweder vom PS-Nutzer über das Userinterface aktiv gestartet oder es wird implizit aus anderen Anwendungsfällen heraus gestartet, in denen das Fachmodul am Status der Akte erkennt, dass die Akte eines Versicherten noch zu aktivieren ist. Das implizite Starten des Anwendungsfalles führt ebenso wie das vom PS angestoßene Starten des Aktenkonto-Aktivierens zu einer Interaktion des Versicherten mit dem Kartenterminal, worüber das PS durch das Event `FM_EPA/ACTIVATE_ACCOUNT/START` informiert wird.

### 5.1.2.1 Schnittstelle

Durch seine PIN bestätigt der Versicherte seine Einwilligung dazu, das Aktenkonto in der in den Vertragsunterlagen ausgewählten Konfiguration zu aktivieren.

**Tabelle 8: Tab\_ILF\_ePA\_Operation\_ActivateAccount**

Operationsname	ActivateAccount [gemSpec_FM_ePA#7.2.1.1]	
Aufrufparameter	Name	Implementierung
	Context	Aufrufkontext gemäß [ConnectorContext.xsd], s. [gemILF_PS#3.3.1]
	EhcHandle	Aufbau einer Kartensitzung gemäß [gemILF_PS#4.2] ergibt <code>CardHandle</code> der eGK des Versicherten
	RecordIdentifizier	RecordIdentifizier gemäß [gemSpec_DM_ePA#3.1.2], s. Kapitel 5.1.1
Rückgabeparameter	Name	Implementierung
	Status	Status nach [gemSpec_Kon#3.5.2] zur Information im PS

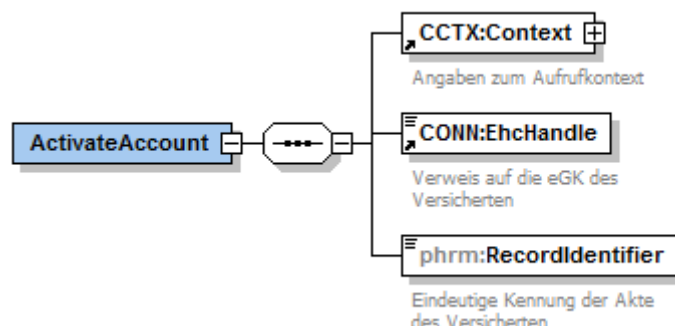


Abbildung 6: Abb\_ILF\_ePA\_Eingabeparameter\_ActivateAccount

### 5.1.2.2 Umsetzung

Die Aktivitäten des Anwendungsfalles *Aktenkonto aktivieren* sind:

#### Vorbedingung:

- Der Versicherte hat in einem ersten vorgelagerten Initialisierungsschritt ein Aktenkonto bei einem Aktenanbieter eingerichtet.
- Durch ein vorgelagertes `GetHomeCommunityID` wurde die `HomeCommunityId` ermittelt.

#### Auslöser:

- Der Versicherte informiert den LE über eine noch zu aktivierende Akte oder, alternativ, wird der Anwendungsfall durch das Event `FM_EPA/ACTIVATE_ACCOUNT/START` gestartet.
- In einem der Anwendungsfälle des PHRService ist der Fehler 7403 aufgetreten, der auf ein nicht aktiviertes Aktenkonto hinweist

#### Aktivitäten:

- Ermitteln des CardHandles zur eGK des Versicherten
- Abfrage `getPinStatus`, ob PIN.CH gesperrt ist
- Aufruf der Konnektorschnittstelle `activateAccount`
- Der Versicherte soll darüber informiert werden, dass er am Kartenterminal seine PIN eingeben muss;
- Der Versicherte autorisiert den LE zur Aktivierung der Akte mit seiner PIN-Eingabe
- Auswertung des Ergebnisses

#### Resultat:

- Das Aktenkonto des Versicherten ist aktiviert

### 5.1.2.3 Nutzung

#### A\_17204 - Informieren aufgrund Event `FM_EPA/ACTIVATE_ACCOUNT/START`

Das PS MUSS bei Erhalt der Events `FM_EPA/ACTIVATE_ACCOUNT/START` eine Information an den Nutzer des PS weiterleiten, dass der Versicherte aktuell mit dem Anwendungsfall beschäftigt ist, das Aktenkonto zu aktivieren. [ $\leq$ ]

Der Versicherte kann so vom Nutzer des PS darauf aufmerksam gemacht werden, dass der Versicherte am Kartenterminal dazu aufgefordert wird, seine PIN einzugeben.

Der Anwendungsfall startet mit der Information des Versicherten, die Aktenaktivierung bereits vorbereitet zu haben, mit einem expliziten Auslösen über das Userinterface des Primärsystems.

Das implizite Aktivieren startet die Aktenkontoaktivierung beispielsweise beim Erteilen einer Ad-hoc-Berechtigung, sofern das Aktenkonto sich in dem Zustand befindet, die ausstehende Aktivierung durchführen zu können. Dabei wird das Event `FM_EPA/ACTIVATE_ACCOUNT/START` ausgelöst.

Wenn die Aktivierung des Aktenkontos erfolgreich beendet wurde und sich das Aktenkonto des Versicherten im aktivierten Zustand befindet, löst das ePA-Fachmodul das Event `FM_EPA/ACTIVATE_ACCOUNT/FINISHED` aus, das für eine Erfolgsmeldung am Primärsystem genutzt werden kann, um den Versicherten über den Erfolg des Anwendungsfalles zu unterrichten.

### **5.1.3 Ad-hoc-Berechtigung erteilen**

*Frau Gundlach möchte Herrn Dr. Weber und seiner Hausarztpraxis Zugriff auf ihre ePA erteilen. Im Gespräch mit der . Medizinischen Fachangestellte (MFA) von Dr. Weber am Empfangstresen, Frau Kunze, wird besprochen, dass der Zugriff auf alle normalen von Leistungserbringern eingestellte Dokumente erfolgen soll, nicht aber auf die vertraulichen Dokumente von Frau Gundlach. Sie überreicht ihre eGK Frau Kunze. Frau Kunze wählt die besprochene Option am PS. Frau Kunze fordert die Ad-hoc-Berechtigung am PS an und dreht das Kartenterminal mit dem Eingabefeld für die PIN-Eingabe zu Frau Weber. Auf dem Display des Kartenterminals sieht Frau Weber die Aufforderung zur PIN-Eingabe für die Ad-hoc-Berechtigung mit den abgesprochenen Optionen, sowie Dauer der Gültigkeit der Zugriffsberechtigung für die Arztpraxis Dr. Weber. Das PS am Empfangstresen fügt der lokalen Primärdokumentation von Frau Gundlach ein ePA-Kennzeichen als Markierung einer bestehenden Zugriffsberechtigung hinzu.*

Zur Umsetzung des Anwendungsfalles *Ad-hoc-Berechtigung durch einen Leistungserbringer anfordern* aus [gemSysL\_ePA#3.6.7, UC 3.7 - Ad-hoc-Berechtigung durch einen Leistungserbringer anfordern] wird die `Operation RequestFacilityAuthorization` des `PHRManagementService` verwendet.

#### **A\_14200-05 - Anwendungsfall Ad-hoc-Berechtigung erteilen**

Das PS MUSS es Leistungserbringern ermöglichen, mittels `RequestFacilityAuthorization` vom Versicherten oder seinem Vertreter eine Ad-hoc-Zugriffsberechtigung auf seine Akte erteilen zu lassen. Dabei wird die Art des gewährten Zugriffs in der `AuthorizationConfiguration` angegeben, sowie die Dauer der Zugriffsberechtigung im `ExpirationDate` (heute+6 Tage als Defaultwert). Die `AuthorizationConfiguration` enthält die vom Versicherten getroffene Festlegung zu folgenden Auswahlmöglichkeiten (`AuthorizationConfidentiality`): a) Vertraulichkeitsstufe `normal` oder `vertraulich (restricted)`, b) die Auflistung der Dokumentenkategorien `DocumentCategory` gemäß [gemSpec\_DM#Tab\_DM\_Dokumentenkategorien], auf die eine Berechtigung erteilt wird. [ $\leq$ ]

Die Vertraulichkeitsstufe vertraulich (`restricted`) betrifft Dokumente, die der Versicherte an seinem FdV als vertraulich gekennzeichnet hat, sowie Dokumente, die von Leistungserbringern auf Wunsch des Versicherten als vertraulich eingestellt wurden. Falls eine Freigabe auf Dokumente der Vertraulichkeitsstufe `restricted` erfolgt, ist damit eine Freigabe auf Dokumente der Vertraulichkeitsstufe `normal` verbunden.

#### **A\_19408 - Auswahlmöglichkeit `AuthorizationConfiguration.DocumentCategory`**

Das PS MUSS ihren Nutzern geeignete Auswahlmöglichkeiten bieten, um die Optionen der `AuthorizationConfiguration.DocumentCategory` auszuwählen, insbesondere die Kombination der mit dem Versicherten besprochenen Dokumentenkategorien gemäß `[gemSpec_DM#Tab_DM_Dokumentenkategorien]`, für die eine Freigabe erfolgt. Das Primärsystem MUSS dem Leistungserbringer je nach dem Sektor, in dem er arbeitet, einen konfigurierbaren Defaultwert anbieten, der die Summe aller Kategorien umfasst, die ihm die Zugriffsunterbindungsregeln erlauben. Die Summe der für den Sektor des Primärsystems möglichen Zugriffsrechte ist aus der Tabelle `[gemSpec_Dokumentenverwaltung#Tab_Dokv_030 - Zugriffsunterbindungsregeln]` abzuleiten.

[<=]

#### **A\_19497 - Auswahlmöglichkeit**

##### **`AuthorizationConfiguration.AuthorizationConfidentiality`**

Das PS MUSS dem LE eine Auswahl an Optionen anzubieten, die dem Wunsch des Versicherten entsprechen, eine Zugriffsberechtigung `AuthorizationConfiguration` aus der Tabelle `Tab_ILF_ePA_Zugriffsberechtigungen` zu erteilen. Eine leere Auswahl ist nicht zulässig. Erfolgt keine anders lautende Auswahl, MUSS das PS für `AuthorizationConfiguration.AuthorizationConfidentiality` den Default-Wert `normal` setzen. Das PS MUSS die ausgewählte Kombination aus Zugriffsberechtigungen im Element `AuthorizationConfiguration` setzen. [<=]

#### **A\_19498 - Speicherung `RecordIdentifier` in der lokalen Primärdokumentation des PS**

Das PS MUSS den `RecordIdentifier` an der lokalen Patientenakte (Primärdokumentation) persistent speichern, falls die Ad-hoc-Autorisierung erfolgreich verlaufen ist. Zusätzlich MUSS die `RequestFacilityAuthorization.AuthorizationConfiguration` gespeichert werden, um für denselben Versicherten bei der nächsten Adhoc-Autorisierung dem Versicherten die Option anbieten zu können, dieselben Optionen wie beim letzten Mal zu setzen. [<=]

Am Aktensystem werden Zugriffe auf Dokumente unterbunden, die nicht den gesetzlich festgelegten berufsgruppenspezifischen Regeln entsprechen. Manche Berufsgruppen verfügen nur über eingeschränkte Zugriffsrechte auf bestimmte Typen von Dokumenten. Die Auswahl von Dokumentenkategorien durch den Versicherten kann diese Zugriffsmöglichkeiten weiter einschränken, nicht jedoch über die gesetzlich festgelegten Rahmenbedingungen hinaus erweitern.

#### **A\_19386 - Respektieren der berufsgruppenspezifischen Zugriffsunterbindungsregeln**

Das PS MUSS die in `[gemSpec_Dokumentenverwaltung#Tab_Dokv - Zugriffsunterbindungsregeln]` aufgeführten Zugriffsunterbindungsregeln beachten, um nicht unnötige Fehlermeldungen zu provozieren. Das PS darf nur solche Dokumentenkategorien zur Auswahl bringen, die der Berufsgruppe der SMC-B entsprechen, die für die Ad-hoc-Berechtigung verwendet wird. [<=]

Über die Operation `ReadCardCertificate` kann das PS die Berufsgruppe derjenigen SMC-B ermitteln, die für die ePA-Zugriffe benutzt wird. Im Authentisierungszertifikat `C.AUT` befindet sich die Berufsgruppe `ProfessionOID` in der ZertifikatsExtension `Admission`, s. [gemSpec\_PKI#Anhang A].

Die Rolle des Versicherten kann teilweise auch vom Vertreter übernommen werden. In diesem Fall übergibt der Vertreter seine eigene eGK, um eine Ad-hoc-Berechtigung für den Versicherten zu erstellen, für den die Vertretung wahrgenommen wird (identifiziert durch dessen `RecordIdentifier`, aufgerufen aus der PS-Dokumentation des Vertretenen).

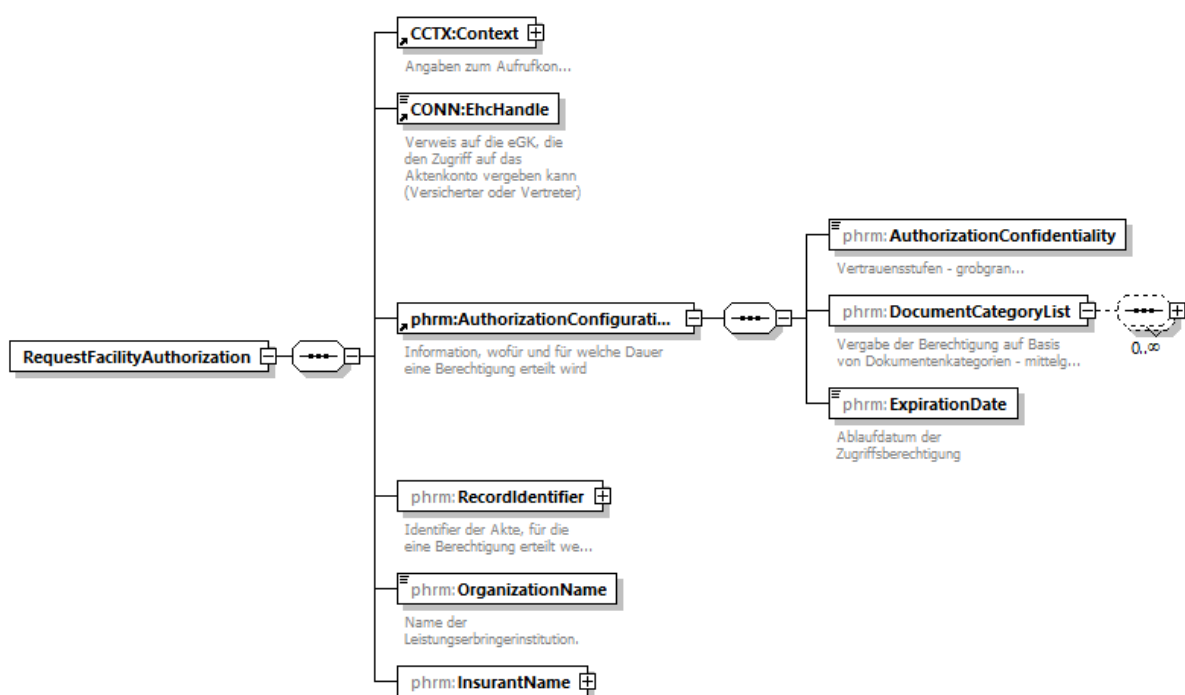
Durch das Starten des Anwendungsfalles aus dem Aktenkonto desjenigen heraus, der vertreten wird, wird dessen `RecordIdentifier` verwendet. Die Ermittlung desjenigen, der vertreten wird, kann nicht über die eGK des Vertreters erfolgen und muss vielmehr im Dialog mit dem Vertreter durchgeführt werden. Falls für den Vertreter die Vertretungsrechte nicht (mehr) vorliegen sollten, scheitert der Anwendungsfall Ad-hoc-Berechtigung durch den Vertreter erteilen. Dabei wird der Fehler 7209 (Keine Berechtigung für das Aktenkonto vorhanden) geworfen.

### 5.1.3.1 Schnittstelle

**Tabelle 9: Tab\_ILF\_ePA\_Operation\_RequestFacilityAuthorization**

Operationsname	RequestFacilityAuthorization [gemSpec_FM_ePA#7.2.1.1]	
Aufrufparameter	Name	Implementierung
	Context	Aufrufkontext gemäß [ConnectorContext.xsd], s. [gemILF_PS#3.3.1]
	EhcHandle	Aufbau einer Kartensitzung gemäß [gemILF_PS#4.2] ergibt <code>CardHandle</code> der eGK des Versicherten oder seines Vertreters
	AuthorizationConfiguration	Art und Gültigkeitsendedatum des Zugriffs, den der Versicherte auf seine Akte gewährt.
	RecordIdentifier	RecordIdentifier mit den Elementen <code>InsurantId</code> und <code>HomeCommunityID</code>
	OrganizationName	Name der LE-Organisation gemäß Selbstbeschreibung Kap. 6.2, Tab_ILF_ePA_Datenfelder_Selbstauskunft für die Anzeige am Kartenterminal
	InsurantName	Vor- und Nachname aus der Primärakte des Versicherten, für den eine

		Berechtigung erteilt wird, für die Anzeige am Kartenterminal.
Rückgabeparameter	Name	Implementierung
	Status	
		Status nach [gemSpec_Kon#3.5.2] zur Information im PS



Generated by XMLSpy

www.altova.com

Abbildung 7: Abb\_ILF\_ePA\_RequestFacilityAuthorization

Der Eingabeparameter AuthorizationConfiguration beschreibt

- Art des Zugriffs: die in Tab\_ILF\_ePA\_Zugriffsberechtigungen erläuterten Werte
- Zugriffsberechtigungs-Endedatum. ExpirationDate berechnet aus der Dauer des Zugriffs (1 Tag, 7 Tage, 18 Monate, flexibel, unbefristet) (Default: 7 Tage).

### A\_15633-06 - Setzen des Elementes ExpirationDate

Das PS MUSS dem LE eine Konfigurationsauswahl gemäß Tabelle Tab\_ILF\_ePA\_Zugriffsberechtigungs-Endedatum anbieten, in der ein Versicherter bestimmt, wie lange er dem LE eine Zugriffsberechtigung erteilt. Außerdem MUSS zusätzlich eine flexible Festlegung möglich sein. Erfolgt keine Festlegung, gilt der Default-Wert. Für die erteilte Berechtigung setzt das PS ein Zugriffsberechtigungs-Endedatum im Element ExpirationDate aufgrund der Berechnung des Datums des letzten Datums ab heute, zu dem die Zugriffsberechtigung noch besteht.



**Tabelle 10: Tab\_ILF\_ePA\_Zugriffsberechtigungs-Endedatum**

Werte zur Auswahl	Erläuterung der Berechnung des ExpirationDate	Default-Wert
1 Tag	ExpirationDate = heutiges Datum	
7 Tage	ExpirationDate = heutiges Datum + 6 Kalendertage	ja
18 Monate	ExpirationDate = heutiges Datum + 18 Kalendermonate	
flexibel	ExpirationDate = beliebiges Datum (heutiges Datum bis 100 Jahre)	
unbefristet	ExpirationDate = 31.12.9999	

**[<=]**

Der Versicherte oder ein von ihm berechtigter Vertreter stimmt der Berechtigung auf Aktenzugriff durch PIN-Eingabe am Kartenterminal, in dem die eGK (des Versicherten bzw. des Vertreters) steckt, zu.

### 5.1.3.2 Umsetzung

Das Primärsystem nutzt beim Erteilen einer Ad-hoc-Berechtigung die grobgranulare Festlegungen (*AuthorizationConfidentiality*) oder mittelgranulare Festlegungen (*DocumentCategoryList*). Feingranulare Berechtigungen, d.h. Zugriffsberechtigungen, die sich auf einzelne ausgewählte Dokumente beziehen, können am PS nicht gesetzt werden. Feingranulare Berechtigungen erteilen kann nur der Versicherte an seinem Frontend.

Falls schon eine Berechtigung vorliegt, wird diese durch die Operation überschrieben.

Die Aktivitäten des Anwendungsfalles *Ad-hoc-Berechtigung erteilen* sind:

#### **Vorbedingung:**

- Ermittelter *RecordIdentifier*

#### **Auslöser:**

- Ein ePA-Anwendungsfall soll ausgeführt werden,
- Leistungserbringer fragen beim Versicherten eine Autorisierung für einen Aktenzugriff an,
- Ein Versuch, einen ePA-Anwendungsfall auszuführen scheiterte mit Fehler 7209 (Keine Berechtigung für das Aktenkonto vorhanden). Vor einem erneuten Versuch, einen ePA-Anwendungsfall auszuführen wird nun erst noch eine Ad-hoc-Berechtigung eingeholt.

#### **Aktivitäten:**

- Ermitteln des *CardHandles* zur eGK des Versicherten

- Abfrage `getPinStatus`, ob `PIN.CH` gesperrt ist
- Auswahl am PS
  - der vom Versicherten intendierten (mündlich mitgeteilten) Art der Zugriffsberechtigung im Element `authorizationConfiguration`
  - des Zeitraumes, für die er dem LE Zugriff auf seine Akte gewährt (1 Tag, 7 Tage [default], 18 Monate, flexibel oder unbefristet);
- Aufruf der Konnektorschnittstelle unter Übergabe der Auswahl-Parameter
- Der Versicherte soll darüber informiert werden, dass er am Kartenterminal seine PIN zur Bestätigung der Auswahl eingeben muss;
- Die Erfolgsmeldung wird vom PS verarbeitet, indem der Zeitraum vermerkt wird, für den die Autorisierung vorliegt, sowie die `RecordIdentifier`

**Resultat:**

- Mit der vorliegenden Berechtigung ist die Voraussetzung für sämtliche Aktenzugriffe und Aktenadministrations-Anwendungsfälle gegeben
- Es liegt die `RecordIdentifier` vor, für die eine Zugriffsautorisierung besteht.

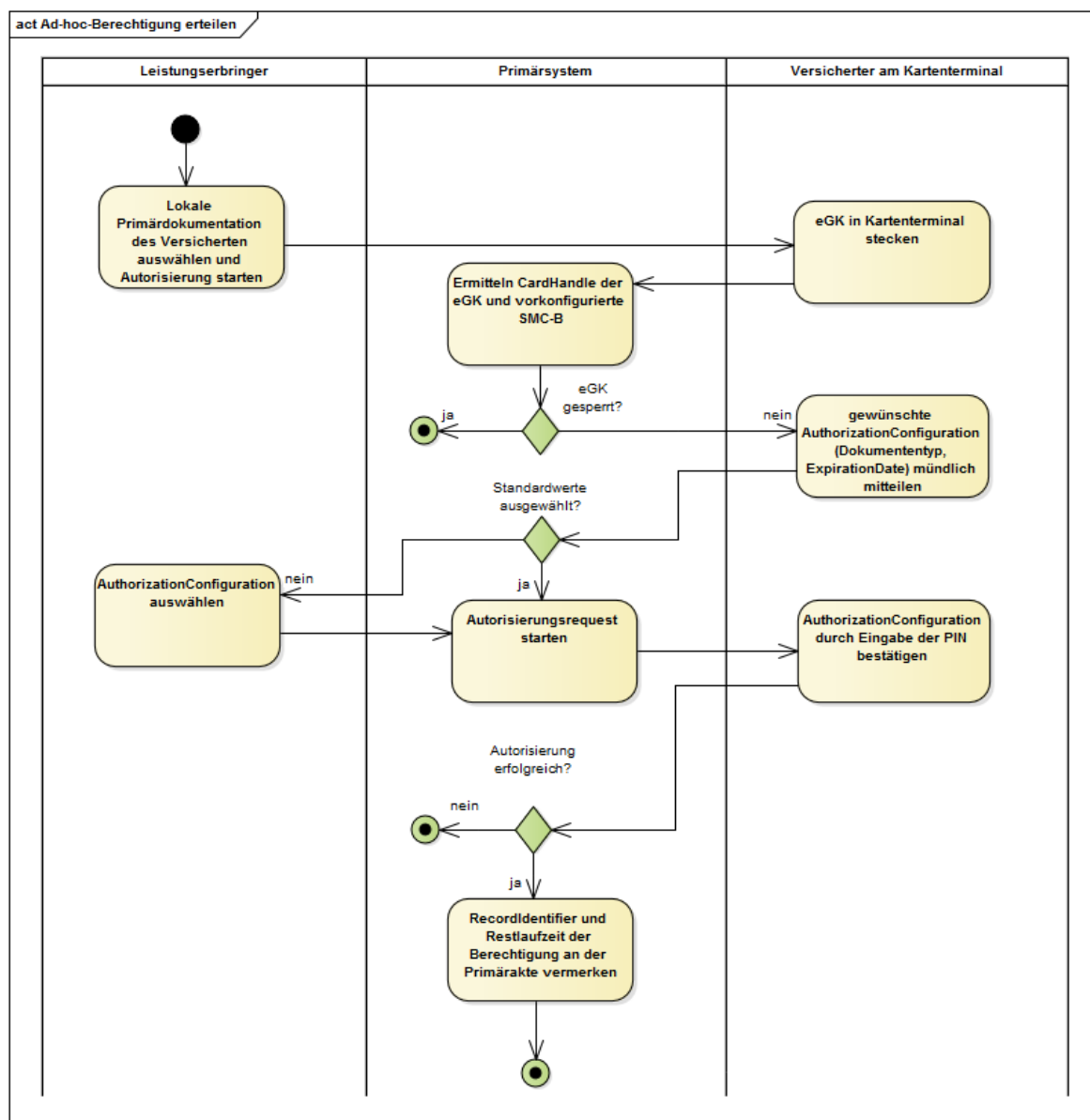


Abbildung 8: Abb\_ILF\_ePA\_Ad-hoc-Berechtigung\_erteilen

### 5.1.3.3 Nutzung

#### A\_14517 - Speicherung RecordIdentifier in der lokalen Primärdokumentation des PS

Das PS MUSS den RecordIdentifier an der lokalen Patientenakte (Primärdokumentation) persistent speichern, falls die Ad-hoc-Autorisierung erfolgreich verlaufen ist. Zusätzlich MUSS das Zugriffsberechtigungs-Endedatum `ExpirationDate` aus `RequestFacilityAuthorization.AuthorizationConfiguration.ExpirationDate` als Ablaufdatum der Zugriffsberechtigung in der Primärakte des Versicherten gespeichert werden.

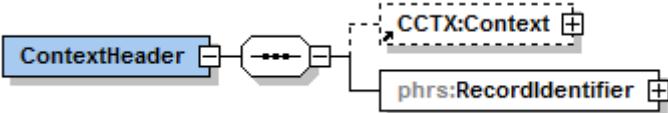
[<=]

Die Ad-hoc-Berechtigung ermöglicht eine Abfrage der Metadaten der ePA-Dokumente und das Anlegen eines lokalen Metadaten-Index für die Dokumente, auf die prinzipiell Zugriffsrechte bestehen, als Vorbereitung von Dokumentenmanagement-Zugriffen.

## 5.2 Dokumentenmanagement

Der Konnektor bietet dem PS mit dem Dienst `DocumentRepository` eine Dokumentenverwaltung auf Basis einer Profilierung der IHE-Spezifikationen rund um das Kernprofil `XDS.b` (Cross-Enterprise Document Sharing) an.

**Tabelle 11: Tab\_ILF\_ePA\_PHRService**

Name	PHRService [gemSpec_FM_ePA#7.1]	
Version	2.0.1	
SOAP-Header		
Namensraum	urn:ihe:iti:xds-b:2007	
Abkürzung Namensraum	ihe	
Operationen	Name	Implementierungshinweise
	DocumentRepository_ProvideAndRegisterDocumentSet-b	Profilierung von [ITI-41], s. Kap. 5.2.1
	DocumentRegistry_RegistryStoredQuery	Profilierung von [ITI-18], s. Kap. 5.2.2
	DocumentRepository_RetrieveDocumentSet	Profilierung von [ITI-43], s. Kap. 5.2.3
	DocumentRegistry_RemoveMetadata	Profilierung von [ITI-62], s. Kap. 5.2.5

<b>WSDL</b>	gemäß: <ul style="list-style-type: none"> <li>• PHRService.wsdl</li> <li>• IHE XCA-Profil [IHE-ITI-TF1]</li> <li>• IHE XDR-Profil [IHE-ITI-TF1]</li> <li>• IHE RMD-Profil [IHE-ITI-RMD]</li> </ul>
<b>XML-Schema</b>	PHRService.xsd

**Tabelle 12: Tab\_ILF\_ePA\_DM\_Profilierung**

<b>Profilierungen des Kernprofiles XDS.b</b>	
<b>Anwendungsfall</b>	<b>IHE-Schnittstelle</b>
<i>Dokumente einstellen</i>	DocumentRepository_ProvideAndRegisterDocumentSet-b [ITI-41]
<i>Dokumente suchen</i>	Registry Stored Query [ITI-18]
<i>Dokumente laden</i>	Retrieve Document Set [ITI-43]
<i>Dokument löschen (auch in Ordnern)</i>	Remove Metadata [ITI-62]

**Tabelle 13: Tab\_ILF\_ePA\_Einschränkungen\_auf\_XDS.b**

<b>Einschränkungen von XDS.b im Rahmen der IHE-Profilierung</b>	<b>Referenz</b>
Kein asynchrones Kommunikationsmuster	nicht umgesetzt: [ITI TF-1#10.2.5]
Beschränkung der Dokumentenformate je nach Ausbaustufe	Kap. 6.3, [gemSpec_DM_ePA#A_14760]
Beschränkung auf RPLC (replace) analog zu Document Replacement Option	[gemSpec_Dokumentenverwaltung#A_14941]

**A\_14418 - MTOM-Pflicht bei [ITI-41]**

Das PS MUSS bei der Umsetzung der IHE XDS-Transaktion [ITI-41] zur Übertragung von Dokumenten eine Kodierung mittels MTOM/XOP [MTOM] gemäß [IHE-ITI-TF2x#V.3.6.] verwenden. [ $\leq$ ]

#### **A\_15084 - SOAP-Header nach [SOAP 1.2]**

Das PS MUSS in der Dokumentenverwaltung die SOAP-Nachricht konform zu [SOAP 1.2] bilden. [ $\leq$ ]

Die Anwendungsfälle des Dokumentenmanagements der Akte erfordern, dass der Nutzer die Berechtigung hat, auf mindestens eine SM-B zuzugreifen, die für die LE-Institution vorliegt und dass eine durch eine Telematik-ID identifizierte Institution oder ein durch eine Telematik-ID identifizierter Teil einer Institution eine Berechtigung erhalten hat. Um diese Berechtigung durchzusetzen ist eine Konfiguration am Konnektor administrativ zu pflegen und vom PS zu nutzen.

Drei Elemente des Aufrufkontextes eines SOAP-Clients geben bei einem Zugriff des Dokumentenmanagements im SOAP-Header darüber Auskunft, von welchem Clientsystem-Arbeitsplatz ein Aufruf auf welche Akte erfolgt:

**Tabelle 14: Tab\_ILF\_ePA\_ClientInformationen**

<b>Name SOAP-Header-Element</b>	<b>Quelle</b>	<b>optional, falls Defaultwert genutzt wird</b>
MandantID	Context/MandantId	ja
ClientSystemID	Context/ClientSystemId	ja
WorkplaceID	Context/WorkplaceId	ja
RecordIdentifier	RecordIdentifier	nein

Die interne Mandantenverwaltung des PS SOLL auf die WS-Kommunikation der ePA über die Nutzung der `MandantID` abgebildet werden. Die `MandantID` steht für die Kennung der PS-Mandanten. Die Konfiguration von PS-Mandanten, SM-Bs und Arbeitsplätzen wird in [gemILF\_PS] geschildert, die Konfiguration für größere LE-Institutionen mit mehreren SM-Bs oder Mandanten in Kapitel 3.3.3.

Der Nutzer ist durch die lokale Mandantenverwaltung seines Primärsystems berechtigt auf die Primärdokumentation des Versicherten zuzugreifen und wird durch die Konfiguration der Mandantenverwaltung im Konnektor derjenigen SM-B zugeordnet, die er für den Zugriff auf die Akte benötigt.

In der Administrationsoberfläche des Konnektors wird gemäß [gemSpec\_Kon#10.3.1.1] im Informationsmodell der LE-Institution die Default-SM-B der Arbeitsplätze, Clientsysteme und Kartenterminals für den Zugriff auf die ePA konfiguriert. Für die Administration des Default-Aufrufkontextes s. [gemSpec\_FM\_ePA#6.4].

*Ad-hoc-Berechtigung erteilen* ist nicht davon abhängig, ob für eine LEI eine oder mehrere SM-Bs im Verzeichnisdienst eingepflegt sind. Falls mehrere SM-Bs in einer LEI verwendet werden, sind die unterschiedlichen Primärsystem-Arbeitsplätze erst dann

zugriffsberechtigt, wenn der Aufrufkontext oder der Default-Aufrufkontext SMC-Bs mit derjenigen Telematik-ID zugeordnet sind, für die eine Berechtigung erteilt wurde.

#### **A\_14475 - SOAP-Header-Clientparameter bei gesamthaft berechtigten LE-Institutionen**

Falls der LE-Institution nur eine einzelne Telematik-ID zugeordnet ist, KANN das PS die in Tab\_ILF\_ePA\_ClientInformationen aufgeführten Parameter des SOAP-Headers in jedem Zugriff des Dokumentenmanagements verwenden. [ $\leq$ ]

Wenn der Parameter nicht gesetzt wird, verwendet das Fachmodul ePA den in der Konnektorkonfiguration hinterlegten Default-Wert.

#### **A\_14476 - SOAP-Header-Clientparameter bei unterschiedlich berechtigten Teilen von LE-Institutionen**

Falls der LE-Institution mehrere Telematik-ID zugeordnet sind, MUSS das PS die in Tab\_ILF\_ePA\_ClientInformationen aufgeführten Parameter des SOAP-Headers in jedem Zugriff des Dokumentenmanagements verwenden. [ $\leq$ ]

#### **A\_14698 - Einstellen von Zugriffsinformationen in Metadaten**

Für die Weiterverarbeitung auf Dokumentenebene MÜSSEN Zugriffsinformationen gemäß Tab\_ILF\_ePA\_Zugriffsinformation\_Werte zusätzlich in die Metadaten der Dokumentenmanagement-Zugriffe eingestellt werden:

**Tabelle 15: Tab\_ILF\_ePA\_Zugriffsinformation\_Werte**

<b>Zugriffsinformationen</b>	<b>IHE-Schnittstellen</b>	<b>Wertgleiches Request-Attribut</b>
InsurantId	[ITI-41], [ITI-18]	XDSSubmissionSet.patientID
	[ITI-41], [ITI-18]	XDSDocumentEntry.patientID
	[ITI-41], [ITI-18]	XDSDocumentEntry.sourcePatientId
HomeCommunityID	[ITI-43]	XDSDocumentEntry.repositoryUniqueID
	[ITI-43]	XDSDocumentEntry.HomeCommunityID
	[ITI-86]	DocumentRequest.RepositoryUniqueID

[ $\leq$ ]

Das Ersetzen eines Dokumentes ist als Kombination mehrerer Anwendungsfälle umzusetzen: Nach dem Ermitteln (Suchen, Kap. 5.2.2) und Löschen des zu ersetzenden Dokumentes (Kap. 5.2.5) nach Rücksprache mit dem Versicherten wird das ersetzende Dokument (als "Original"-Dokument, s. A\_14250) in die ePA eingestellt (Kap. 5.2.1).

### **5.2.1 Dokumente einstellen**

*Herr Dr. Weber hatte für Frau Gundlach vor einigen Monaten einen Notfalldatensatz auf ihre eGK geschrieben. Dr. Weber bespricht mit Frau Gundlach, ihren Notfalldatensatz auch in ihre ePA einzustellen. Frau Gundlach erteilt eine Ad-hoc-Berechtigung für diesen Zugriff. Bei Auswahl der entsprechenden Funktion nutzt Dr. Weber die Möglichkeit, die Metadaten zu kontrollieren, mit denen der Notfalldatensatz automatisch für die Akte von Frau*

*Gundlach konnotiert werden. Dr. Weber nimmt kurz Notiz von der Bestätigungsmeldung über den Erfolg des Einstellens.*

#### **A\_15653 - Funktionsmerkmal Dokumente Einstellen**

Das PS MUSS es dem Leistungserbringer ermöglichen, ePA-Dokumente in die Akte eines Versicherten einstellen zu können. Dafür MUSS das PS die Konnektorschnittstellenoperation `ProvideAndRegisterDocumentSet-b` verwenden.[<=]

Zur Umsetzung des Anwendungsfalles *Dokumente durch einen Leistungserbringer Einstellen* aus [gemSysL\_ePA#3.7.1, UC 4.1 - Dokumente durch einen Leistungserbringer einstellen] wird `Provide & Register Document Set-b` [ITI-41] gemäß Cross-Enterprise Document Reliable Interchange (XDR) Profile profiliert.

**Tabelle 16: Tab\_ILF\_ePA\_IHE-Profilierung\_ITI41**

<b>IHE-Konzept</b>	<b>Wert</b>	<b>Referenz</b>
PS als IHE Akteur	XDR Document Source	[IHE ITI-41]
XDR Document Source Options	keine	[IHE ITI-41#3.41.4.1.2.1]
Document Relationships [ITI TF-3#Table4.2.2.2-1]	RPLC (replace) analog zu Document Replacement Option einer XDS.b Document Source	[ITI TF-1#10.2.2] und [ITI TF-1#10.2.3]
SOAP-Action	urn:ihe:iti:2007:ProvideAndRegisterDocumentSet-b	[IHE ITI-41#3.41.4.1.2]

Die Unterstützung für RPLC (replace) hat zur Folge, dass Dokumente ersetzt werden können durch eine neue Version des gleichen Dokuments. Das hat zur Folge, dass das alte Dokument in den Status (`DocumentEntry.availabilityStatus`) "Deprecated" wechselt und mit dem neuen Dokument (Status "Approved") über eine "RPLC"-Association verbunden wird.

#### **5.2.1.1 Schnittstelle**

Das Fachmodul ePA bietet zur logischen Schnittstelle `I_PHR_Management` am Webservice `PHR_Service` (analog IHE-Dienst `DocumentRepository`) die Operation `DocumentRepository_ProvideAndRegisterDocumentSet-b` an, und übernimmt gemäß [ITI-41] die Rolle eines IHE `DocumentRepository` gegenüber dem PS.

**Tabelle 17: Tab\_ILF\_ePA\_Operation\_Dokument\_einstellen**

<b>Operationsname</b>	<b>DocumentRepository_ProvideAndRegisterDocumentSet-b [gemSpec_FM_ePA#7.1.1.1]</b>	
<b>Aufrufparameter</b>	<b>Name</b>	<b>Implementierung</b>
	<code>ProvideAndRegisterDocumentSetRequest</code>	[ITI-41#3.41.4.1.2]



Rückgabeparameter	Name	Implementierung
	RegistryResponse	[ITI-41#3.41.4.2]

### **A\_14201 - Anwendungsfall Dokumente einstellen**

Das PS MUSS bei vorliegender Berechtigung Dokumente in die Akte eines Versicherten einstellen können. Das Primärsystem MUSS im Dienst `DocumentRepository` des Konnektor-Fachmoduls die Operation

`DocumentRepository_ProvideAndRegisterDocumentSet-b` nutzen

[gemSpec\_FM\_ePA#7.1.1.1] und dazu schemakonforme SOAP-Nachrichten erstellen können. [≤]

### **A\_14253 - Metadaten-Pflicht für Dokumente**

Das PS MUSS Metadaten ausschließlich aus der im [gemSpec\_DM\_ePA] 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\_DM\_ePA#Tabelle Nutzungsvorgaben für Metadatenattribute XDS.b] befüllen. Das PS MUSS alle als `R=required` markierten Metadatenfelder setzen. [≤]

Die Auswahl der Metadaten soll möglichst weitgehend automatisiert werden.

### **A\_16194 - Änderbarkeit der Metadaten - Auswahllisten**

Bei der Auswahl der Metadaten zum Zwecke des Einstellens von Dokumenten MUSS das PS insbesondere im Falle erforderlicher Auswahl-dialoge beachten:

- Die Bildung von Auswahllisten erfolgt gemäß [gemSpec\_DM\_ePA] und Kap. 6;
- Auswahllisten sind konfiguratv änderbar;
- Das PS kann Metadaten dem Benutzer automatisch gefüllte Metadaten zur händischen Nacheditierung anbieten.

[≤]

### **A\_20179-01 - Setzen der Vertraulichkeitsstufe**

Beim Einstellen von Dokumenten MUSS das PS für jedes Dokument eine Vertraulichkeitsstufe wählen, die dem Wunsch des Versicherten entspricht, d.h. entweder "streng vertraulich" (`very restricted`), "vertraulich" (`restricted`) oder "normal" (`normal`). [≤]

Eine entsprechende Absprache zwischen LEI und Versichertem muss nicht zwangsläufig explizit für jedes einzelne Dokument getroffen werden, sondern kann auch im Vorfeld stattfinden, z. B. über eine Vereinbarung über die Vertraulichkeitsstufe von bestimmten Dokumententypen oder ähnliche Mechanismen.

### **A\_20517 - Exklusivität der Dokumentenkategorien**

Das PS MUSS beim Einstellen von Dokumenten die Dokumentenkategorien (aufgelistet in der [gemSpec\_DM\_ePA#Tab\_DM\_Dokumentenkategorien]) exklusiv anwenden, d.h. die Metadaten müssen so gesetzt werden, dass jedes Dokument in genau eine der Kategorie fällt.

Die Kennzeichnung erfolgt

- durch Ablage in einen entsprechenden, vom Aktensystem angelegten Ordner (Kategorien 1a\* und 7, s. [gemSpec\_DM\_ePA#Tab\_DM\_112: Codes in ValueSet für Folder.codeList])

- durch Kennzeichnung mit Metadaten (restliche Kategorien)

#### **[<=]**

Daten zu Befunden, Diagnosen, durchgeführten und geplanten Therapiemaßnahmen, Früherkennungsuntersuchungen, zu Behandlungsberichten und sonstige untersuchungs- und behandlungsbezogene medizinische Informationen (Kategorien 1a\*, siehe [gemSpec\_DM\_ePA#Tab\_DM\_Dokumentenkategorien] und [Tab\_DM\_112: Codes in ValueSet für Folder.codeList]) müssen einer einzelnen Unterkategorie (z.B. 1a1, Befund eines Hausarztes/ einer Hausärztin) zugeordnet werden. Auf diese Unterkategorien kann der Versicherte Zugriffsberechtigungen erteilen.

#### **A\_20180-01 - Unterkategorien von Kategorie 1a\* auswählen**

Falls das Dokument in die Kategorien 1a\* (siehe [gemSpec\_DM\_ePA#Tab\_DM\_Dokumentenkategorien]) fällt, MUSS das PS das Dokument genau eine dieser Kategorien 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 `uniqueId` verbindet, vgl. u.a. [IHE-ITI-TF3#4.2.1.3]. [**<=**]

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

#### **A\_14932 - Bildung und Verwendung einer UUID für Dokumente**

Das PS MUSS eine `DocumentEntry.UniqueID` gemäß [ITI-TF-3#4.2.3.2.26] erstellen. Für die Dokumentenverwaltung im ePA-Aktensystem wird die `DocumentEntry.UniqueID` in die Metadaten der IHE-Nachrichten eingestellt:

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

#### **[<=]**

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

### **5.2.1.2 Umsetzung**

Die Aktivitäten des Anwendungsfalles *Dokumente einstellen* sind:

#### **Vorbedingung:**

- Ermittelter `RecordIdentifier`
- Das einzustellende Dokument sollte mit dem Versicherten besprochen sein
- `ExpirationDate` der Aktenzugriffsberechtigung noch nicht abgelaufen

#### **Auslöser:**

- Nutzerinteraktion

#### Aktivitäten:

- Auswahl der RecordIdentifier
- 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.

#### Beispiel 3: Bsp\_ILF\_ePA\_ProvideAndRegisterDocumentSetRequest

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:m2="http://ws.gematik.de/fa/phr/v1.1"
xmlns:m1="http://ws.gematik.de/conn/ConnectorCommon/v5.0"
xmlns:m0="http://ws.gematik.de/conn/ConnectorContext/v2.0"
xmlns:soap="http://www.w3.org/2003/05/soap-envelope"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soap:Header>
    <m:ContextHeader
xmlns:m="http://ws.gematik.de/conn/phrs/PHRService/v1.3">
      <m0:Context>
        <m1:MandantId>Mandant1</m1:MandantId>
        <m1:ClientSystemId>ClientID1</m1:ClientSystemId>
        <m1:WorkplaceId>CATS</m1:WorkplaceId>
      </m0:Context>
      <m:RecordIdentifier>
        <m2:InsurantId extension="X110411319" root="1.2.276.0.76.4.8"/>
        <m2:HomeCommunityId>urn:oid:1.2.276.0.76.3.1.315.3.2.1.1</m2:HomeCo
mmunityId>
      </m:RecordIdentifier>
    </m:ContextHeader>
    <Action
xmlns="http://www.w3.org/2005/08/addressing">urn:ihe:iti:2007:ProvideA
ndRegisterDocumentSet-b</Action>
    <MessageID xmlns="http://www.w3.org/2005/08/addressing">cc7f3acb-
d210-4ca0-9d9e-7143f1b95ee3</MessageID>
    <To
xmlns="http://www.w3.org/2005/08/addressing">http://10.11.217.160:80
/ws/PHRService</To>
    <ReplyTo xmlns="http://www.w3.org/2005/08/addressing">
      <Address>http://www.w3.org/2005/08/addressing/anonymous</Address>
    </ReplyTo>
    <xdr:homeCommunityBlock xmlns:xdr="urn:ihe:iti:xdr:2014">
      <xdr:homeCommunityId>urn:oid:1.2.276.0.76.3.1.315.3.2.1.1</xdr:homeCo
mmunityId>
    </xdr:homeCommunityBlock>
```

```

</soap:Header>
<soap:Body>
<ProvideAndRegisterDocumentSetRequest xmlns="urn:ihe:iti:xds-b:2007"
xmlns:lcm="urn:oasis:names:tc:ebxml-regrep:xsd:lcm:3.0"
xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0"
xmlns:rsm="urn:oasis:names:tc:ebxml-regrep:xsd:rsm:3.0">
<lcm:SubmitObjectsRequest>
<rs:RequestSlotList>
<rim:Slot name="homeCommunityId">
<rim:ValueList>
<rim:Value>urn:oid:1.2.276.0.76.3.1.315.3.2.1.1</rim:Value>
</rim:ValueList>
</rim:Slot>
</rs:RequestSlotList>
<rim:RegistryObjectList>
<!-- SubmissionSet -->
<rim:RegistryPackage home="urn:oid:1.2.276.0.76.3.1.315.3.2.1.1"
objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:RegistryPackage" id="submissionset">
<!-- SubmissionSet.submissionTime -->
<rim:Slot name="submissionTime">
<rim:ValueList>
<rim:Value>20201218172143</rim:Value>
</rim:ValueList>
</rim:Slot>
<!-- SubmissionSet.author -->
<rim:Classification objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification" id="author"
classifiedObject="submissionset" classificationScheme="urn:uuid:a7058bb9-
b4e4-4307-ba5b-e3f0ab85e12d">
<rim:Slot name="authorRole">
<rim:ValueList>
<rim:Value>11^^^&1.3.6.1.4.1.19376.3.276.1.5.13&ISO</rim:Value>
</rim:ValueList>
</rim:Slot>
<rim:Slot name="authorPerson">
<rim:ValueList>
<rim:Value>^Münchenhausen^David^^^Prof. Dr.^^^</rim:Value>
</rim:ValueList>
</rim:Slot>
<rim:Slot name="authorInstitution">
<rim:ValueList>
<rim:Value>Praxis David Graf MünchenhausenNOT-
VALID^^^&1.2.276.0.76.4.188&ISO^^^1-SMC-B-Testkarte-
783110000092399</rim:Value>
</rim:ValueList>
</rim:Slot>
</rim:Classification>
<!-- SubmissionSet.contentTypeCode -->
<rim:Classification objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification" id="contentType"
classifiedObject="submissionset" classificationScheme="urn:uuid:aa543740-
bdda-424e-8c96-df4873be8500" nodeRepresentation="8">

```

```
<rim:Slot name="codingScheme">
<rim:ValueList>
<rim:Value>1.3.6.1.4.1.19376.3.276.1.5.12</rim:Value>
</rim:ValueList>
</rim:Slot>
<rim:Name>
<rim:LocalizedString xml:lang="de-DE" value="Veranlassung durch
Patient"/>
</rim:Name>
</rim:Classification>
<!-- SubmissionSet Classification of RegistryPackage -->
<rim:Classification objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification"
id="SubmissionSetClassification" classifiedObject="submissionset"
classificationNode="urn:uuid:a54d6aa5-d40d-43f9-88c5-b4633d873bdd"/>
<!-- SubmissionSet.patientId -->
-<rim:ExternalIdentifier objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:ExternalIdentifier" id="patientId"
value="X110411319^^^&1.2.276.0.76.4.8&ISO"
registryObject="submissionset" identificationScheme="urn:uuid:6b5aea1a-
874d-4603-a4bc-96a0a7b38446">
-<rim:Name>
<rim:LocalizedString value="XDSSubmissionSet.patientId"/>
</rim:Name>
</rim:ExternalIdentifier>
<!-- SubmissionSet.uniqueId -->
-<rim:ExternalIdentifier objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:ExternalIdentifier" id="uniqueId"
value="1.2.840.113556.1.8000.2554.35589.34102.63238.18691.36463.16560
801.3400984" registryObject="submissionset"
identificationScheme="urn:uuid:96fdda7c-d067-4183-912e-bf5ee74998a8">
<rim:Name>
<rim:LocalizedString value="XDSSubmissionSet.uniqueId"/>
</rim:Name>
</rim:ExternalIdentifier>
</rim:RegistryPackage>
<rim:Association id="association-0" targetObject="DocumentEntry-0"
sourceObject="submissionset" associationType="urn:oasis:names:tc:ebxml-
regrep:AssociationType:HasMember">
<rim:Slot name="SubmissionSetStatus">
<rim:ValueList>
<rim:Value>Original</rim:Value>
</rim:ValueList>
</rim:Slot>
</rim:Association>
<rim:ExtrinsicObject home="urn:oid:1.2.276.0.76.3.1.315.3.2.1.1"
objectType="urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1"
id="DocumentEntry-0" mimeType="application/xml">
<!-- DocumentEntry.creationTime -->
<rim:Slot name="creationTime">
<rim:ValueList>
<rim:Value>20191209124919</rim:Value>
</rim:ValueList>
```

```

</rim:Slot>
<!-- DocumentEntry.languageCode -->
<rim:Slot name="languageCode">
<rim:ValueList>
<rim:Value>de-DE</rim:Value>
</rim:ValueList>
</rim:Slot>
<rim:Slot name="URI">
<rim:ValueList>
<rim:Value>pssim_nfd.xml</rim:Value>
</rim:ValueList>
</rim:Slot>
<!-- DocumentEntry.Title -->
<rim:Name>
<rim:LocalizedString xml:lang="de-DE" value="PsSim: Notfalldaten"/>
</rim:Name>
<!-- DocumentEntry.classCode -->
<rim:Classification objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification" id="class-0"
classifiedObject="DocumentEntry-0"
classificationScheme="urn:uuid:41a5887f-8865-4c09-adf7-e362475b143a"
nodeRepresentation="AUS">
<rim:Slot name="codingScheme">
<rim:ValueList>
<rim:Value>1.3.6.1.4.1.19376.3.276.1.5.8</rim:Value>
</rim:ValueList>
</rim:Slot>
<rim:Name>
<rim:LocalizedString xml:lang="de-DE" value="Medizinischer Ausweis"/>
</rim:Name>
</rim:Classification>
<!-- DocumentEntry.confidentialityCode -->
<rim:Classification objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification" id="confidentiality-0"
classifiedObject="DocumentEntry-0"
classificationScheme="urn:uuid:f4f85eac-e6cb-4883-b524-f2705394840f"
nodeRepresentation="LEI">
<rim:Slot name="codingScheme">
<rim:ValueList>
<rim:Value>1.2.276.0.76.5.491</rim:Value>
</rim:ValueList>
</rim:Slot>
<rim:Name>
<rim:LocalizedString xml:lang="de-DE" value="Dokument einer
Leistungserbringerinstitution"/>
</rim:Name>
</rim:Classification>
<!-- DocumentEntry.formatCode -->
<rim:Classification objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification" id="formatCode-0"
classifiedObject="DocumentEntry-0"
classificationScheme="urn:uuid:a09d5840-386c-46f2-b5ad-9c3699a4309d"
nodeRepresentation="urn:gematik:ig:Notfalldatensatz:r3.1">

```

```

<rim:Slot name="codingScheme">
<rim:ValueList>
<rim:Value>1.3.6.1.4.1.19376.3.276.1.5.6</rim:Value>
</rim:ValueList>
</rim:Slot>
<rim:Name>
<rim:LocalizedString xml:lang="de-DE" value="Notfalldatensatz"/>
</rim:Name>
</rim:Classification>
<!-- DocumentEntry.healthCareFacilityTypeCode -->
<rim:Classification objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification" id="healthCare-0"
classifiedObject="DocumentEntry-0"
classificationScheme="urn:uuid:f33fb8ac-18af-42cc-ae0e-ed0b0bdb91e1"
nodeRepresentation="PRA">
<rim:Slot name="codingScheme">
<rim:ValueList>
<rim:Value>1.3.6.1.4.1.19376.3.276.1.5.2</rim:Value>
</rim:ValueList>
</rim:Slot>
<rim:Name>
<rim:LocalizedString xml:lang="de-DE" value="Arztpraxis"/>
</rim:Name>
</rim:Classification>
<!-- DocumentEntry.authorPerson and DocumentEntry.authorRole -->
<rim:Classification objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification" id="author-0"
classifiedObject="DocumentEntry-0"
classificationScheme="urn:uuid:93606bcf-9494-43ec-9b4e-a7748d1a838d">
<rim:Slot name="authorRole">
<rim:ValueList>
<rim:Value>11^^^&1.3.6.1.4.1.19376.3.276.1.5.13&ISO</rim:Value>
</rim:ValueList>
</rim:Slot>
<rim:Slot name="authorPerson">
<rim:ValueList>
<rim:Value>^Müller-Holzscheit^Marcello-
Bernhardino^^^Dr.^^^</rim:Value>
</rim:ValueList>
</rim:Slot>
</rim:Classification>
<!-- DocumentEntry.practiceSettingCode -->
<rim:Classification objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification" id="practiceSettingCode-0"
classifiedObject="DocumentEntry-0"
classificationScheme="urn:uuid:ccc55598-8b07-4b77-a05e-ae952c785ead"
nodeRepresentation="ALLG">
<rim:Slot name="codingScheme">
<rim:ValueList>
<rim:Value>1.3.6.1.4.1.19376.3.276.1.5.4</rim:Value>
</rim:ValueList>
</rim:Slot>
<rim:Name>

```



```
<rim:LocalizedString xml:lang="de-DE" value="Allgemeinmedizin"/>
</rim:Name>
</rim:Classification>
<!-- DocumentEntry.typeCode -->
<rim:Classification objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:Classification" id="typeCode-0"
classifiedObject="DocumentEntry-0"
classificationScheme="urn:uuid:f0306f51-975f-434e-a61c-c59651d33983"
nodeRepresentation="BESC">
<rim:Slot name="codingScheme">
<rim:ValueList>
<rim:Value>1.3.6.1.4.1.19376.3.276.1.5.9</rim:Value>
</rim:ValueList>
</rim:Slot>
<rim:Name>
<rim:LocalizedString xml:lang="de-DE" value="Ärztliche Bescheinigungen"/>
</rim:Name>
</rim:Classification>
<rim:ExternalIdentifier objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:ExternalIdentifier" id="patientId-0"
value="X110411319^^^&1.2.276.0.76.4.8&ISO"
registryObject="DocumentEntry-0"
identificationScheme="urn:uuid:58a6f841-87b3-4a3e-92fd-a8ffeff98427">
<rim:Name>
<rim:LocalizedString value="XDSDocumentEntry.patientId"/>
</rim:Name>
</rim:ExternalIdentifier>
<rim:ExternalIdentifier objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:ExternalIdentifier" id="uniqueId-0"
value="1.2.840.113556.1.8000.2554.20502.5074.39693.19397.40947.396234
1.16685811" registryObject="DocumentEntry-0"
identificationScheme="urn:uuid:2e82c1f6-a085-4c72-9da3-8640a32e42ab">
<rim:Name>
<rim:LocalizedString value="XDSDocumentEntry.uniqueId"/>
</rim:Name>
</rim:ExternalIdentifier>
</rim:ExtrinsicObject>
</rim:RegistryObjectList>
</lcm:SubmitObjectsRequest>
<Document id="DocumentEntry-0">
<Include xmlns="http://www.w3.org/2004/08/xop/include"
href="cid:Document0@PHRService.konlan"/>
</Document>
</ProvideAndRegisterDocumentSetRequest>
</soap:Body>
</soap:Envelope>
```

## XDS-Option „Document Replacement“ - Ersetzen eines existierenden Dokuments



Ein eingestelltes Dokument kann auch ein existierendes Dokument ersetzen. Dies erfolgt durch Verwendung der „Document Replacement“-Option. Dazu wird das gleiche Dokument (mit geänderten 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“-Assoziation miteinander verbunden, so dass nach dem Einstellen erkennbar ist, dass das neue Dokument das alte ersetzt. Lädt man erneut eine neue Fassung hoch, erhält man analog zwei Dokumente im Status "Deprecated" und das neueste im Status "Approved".

Alle alten Dokumente (Status "Deprecated") können nach wie vor gefunden und heruntergeladen werden. Einige Suchen erlauben das Filtern nach Status bzw. zeigen per Default auch nur Dokumente im Status „Approved“ an.

Eingestellt (im „Submission Set“) wird das neue Dokument inkl. DocumentEntry-Metadaten, ein Verweis auf das alte Dokument und die verbindende „Replace“-Association (urn:ihe:iti:2007:AssociationType:RPLC).

### **XDS-Option „Document Addendum“ - Verlinken von Dokumenten**

Die XDS-Option „Document Addendum“ (XDS.b Document Source) wird benötigt, um Dokumente verschiedener Formate als Ergänzung bestehender Dokumente unter Verwendung der „Append“-Association zu kennzeichnen. Sie ermöglicht es, ein Dokument durch ein neues Dokument zu ergänzen. Der Vorgang ist ähnlich wie beim Document Replacement. Abweichend davon sind am Ende beide Dokumente im Status Approved und werden über eine „Append“-Assoziation (urn:ihe:iti:2007:AssociationType:APND) miteinander verbunden.

In ePA 2.0 ist die „Append“-Association noch nicht zur Verwendung freigegeben.

### **5.2.1.3 Nutzung**

Dokumente, die Leistungserbringer einstellen, werden unabhängig vom Inhalt des Dokumentes als LE-Dokumente (Kennzeichnung über entsprechende Auswahl aus `SubmissionSet.AuthorRole`, siehe [gemSpec\_DM\_ePA#2.1.4.1], und dem konfigurierten `XSDocumentEntry.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\_DM\_ePA]#Tabelle Nutzungsvorgaben für Metadatenattribute XDS.b zu befüllen;
- `XSDocumentEntry.author.authorSpecialty` wird mit einem die Fachrichtung der LEI beschreibenden Wert der Selbstauskunft der LEI (Kap. 6.2, A\_15086) befüllt, es sei denn, der Autor des Dokumentes entstammt nicht der das Dokument einstellenden Institution;
- `XSDocumentEntry.healthcareFacilityTypeCode` wird mit einem den Typ der LEI beschreibenden Wert der Selbstauskunft der LEI (Kap. 6.2, A\_15086) befüllt, es sei denn, der Autor des Dokumentes entstammt nicht der das Dokument einstellenden Institution;

- Das PS MUSS sicherstellen, dass der `XSDDocumentEntry.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\_14251 - Vom LE in die Akten einstellbare Dokumententypen**

Das Primärsystem MUSS die in die ePA einstellbaren Dokumententypen aus [gemSpec\_DM\_ePA#A\_14760] in die ePA einstellen können.

[<=]

### **Beispiel 4: Bsp\_ILF\_ePA\_ProvideAndRegisterDocumentSetResponse**

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
  <soap:Header>
    <Action xmlns="http://www.w3.org/2005/08/addressing"/>
    <MessageID xmlns="http://www.w3.org/2005/08/addressing">urn:uuid:48d9984a-
    eaa9-4b54-b968-216e98a13e3b</MessageID>
    <To
    xmlns="http://www.w3.org/2005/08/addressing">http://www.w3.org/2005/08/addres
    sing/anonymous</To>
    <RelatesTo xmlns="http://www.w3.org/2005/08/addressing">6e2fa9e2-18fb-4071-
    b796-a49c5fe9a303</RelatesTo>
  </soap:Header>
  <soap:Body>
    <ns8:RegistryResponse status="urn:oasis:names:tc:ebxml-
    regrep:ResponseStatusType:Success"
    xmlns:ns2="http://ws.gematik.de/conn/ConnectorCommon/v5.0"
    xmlns:ns3="http://ws.gematik.de/conn/ConnectorContext/v2.0"
    xmlns:ns4="http://ws.gematik.de/fa/phr/v1.1"
    xmlns:ns5="http://ws.gematik.de/conn/phrs/PHRService/v1.3"
    xmlns:ns6="urn:ihe:iti:xds-b:2007" xmlns:ns7="urn:oasis:names:tc:ebxml-
    regrep:xsd:rim:3.0" xmlns:ns8="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0"
    xmlns:ns9="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0"
    xmlns:ns10="urn:oasis:names:tc:ebxml-regrep:xsd:lcm:3.0"
    xmlns:ns11="http://ws.gematik.de/fa/vsdm/vsd/v5.2"
    xmlns:ns12="http://www.w3.org/2006/05/addressing/wsdl"
    xmlns:ns13="http://ws.gematik.de/tel/error/v2.0"
    xmlns:ns14="urn:oasis:names:tc:dss:1.0:core:schema"
    xmlns:ns15="http://www.w3.org/2000/09/xmldsig#" xmlns:ns16="urn:hl7-org:v3"
    xmlns:ns17="urn:oasis:names:tc:SAML:1.0:assertion"
    xmlns:ns18="urn:ihe:iti:rm:2017"/>
  </soap:Body>
</soap:Envelope>
```

In [gemSpec\_DM\_ePA#A\_14760] ist beschrieben, bei Einhaltung welcher Vorgaben konsistente Metadaten für das Einstellen des Dokumentes erzeugt werden können.

#### **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\_16188 - MTOM-Pflicht bei [ITI-43]**

Das PS MUSS bei der Umsetzung der IHE XDS-Transaktion [ITI-43] die Übertragung von Dokumenten mit MTOM/XOP [MTOM] umsetzen.  
[≤]

**Tabelle 18: Tab\_ILF\_ePA\_Fehlerbehandlung\_Dokumente\_einstellen**

Fehlercode	Beschreibung	Handlungsanweisung
7211	Dokument überschreitet maximal zulässige Größe von 25 MB	Den Versicherten bei Bedarf über das Fehlen der Möglichkeit zum Einstellen des übergroßen Dokumentes informieren.
7212	Summe der Dokumente überschreitet maximal zulässige Größe von 250 MB	Dokumentenpaket verkleinern (etwa durch Aufteilung) und ein kleineres Dokumentenpaket einstellen.

## **5.2.2 Dokumente suchen**

*Frau Gundlach berichtet Dr. Weber über den Arztbrief, den ihr Radiologe vor wenigen Tagen in ihre Patientenakte geschrieben hat. Dr. Weber sieht in seiner lokalen Akte, dass die 7 Tage lang gültige Berechtigung auf die elektronische Akte zuzugreifen, noch nicht abgelaufen ist. Er sucht nach dem Arztbrief des Radiologen über dessen Namen in der ePA-Suchmaske des PVS. Sein PVS zeigt ihm Metadaten zum Arztbrief des Kollegen an.*

Zur Umsetzung des Anwendungsfalles *Dokumente durch einen Leistungserbringer suchen* aus [gemSysL\_ePA#3.7.3, UC 4.3 - Dokumente durch einen Leistungserbringer suchen] wird Registry Stored Query [ITI-18] profiliert.

#### **A\_15652 - Funktionsmerkmal Dokumente Suchen**

Das PS MUSS es dem Leistungserbringer ermöglichen, ePA-Dokumente in der Akte eines Versicherten suchen zu können. Dafür MUSS das PS die Konnektorschnittstellenoperation `RegistryStoredQuery` verwenden.  
[≤]

Tabelle 19: Tab\_ILF\_ePA\_IHE-Profilierung\_ITI18

IHE-Konzept	Wert	Referenz
PS als IHE Akteur	Document Consumer	Registry Stored Query [ITI-18] (ITI TF-2a: 3.18)
Document Relationships [ITI TF-3#Table4.2.2.2-1]	RPLC (replace) analog zu Document Replacement Option einer XDS.b Document Source	[ITI TF-1#10.2.2] und [ITI TF-1#10.2.3]
Stored Queries	FindDocuments, FindDocumentsByTitle, FindSubmissionSets, FindDocumentsByReferenceID, GetSubmissionSets, GetSubmissionSetsAndContents, GetAll und GetDocuments, GetAssociations, GetDocumentsAndAssociations, GetRelatedDocuments, FindFolders, GetFolders, GetFoldersForDocument, GetFolderAndContents	Registry Stored Query [ITI-18]
SOAP-Action	urn:ihe:iti:2007:RegistryStoredQuery	[ITI-18#3.18.4.1]

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

Um *Dokumente suchen* zu können, brauchen Leistungserbringer nicht zu wissen, welche Art Berechtigung sie erhalten haben (Zugriffsberechtigung auf LE-Dokumente, Versicherten-Dokumente oder mehrere dieser Dokumententypen). Die Suche erfolgt immer ausschließlich auf den berechtigungsgemäß tatsächlich zugänglichen Dokumenten, nie auf Dokumenten, für die keine Zugriffsberechtigung besteht.

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

- kein Filter
- Zeitintervall
- Dokumentenkategorie, darunter auch Dokumentenkategorie 1a (Suche über Ordner)

- Dokumentenquelle (z.B. eine bestimmte Facharztgruppe)
- SubmissionSet-Identifizier
- Submission-Zeit

Weitere für Suchstrategien geeignete Metadaten von Dokumenten (Metadaten) können [gemSpec\_DM\_ePA] entnommen werden. Sie beziehen sich vor allem auf Informationen der Dokumentenverwaltung, weniger auf den (medizinischen) Inhalt der Dokumente.

#### **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 Auswahlsschritt 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-Identifizier als UUID.

#### **A\_21133 - Identifizierung unscharfer Ergebnisse**

Das PS SOLL etwaige unscharfe Suchergebnisse (siehe gemSpec\_Dokumentenverwaltung#A\_21131) in der Ergebnismenge als solche kennzeichnen können.

[<=]

### **5.2.2.1 Schnittstelle**

Das Fachmodul ePA bietet zur logischen Schnittstelle `I_PHR_Management` am Webservice `PHR_Service` (analog IHE-Dienst `DocumentRegistry`) die Operation `DocumentRegistry_RegistryStoredQuery` an, die in ihrem Außenverhalten der Schnittstellendefinition des [ITI-18] folgt und die Rolle eines IHE `DocumentRegistry` gegenüber dem PS übernimmt.

**Tabelle 20: Tab\_ILF\_ePA\_Operation\_Dokument\_suchen**

Operationsname	DocumentRegistry_RegistryStoredQuery [gemSpec_FM_ePA#7.1.1.2]	
Aufrufparameter	Name	Implementierung

	AdhocQueryRequest	Stored Query aus Tab_ILF_ePA_StoredQueries
<b>Rückgabeparameter</b>	<b>Name</b>	<b>Implementierung</b>
	AdhocQueryResponse	ebXML version 3 [ebRS] gemäß [ITI-18]#3.18.4.1.2.6

### **A\_17198-01 - Nutzung des um XSDDocumentEntryTitle erweiterten Registry Stored Query FindDocuments**

Das PS MUSS den in [ITI-18] nicht enthaltenen zusätzlichen Anfragetyp `FindDocumentsByTitle` mit der Query-ID "urn:uuid:ab474085-82b5-402d-8115-3f37cb1e2405" und denselben Parameternutzungsvorgaben der Registry `Stored QueryFindDocuments` gemäß [IHE-ITI-TF2a#3.18.4.1.2.3.7.1] in Verbindung mit dem zusätzlich zu [ITI-18] eingeführten Suchparameter `$XSDDocumentEntryTitle` nutzen können. Der zusätzliche Parameter `$XSDDocumentEntryTitle` ist verpflichtend und filtert die Suchergebnismenge über das Attribut `XSDDocumentEntry.title`, siehe auch [gemSpec\_Dokumentenverwaltung#A\_17184]. [**<=**]


### **A\_18197 - Suche nach Institutionen im Anfragetyp "FindDocumentsByTitle"**

Das PS KANN im Anfragetyp `FindDocumentsByTitle` den optionalen Parameter `$XSDDocumentEntryAuthorInstitution` setzen, um eine Suchanfrage nach Institutionen durchzuführen, bei denen die Ergebnismenge auf Einträge eingeschränkt wird, die im `XSDDocumentEntry.author`-Slot über ein zutreffendes `authorInstitution`-Sub-Attribut verfügen. [**<=**]

Für die Suche über beiden Parameter

- `$XSDDocumentEntryTitle` und
- `$XSDDocumentEntryAuthorInstitution`

ist eine Ähnlichkeitssuche möglich, wie auch beim Parameter `$XSDDocumentEntryAuthorPerson`. 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:

- `$XSDDocumentEntryTitle`
- `$XSDDocumentEntryAuthorInstitution`
- `$XSDDocumentEntryAuthorPerson`
- `$XDSSubmissionSetAuthorPerson`

Ob und inwieweit unscharfe Ergebnisse für diese Parameter zurückgegeben werden, kann das PS nicht steuern.

### 5.2.2.2 Umsetzung

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

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

**Tabelle 21: Tab\_ILF\_ePA\_FindDocuments\_Pflichtfelder**

Parametername	Attribut	Befüllung
\$XDSDocumentEntryPatientId	XDSDocumentEntry.patientId	patientID
\$XDSDocumentEntryStatus	XDSDocumentEntry.availabilityStatus	urn:oasis:names:tc:ebxml-regrep:StatusType:Approved

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].

Die Aktivitäten des Anwendungsfalles *Dokumente suchen* sind:

**Vorbedingung:**

- Ermittelter `RecordIdentifier`
- `ExpirationDate` der Aktenzugriffsberechtigung noch nicht abgelaufen

**Auslöser:**

- Nutzerinteraktion
- anlassbezogene Suche

**Aktivitäten:**

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

**Resultat:**

- Ergebnismeldung
- Dokumenten-UUID-Liste (`XDSDocumentEntry_uniqueId`)

### 5.2.2.3 Nutzung

#### A\_14907 - Setzen des Message-Identifiers im Dokumentensuche-Request

Die WS-Requests der Dokumentensuche werden als `AdhocQuery` mit der Stored Query ID aus [ITI-18#3.18.4.1.2.4] an die ePA-Aktensysteme versendet. Dabei MUSS das PS die `wsa:MessageID` als `UUID` gemäß `PHR_Common.xsd` im SOAP-Header des Requests setzen. [≤]

#### Beispiel 5: Bsp\_ILF\_ePA\_Request\_AdhocQuery

```
<query:AdhocQueryRequest xmlns="urn:ihe:iti:xds-b:2007"
xmlns:query="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0"
xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0">
  <query:ResponseOption returnComposedObjects="true"
  returnType="LeafClass"/>
  <rim:AdhocQuery home="urn:oid:1.2.276.0.76.3.1.405"
  id="urn:uuid:14d4debf-8f97-4251-9a74-a90016b0af0d">
    <rim:Slot name="$XSDDocumentEntryPatientId">
      <rim:ValueList>
        <rim:Value>'X110473550^^^&1.2.276.0.76.4.8&ISO'</rim:Value>
      </rim:ValueList>
    </rim:Slot>
    <rim:Slot name="$XSDDocumentEntryStatus">
      <rim:ValueList>
        <rim:Value>('urn:oasis:names:tc:ebxml-
        regrep:StatusType:Approved')</rim:Value>
      </rim:ValueList>
    </rim:Slot>
  </rim:AdhocQuery>
</query:AdhocQueryRequest>
```

Das PS soll Stored Query IDs der `Tab_ILF_ePA_StoredQueries` gemäß [ITI-18#3.18.4.1.2.4] verwenden.

**Tabelle 22: Tab\_ILF\_ePA\_StoredQueries**

Stored Queries	Implementierungshinweis (beispielhaft)
FindDocuments	Query verwendet id des <code>AdhocQuery</code> -Elements, weil nur zu einem einzelnen Versicherten aus ihrer lokalen Patientenakte der Query durchgeführt wird. Für die Suche nach Arztbriefen allgemein: Angabe von <code>classCode=BRI</code> . Für die Suche speziell nach Arztbriefen gemäß Kap. 6.3.3: Angabe von <code>formatCode=urn:gematik:ig:Arztbrief:r3.1</code> .
FindSubmissionSets	<code>\$XDSSubmissionSetSubmissionTimeFrom</code> und <code>\$XDSSubmissionSetSubmissionTimeTo</code> schränken einen Zeitraum ein, in dem Ergebnisse der <code>SubmissionSet</code> -Suche hochgeladen wurden.



	Nutzbar für eine Delta-Suche in der Benachrichtigungsverwaltung: Es wird nach aktuell eingestellten SubmissionSets gesucht.
FindDocumentsByReferenceID	Semantisch identisch zum FindDocuments Stored Query
GetSubmissionSets	Parameter \$uuid mit XSDDocumentEntry.entryUUID ermittelt den SubmissionSet zu einem Dokument, z.B. zu einem eArztbrief, um verknüpfte Dokumente zu finden.
GetSubmissionSetsAndContents	Unter Angabe z.B. des formatCode für den eArztbrief werden DocumentEntries gefunden, die zum selben SubmissionSet eine HasMember Association aufweisen.
GetAll	Für die Benachrichtigungsverwaltung (Kap. 5.4.1) können Metadaten aller Dokumente einer Akte erhalten werden, für die eine Zugriffsberechtigung besteht.
GetDocuments	\$homeCommunityId erforderlich
FindFolders	

### **A\_15088-01 - LE-Dokumente suchen**

Das PS SOLL mittels RegistryStoredQuery

über SubmissionSet.authorPerson Dokumente herausfiltern können, die von Leistungserbringern eingestellt wurden.

[<=]

Beispiel 6: Bsp\_ILF\_ePA\_Request\_getDocuments

```
<soapenv:Body>
  <query:AdhocQueryRequest xmlns:query="urn:oasis:names:tc:ebxml-
regrep:xsd:query:3.0">
    <query:ResponseOption returnComposedObjects="true"
returnType="LeafClass"/>
    <AdhocQuery xmlns="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0"
id="urn:uuid:5c4f972b-d56b-40ac-a5fc-c8ca9b40b9d4">
      <Slot name="$MetadataLevel">
        <ValueList>
          <Value>
            1
          </Value>
        </ValueList>
      </Slot>
      <Slot name="$XDSDocumentEntryEntryUUID">
        <ValueList>
          <Value>
            ('urn:uuid:744e9ad5-bc2d-453d-b20e-a91c6e33eaf1')
          </Value>
        </ValueList>
      </Slot>
    </AdhocQuery>
  </query:AdhocQueryRequest>
</soapenv:Body>
```

Beispiel 7: Bsp\_ILF\_ePA\_Response\_getDocuments

```
<S:Envelope xmlns:S="http://www.w3.org/2003/05/soap-envelope">
  <S:Header>
    ...
  </S:Header>
  <S:Body>
    <query:AdhocQueryResponse xmlns:query="urn:oasis:names:tc:ebxml-
regrep:xsd:query:3.0" status="urn:oasis:names:tc:ebxml-
regrep:ResponseStatusType:Success">
      <rim:RegistryObjectList xmlns:rim="urn:oasis:names:tc:ebxml-
regrep:xsd:rim:3.0">
        <rim:ExtrinsicObject id="urn:uuid:744e9ad5-bc2d-453d-b20e-
a91c6e33eaf1" mimeType="application/pdf" objectType="urn:uuid:7edca82f-
054d-47f2-a032-9b2a5b5186c1" lid="urn:uuid:744e9ad5-bc2d-453d-b20e-
a91c6e33eaf1" status="urn:oasis:names:tc:ebxml-
regrep:StatusType:Approved">
          (...)

          <rim:Slot name="sourcePatientId">
            <rim:ValueList>
              <rim:Value>
                89765a87b^^^&1.2.3.4.5&ISO
              </rim:Value>
            </rim:ValueList>
          </rim:Slot>

          (...)

          <rim:ExternalIdentifier identificationScheme="urn:uuid:2e82c1f6-a085-
4c72-9da3-8640a32e42ab" value="1.2.42.20180828094414.4"
objectType="urn:oasis:names:tc:ebxml-
regrep:ObjectType:RegistryObject:ExternalIdentifier" id="urn:uuid:96e39549-
887b-444d-9e10-a58708d63e71" registryObject="urn:uuid:744e9ad5-bc2d-
453d-b20e-a91c6e33eaf1">
            <rim:Name>
              <rim:LocalizedString value="XSDDocumentEntry.uniqueId"/>
            </rim:Name>
            <rim:VersionInfo versionName="-1"/>
          </rim:ExternalIdentifier>

        </rim:ExtrinsicObject>
      </rim:RegistryObjectList>
    </query:AdhocQueryResponse>
  </S:Body>
</S:Envelope>
```

Tabelle 23: 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 patientdoc, kann eine Suche mittels FindFolders auf Dokumentenkategorie erfolgen, die in Folder.Codelist angegeben sind.

### Filtern

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\_15087 - Identifizierung von LE-Dokumente in Ergebnismengen**

Eine metadatengestützte Sortierfunktion unterstützt das Filtern von Dokumenten. Das PS SOLL eine Ergebnismenge unter Identifizierung der LE-Dokumente einschränken können.[<=]

## 5.2.3 Dokumente laden

*Dr. Weber erkennt anhand der Metadaten aus seiner Dokumentensuche, dass in der Akte von Frau Gundlach ein Arztbrief im eArztbrief-Format enthalten ist. Das PVS zeigt Dr. Weber an, dass dieses Dokumentenformat strukturiert in die lokale Patientenakte übernommen und dort verarbeitet werden kann. Dr. Weber wählt dieses Dokument aus den Suchergebnissen aus, lässt es sich anzeigen und speichert es in seine lokale Patientenakte.*

Zur Umsetzung des Anwendungsfalles *Dokumente durch einen Leistungserbringer anzeigen* aus [gemSysL\_ePA#3.7.9, UC 4.9 - Dokumente durch einen Leistungserbringer anzeigen] wird Retrieve Document Set [ITI-43] profiliert.

#### **A\_15651 - Funktionsmerkmal Dokumente laden**

Das PS MUSS es dem Leistungserbringer ermöglichen, ePA-Dokumente aus der Akte in das PS laden zu können. Dafür MUSS das PS die Konnektorschnittstellenoperation `RetrieveDocumentSet` verwenden.[<=]

**Tabelle 24: Tab\_ILF\_ePA\_IHE-Profilierung\_ITI43**

IHE-Konzept	Wert	Referenz
PS als IHE Akteur	Document Consumer	Retrieve Document Set [ITI-43]
Format Ergebnis-Dokument(e)	XOP-InfoSet	[IHE-ITI-TF2x#Appendix v.8]

Das Fachmodul stellt kein Integrated Document Source/Repository und keine On-Demand Document Source dar.

Das Anzeigen von Dokumenten beinhaltet auch das Anzeigen der Metadaten des Dokumentes.

Das Anzeigen ist nicht zwingend mit dem persistenten Abspeichern des Dokumentes verbunden.

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.

Es lassen sich nur solche Dokumente laden, für welche die LEI über eine Berechtigung verfügt.

### 5.2.3.1 Schnittstelle

Das Fachmodul ePA bietet zur logischen Schnittstelle `I_PHR_Management` am Webservice `PHR_Service` (analog IHE-Dienst `DocumentRepository`) die Operation `RetrieveDocumentSet` an, die in ihrem Außenverhalten der Schnittstellendefinition des [ITI-43] folgt und die Rolle eines IHE ITI `DocumentRepository` gegenüber dem PS übernimmt.

**Tabelle 25: Tab\_ILF\_ePA\_Operation\_Dokumente\_anzeigen**

Operationsname	DocumentRepository_RetrieveDocumentSet [gemSpec_FM_ePA# 7.1.1.3]	
Aufrufparameter	Name	Implementierung
	RetrieveDocumentSetRequest	[ITI-43#3.43.4.1]
Rückgabeparameter	Name	Implementierung
	RetrieveDocumentSetResponse	[ITI-43#3.43.4.2]

### 5.2.3.2 Umsetzung

Die Aktivitäten des Anwendungsfalles Dokumente anzeigen sind:

**Vorbedingung:**

- Ermittelter `RecordIdentifier`
- `ExpirationDate` der Aktenzugriffsberechtigung noch nicht abgelaufen
- `XSDDocumentEntry_uniqueId (DocumentEntry.uniqueId)` bekannt

**Auslöser:**

- Fachliches Erfordernis

- Nutzerinteraktion

**Aktivitäten:**

- Auswahl `RecordIdentifier`, ggf. anhand von Dokument-Metadaten
- Auswahl `XSDDocumentEntry_uniqueId`
- Generierung und Versand der Nachricht
- Dekodierung des empfangenen Dokumentes (Base64 oder XOP)
- Anzeige des angefragten Dokumentes oder der Dokumentenmenge
- Auswertung des Ergebnisses

**Resultat:**

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

**Beispiel 8: Bsp\_ILF\_ePA\_RetrieveDocumentSetRequest**

```
<RetrieveDocumentSetRequest xmlns="urn:ihe:iti:xds-b:2007">
  <DocumentRequest xmlns="urn:ihe:iti:xds-b:2007">
    <HomeCommunityId>urn:oid:1.2.276.0.76.3.1.315.3.2.1.1</HomeCommunity
    Id>
    <RepositoryUniqueId>1.2.276.0.76.3.1.315.3.2.1.1</RepositoryUniqueId>
    <DocumentUniqueId>1.2.840.113556.1.8000.2554.17930.51373.54354.2004
    0.33122.16728266.12168687</DocumentUniqueId>
  </DocumentRequest>
</RetrieveDocumentSetRequest>
```

**Beispiel 9: Bsp\_ILF\_ePA\_RetrieveDocumentSetResponse**

```
<ns9:RetrieveDocumentSetResponse xmlns:ns9="urn:ihe:iti:xds-b:2007"
xmlns:ns8="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0"
xmlns:ns7="urn:oasis:names:tc:ebxml-regrep:xsd:rsm:3.0"
xmlns:ns6="http://ws.gematik.de/conn/ConnectorContext/v2.0"
xmlns:ns5="http://ws.gematik.de/conn/phrs/PHRManagementService/v1.3"
xmlns:ns4="http://ws.gematik.de/fa/phr/v1.1"
xmlns:ns3="http://ws.gematik.de/tel/error/v2.0"
xmlns:ns2="http://ws.gematik.de/conn/ConnectorCommon/v5.0"
xmlns:ns11="urn:oasis:names:tc:ebxml-regrep:xsd:lcm:3.0"
xmlns:ns10="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0">
  <ns8:RegistryResponse status="urn:oasis:names:tc:ebxml-
  regrep:ResponseStatusType:Success"/>
  <ns9:DocumentResponse>
    <ns9:HomeCommunityId>urn:oid:1.2.276.0.76.3.1.315.3.2.1.1</ns9:HomeCo
    mmunityId>
    <ns9:RepositoryUniqueId>1.2.276.0.76.3.1.315.3.2.1.1</ns9:RepositoryUniq
    ueId>
    <ns9:DocumentUniqueId>1.2.840.113556.1.8000.2554.17930.51373.54354.2
    0040.33122.16728266.12168687</ns9:DocumentUniqueId>
    <ns9:mimeType>application/xml</ns9:mimeType>
    <ns9:Document>
      <xop:Include href="cid:85130d97-672a-4000-b09c-43a4ac630403%40null"
```

```
xmlns:xop="http://www.w3.org/2004/08/xop/include"/>
</ns9:Document>
</ns9:DocumentResponse>
</ns9:RetrieveDocumentSetResponse>
```

### 5.2.3.3 Nutzung

Die Retrieve Document Set Request Message muss mindestens eine `DocumentUniqueID` enthalten.

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

#### **A\_16519 - Größenbeschränkung beim Laden von Dokumentensätzen**

Das *Dokumente Laden* unterliegt der Beschränkung der Gesamtgröße einer Dokumentenmenge, die mit einem einzelnen Aufruf geladen werden können. Das PS MUSS beachten, dass die in den Dokument-Metadaten `size` aufgeführte Größe der Dokumente, die in der Response der Nachricht zu erwarten sind, in Summe 250 MB nicht überschreiten darf, um eine Fehlermeldung des Fachmodules oder des Aktensystems zuverlässig zu vermeiden. [`<=`]

Dokumente werden in das ePA-Aktensystem Ende-zu-Ende verschlüsselt eingestellt. Dadurch können die Dokumente nicht an zentraler Stelle auf mögliche Schadsoftware geprüft werden. Eine Absicherung gegen mögliche Schadsoftware in heruntergeladenen Dokumenten muss im Primärsystem erfolgen.

#### **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 Inhalt des heruntergeladenen Dokumentes nicht mit dem angegebene Dokumententyp in der Metadaten überein stimmen;
- das Format oder Inhalt des heruntergeladenen Dokumentes nicht den zulässigen Dokumententypen gemäß `Tab_ILF_ePA_Dokumentenformate` 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\_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. [ $\leq$ ]

#### **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. [ $\leq$ ]

#### **A\_16196 - Verarbeitung strukturierter Inhalte**

Das PS SOLL nach Möglichkeit in der Lage sein, aus ePA-Dokumenten, deren Inhalte strukturiert vorliegen, die strukturierten Inhalte in die Primärdokumentation des Versicherten zu übernehmen. [ $\leq$ ]

### **5.2.4 Dokumente löschen**

*Dr. Weber erstellt einen neuen Notfalldatensatz für Frau Gundlach und löscht in Absprache mit ihr den alten NFD aus ihrer Akte, um den aktualisierten Notfalldatensatz in die Akte einzustellen. Frau Gundlach hat kein Interesse daran, überholte Versionen ihrer Notfalldaten in der ePA zu archivieren.*

Zur Umsetzung des Anwendungsfalles *Dokumente durch einen Leistungserbringer löschen* aus [gemSysL\_ePA#3.7.7, UC 4.7 - Dokumente durch einen Leistungserbringer löschen] wird Remove Metadata [ITI-62] profiliert.

#### **A\_14247-04 - Funktionsmerkmal Dokumente Löschen**

Das PS MUSS es dem LE ermöglichen, dem Wunsch des Versicherten nach Löschung von Dokumenten entsprechen zu können. Dafür MUSS das PS die Konnektorschnittstellenoperation `RemoveMetadata` verwenden. Technische Dokumente der ePA (Policy-Dateien) können nicht vom LE gelöscht werden. [ $\leq$ ]

Das Löschen eines Dokumentes aus einer ePA wird als ein strukturierter Anwendungsfall realisiert, dem unmittelbar ein Suchen des Dokumentes vorhergeht, so dass vom Fachmodul eine Aktensession eröffnet wurde, die vom Löschen nachgenutzt wird.

**Tabelle 26: Tab\_ILF\_ePA\_IHE-Profilierung\_ITI86**

IHE-Konzept	Wert	Referenz
PS als IHE Akteur	Document Administrator	Remove Metadata [ITI-62]

Ein LE kann alle Dokumente in Rücksprache mit dem Versicherten löschen, für die er Zugriffsrechte gemäß Tab\_ILF\_ePA\_Zugriffsberechtigungen erhalten hat.



Der Aktenanbieter löscht mit den Dokumenten auch die Metadaten des Dokumentes.

Für das nach der Löschung des Dokumentes in der ePA gegebenenfalls in der Primärdokumentation des Leistungserbringers verbleibende Dokument sind die in Kap. 7.1 aufgeführten Empfehlungen zur Archivierung zu beachten.

Das direkte Löschen von Ordnern für den Versicherten ist keine UseCase für das PS.

#### **5.2.4.1 Schnittstelle**

Das Fachmodul ePA bietet zur logischen Schnittstelle `I_PHR_Management` am Webservice `PHR_Service` (analog IHE-Dienst `DocumentRegistry`) die Operation `RemoveMetadata` an, die in ihrem Außenverhalten der Schnittstellendefinition des [ITI-62] folgt und die Rolle einer IHE `DocumentAdministrator` gegenüber dem PS übernimmt.

**Tabelle 27: Tab\_ILF\_ePA\_Operation\_Dokumente\_löschen**

Operationsname	DocumentRegistry_RemoveMetadata [gemSpec_FM_ePA#7.1.1.6]	
Aufrufparameter	Name	Implementierung
	RemoveObjectsRequest	[IHE-ITI-RMD#3.62.4.1]
Rückgabeparameter	Name	Implementierung
	RegistryResponse	[IHE-ITI-RMD#3.62.4.2]

#### **5.2.4.2 Umsetzung**

Die Aktivitäten des Anwendungsfalles Dokumente löschen sind:

##### **Vorbedingung:**

- Ermittelter `RecordIdentifier`
- `ExpirationDate` der Aktenzugriffsberechtigung noch nicht abgelaufen
- Absprache zwischen LE und Versicherten zur Löschung liegt vor
- Die zu löschenden Dokumente innerhalb einer Document-Request-Liste anhand ihrer `XSDDocumentEntry.entryUUID`

##### **Auslöser:**

- Nutzerinteraktion

##### **Aktivitäten:**

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

**Resultat:**

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

### 5.2.4.3 Nutzung

Der RMD-Request MUSS enthalten:

- Einen Content-Type HTTP header mit action  
Parameterwert "urn:ihe:iti:2010:DeleteDocumentSet"
- Ein SOAP element <wsa:Action/> mit dem Wert  
"urn:ihe:iti:2010:DeleteDocumentSet"
- Ein SOAP element <soap12:Body/> mit dem Wert  
"<lcm:RemoveObjectsRequest>", der wiederum das Element <rim:ObjectRefList>  
enthält.
- <rim:ObjectRefList> MUSS für jedes zu löschende Objekt das  
Element<rim:ObjectRef> enthalten, in dessen Attribut "id" die  
DocumentEntry.entryUUID des zu löschende Objekt anzugeben ist

## 5.2.5 Artefakte

### 5.2.5.1 Namensräume

Tabelle 28: 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	<a href="http://docs.oasis-open.org/wsfed/federation/200706">http://docs.oasis-open.org/wsfed/federation/200706</a>
wsp	<a href="http://schemas.xmlsoap.org/ws/2004/09/policy">http://schemas.xmlsoap.org/ws/2004/09/policy</a>

wsa	<a href="http://www.w3.org/2005/08/addressing">http://www.w3.org/2005/08/addressing</a>
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	<a href="http://www.w3.org/2003/05/soap-envelope">http://www.w3.org/2003/05/soap-envelope</a>

### 5.2.5.2 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.

### 5.2.6 Testunterstützung

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

## 5.3 Protokolle und Benachrichtigungen

### 5.3.1 Benachrichtigungen erhalten

*Frau Gundlach hat Herrn Dr. Weber angekündigt, sie werde ihm in Kürze eine Zugriffsberechtigung von ihrem ePA-Frontend des Versicherten aus erteilen (ihre eGK führte sie für die Ad-hoc-Berechtigung nicht mit sich). Am folgenden Tag findet sie am Frontend des Versicherten ihren Hausarzt Dr. Weber über den Verzeichnisdienst und erteilt ihm eine Berechtigung für einen 7-Tage-Zugriff (Default-Zeitraum) auf ihre ePA. Ein Mitarbeiter von Dr. Weber öffnet die Primärakte von Frau Gundlach und erhält dabei die Benachrichtigung, dass Dr. Weber eine Zugriffsberechtigung erhalten hat und dass der Facharzt, zu dem er Frau Gundlach überwiesen hatte, einen eArztbrief in die Patientenakte eingestellt hat.*

Zur Umsetzung des UseCases "Benachrichtigungen durch einen LE verwalten" aus [gemSysL\_ePA#3.8.1] gibt es keine dedizierte Konnektorschnittstelle, auch nicht zur dedizierten Abfrage der Zugriffsrechte, über die ein LE verfügt. Stattdessen setzt sich das

Funktionsmerkmal aus einer Reihe von Informationsquellen zusammen, die gesamthaft eine zuverlässige Informationsgrundlage bieten können, die jedoch keine Vollständigkeit beanspruchen kann.

Die Benachrichtigungsverwaltung kann aus dem Vergleich der Werte des Zugriffsberechtigungsstatus und der Info-Quellen einen Vergleich über Änderungen ziehen und über diese Änderungen den LE geeignet informieren.

Benachrichtigungen über Änderungen an der ePA eines Versicherten können aus folgenden Quellen stammen:

**Tabelle 29: Tab\_ILF\_ePA\_Benachrichtigungsquellen**

Kürzel	Beschreibung	Verweis
Quelle_Ad-hoc	Ausstellen von Ad-hoc-Berechtigungen zu einem Versicherten	Kap. 5.1.3
Quelle_GetAuthorizationList	Aufruf der Operation <code>GetAuthorizationList()</code>	Kap. 5.3.1.2
Quelle_getAll	Register Stored Query <code>GetAll</code> in <i>Dokumente suchen</i>	Kap. 5.2.2
Quelle_Event	Info/Event im Systeminformationsdienst	Kap. 5.3.1.3
Quelle_Fehler	Spezielle Fehler melden den Entzug einer Berechtigung	Kap. 5.3.1.4

Die Dokumentation durchgeführter Ad-hoc-Berechtigungen ergibt kein vollständiges Bild der erteilten Zugriffsberechtigungen, da Zugriffsberechtigungen für die LEI auch vom ePA-Frontend des Versicherten heraus erteilt werden können.

#### **A\_14351 - Benachrichtigung über ePA-Änderungen bei Auswahl des Versicherten**

Falls die Benachrichtigungsfunktion aktiviert ist, MUSS das PS Leistungserbringer (sowie ihre Gehilfen) bei Auswahl einer Ansicht mit Versichertenbezug in Bezug auf diesen Versicherten in folgenden Konstellationen (ein- und abschaltbar, mit Einstellbarkeit der Frequenz der Benachrichtigung) informieren können:

1. bei bestehender Zugriffsberechtigung auf die Akte informieren über:
  - a. neu eingestellte Dokumente (oder aufgrund einer Umklassifizierung neu zugänglich gemachte Dokumente);
  - b. gelöschte Dokumente;
2. bei veränderten Zugriffsrechten informieren über:
  - a. das Endedatum einer Zugriffsberechtigung (sofern bekannt);
  - b. eine neue Berechtigung, die bisher nicht bestand.

**Tabelle 30: Tab\_ILF\_ePA\_Benachrichtigungs\_InfoModell**

Kürzel	Beschreibung	Benachrichtigungsquellen	Datentyp
--------	--------------	--------------------------	----------

Info_Neu_Zugriff	Info über (neu) erhaltene Akten-Zugriffsberechtigungen	Quelle_Ad-hoc, Quelle_GetAuthorizationList, Quelle_getAll, Quelle_Event	RecordIdentifier
Info_Ende_Zugriff	Info über das Ende der Zugriffsberechtigung auf eine Akte (ExpirationDate < heute)	Quelle_Ad-hoc, Quelle_GetAuthorizationList, Quelle_getAll, Quelle_Event, Quelle_Fehler	date
Info_Neu_Doc	Info über neu in eine Akte eingestellte Dokumente	Quelle_getAll, Quelle_Event	DocumentUniqueId
Info_Lösch_Doc	Info über gelöschte Dokumente	Quelle_getAll, Quelle_Fehler	DocumentUniqueId

## **[<=]**

Handlungsanweisungen auf Basis der Informationen von  
Tab\_ILF\_ePA\_Benachrichtigungs\_InfoModell:

- Bei Nutzung der Benachrichtigungsfunktion werden ePA-Daten des Versicherten aktualisiert. Diese Aktualisierung SOLL ausschließlich aus der geöffneten Primärakte eines einzelnen Versicherten heraus erfolgen und nicht als Sammelverarbeitung über mehrere Akten gleichzeitig.
- An der Primärdokumentation eines Versicherten lokal gespeicherte Informationen zum Zugriffsberechtigungsstatus MUSS das PS durch die Benachrichtigungsinformationen aktualisieren.
- Nach Ablauf der Zugriffsberechtigung MUSS die nicht mehr vorliegende Zugriffsberechtigung dem Anwender kenntlich gemacht werden, etwa anhand des ExpirationDate.
- Falls die Benachrichtigungsverwaltung im PS Performance-Probleme verursacht, MUSS die Frequenz der Abfrage der Benachrichtigungsquellen verringert werden oder es müssen Abfragen temporär ganz ausgeschaltet werden.

Das Erhalten von Berechtigung ist die Nachbedingung der Anwendungsfälle "Berechtigung durch einen Versicherten vergeben" aus [gemSysL\_ePA#3.6.1] und "Bestehende Berechtigungen durch einen Versicherten verwalten" [gemSysL\_ePA#3.6.6].

### **5.3.1.1 Info-Quelle ePA-Administration**

Im Rahmen der Ad-hoc-Berechtigung wird der `RecordIdentifier` bekannt, für den eine Zugriffsberechtigung erteilt wird, und das `ExpirationDate` der Zugriffsberechtigung (Quelle\_Ad-hoc). Als alleinige Quelle dieser Informationen ist die Ad-hoc-Berechtigung u.a. deswegen nicht geeignet, weil der Versicherte vom ePA- Frontend des Versicherten ebenfalls Zugriffsberechtigungen erteilen kann.

### **A\_15656 - Nutzung Ad-hoc-Berechtigung Erteilen für die Benachrichtigungsverwaltung**

Das PS MUSS das Funktionsmerkmal *Aktenkonto Aktivieren* nutzen, um für die im Erfolgsfall zu einem `RecordIdentifier` das `ExpirationDate` für die Benachrichtigungsfunktion zu erhalten. [≤]

### 5.3.1.2 Info-Quelle Berechtigungs-Abfrage

Durch Aufruf der Operation `PHRManagementService::GetAuthorizationList` erhält das PS eine Liste sämtlicher zum Zeitpunkt der Abfrage vorliegenden `RecordIdentifier`, auf die die LEI zugriffsberechtigt ist, sowie das jeweilige Ablaufdatum der Zugriffsberechtigung.

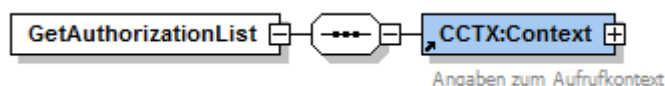
Der LE erhält über die Schnittstelle nicht nur Kenntnis über Zugriffsberechtigungen, die in der Ad-hoc-Autorisierung in seiner LEI erteilt wurden, sondern auch über Zugriffsberechtigungen, die vom ePA-Frontend des Versicherten aus erteilt oder geändert wurden.

Nutzungsvoraussetzungen:

- Eine dem Aufrufkontext zugeordnete SM-B.

**Tabelle 31: Tab\_ILF\_ePA\_Operation\_GetAuthorizationList**

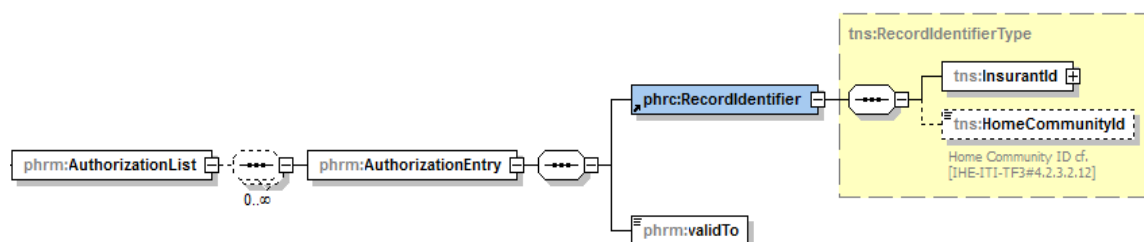
Operationsname	GetAuthorizationList [gemSpec_FM_ePA#7.2.1.5]	
Aufrufparameter	Name	Implementierung
	Context	Aufrufkontext gemäß [ConnectorContext.xsd], s. [gemILF_PS#3.3.1]
Rückgabeparameter	Name	Implementierung
	AuthorizationList	Liste aller Zugriffsberechtigungen für die LEI
	Status	Status nach [gemSpec_Kon#3.5.2] zur Information im PS.



**Abbildung 9: Abb\_ILF\_ePA\_Eingabeparameter\_GetAuthorizationList**

Die `AuthorizationList` als Liste von Tupeln aus `RecordIdentifier` und Ablaufdatum der Zugriffsberechtigung erlaubt die Aktualisierung von `Info_Neu_Zugriff` (über den `RecordIdentifier`) und `Info_End_Zugriff` (über das `validTo-Element`), indem die

Liste der `AuthorizationEntry`-Elemente mit der Liste der bisher schon bekannten Berechtigungen auf Aktenzugriff verglichen wird.



**Abbildung 10: Abb\_ILF\_ePA\_GetAuthorizationListResponse**

### **A\_17143 - Nutzung von GetAuthorizationList für die Benachrichtigungsverwaltung**

Das PS MUSS regelmäßige Änderungsabfragen mit `GetAuthorizationList` initiieren, um die Liste der Tupel aus `RecordIdentifier` und `ExpirationDate` seiner Berechtigungen zu erhalten, mit denen die zur Verwaltung der Benachrichtigungen aktualisiert wird. [`<=`]

### **A\_19008 - Einschränkung der Häufigkeit der Abfrage `getAuthorizationList`**

Das PS DARF den Request `getAuthorizationList` NICHT öfter als einmal in 10 Minuten stellen. Häufigere Abfragen werden mit dem Fehler 7231 abgewiesen. Die Häufigkeit der Abfrage sollte durch den Nutzer konfigurierbar sein, falls sie automatisiert in einem festen Intervall erfolgt.  
[`<=`]

Falls die `AuthorizationList` Versicherten-IDs enthält, die dem Primärsystem nicht bekannt sind, so dass sie keiner Primärdokumentation und keinem bestehenden oder vergangenen Behandlungskontext entsprechen, so soll dieser `RecordIdentifier` verworfen werden. Falls dieser noch unbekannte Versicherte zu einem späteren Zeitpunkt eine neue Primärakte im PS erhält, kann sein `RecordIdentifier` mit `getHomeCommunityID` ermittelt werden. Die Informationen der Tab\_ILF\_ePA\_Benachrichtigungs\_InfoModell werden dann wie bei `Quelle_getAll` beschrieben ermittelt, wo implizit auch `Quelle_Event` ausgewertet werden kann, um die Benachrichtigungsinformationen zu vervollständigen.

Das PS erhält Kenntnis vom Aktenanbieterwechsel eines Versicherten über `GetAuthorizationList`. Sobald ein Versicherter den Aktenanbieter gewechselt hat, wird der alte `RecordIdentifier` (zum alten Aktenanbieter) aus der `AuthorizationEntry`-Liste entfernt. Beim Aktenanbieterwechsel wird die Berechtigung der LEI in die neue Akte transferiert, so dass ein neuer `RecordIdentifier` in der `AuthorizationEntry`-Liste erscheint. Anhand der bekannten `InsurantId` kann das PS feststellen, dass der bekannte Versicherte die Akte gewechselt hat, so dass der in der Primärakte für den Versicherten dokumentierte `RecordIdentifier` im PS aktualisiert werden kann.

### **5.3.1.3 Info-Quelle Dokumentensuche**

Die Dokumentensuche mit `GetAll` (`Quelle_getAll`) liefert die umfangreichsten Informationen für die Benachrichtigungsverwaltung, sollte aber aus Performancegründen nicht zu oft für Änderungsabfragen verwendet werden.

Das PS erhält nur Kenntnis von solchen Dokumenten, für die es berechtigt ist. Bei einer Änderung des Berechtigungstyps aus Tab\_ILF\_ePA\_Zugriffsberechtigungen kann sich auch die Ergebnismenge des Querys ändern.

#### **A\_14708 - Nutzung StoredQuery [ITI-18] für die Benachrichtigungsverwaltung**

Das PS MUSS dem Leistungserbringer die Möglichkeit geben, zur Verwaltung von Benachrichtigungen gemäß dem in Kapitel 5.3.2 profilierten [ITI-18] die StoredQueries `GetALL` oder `GetDocuments` zu verwenden, um regelmäßige Änderungsabfragen zu initiieren.

[<=]

#### **A\_15654 - Keine regelmäßige Änderungsabfrage über sämtliche Versicherten eines LE**

Das PS MUSS seine regelmäßigen Änderungsabfragen beschränken auf Akten zu Primärdokumentationen, in denen Leistungserbringer aktiv arbeiten. Eine regelmäßige Änderungsabfrage mittels StoredQuery über sämtliche Versicherte einer LE-Umgebung DARF NICHT erfolgen. [<=]

### **5.3.1.4 Info-Quelle Systeminformationsdienst**

Wenn das Fachmodul ePA den Leistungserbringer gegenüber der Akte eines Versicherten erfolgreich autorisiert, erzeugt das Fachmodul ePA unter Verwendung des Systeminformationsdienstes des Konnektors ein Event mit dem in [gemSpec\_FM\_ePA#6.5.4] aufgeführten Inhalt ("Zugriffspolicy-Event"). Das Zugriffspolicy-Event gibt Auskunft über den `RecordIdentifier`, für den eine Zugriffsberechtigung erteilt wird, sowie über das `ExpirationDate` (`Quelle_Event`).

Das Zugriffspolicy-Event liefert zum aktuellen Zeitpunkt korrekte Informationen und informiert somit über Aktualisierungen über Zugriffsberechtigungen, auch solche, die der Versicherte am ePA-Frontend des Versicherten vorgenommen hat.

Das Zugriffspolicy-Event wird implizit bei jedem Aktenzugriff am Fachmodul ePA geworfen, der einen Zugriff auf den Berechtigungsschlüssel des LE erfordert, z.B. wie bei `Quelle_getAll` beschrieben.

#### **A\_15655 - Nutzung Systeminformationsdienst für die Benachrichtigungsverwaltung**

Das PS MUSS den Systeminformationsdienst des Konnektors nutzen, um zum Topic `FM_EPA/POLICY_LEI` und der `TelematikID` der Leistungserbringerinstitution das Ablaufdatum der Zugriffsberechtigung für einen `RecordIdentifier` im Element `validTo` für die Benachrichtigungsfunktion zu erhalten. [<=]

### **5.3.1.5 Info-Quelle Fehlermeldung**

#### **A\_15657 - Nutzung von Fehlermeldungen für die Benachrichtigungsverwaltung**

Bei Auftreten der in Tab\_ILF\_ePA\_Infoquelle\_Fehlermeldung aufgelisteten Fehlercodes MUSS das PS die geschilderten Handlungsweisen umsetzen.

**Tabelle 32: Tab\_ILF\_ePA\_Infoquelle\_Fehlermeldung**

<b>Fehlercode</b>	<b>Beschreibung</b>	<b>Handlungsanweisung</b>
7209	Keine Berechtigung für das Aktenkonto vorhanden	Das PS MUSS den Ablauf der Zugriffsberechtigung bzw. die nicht vorliegende Zugriffsberechtigung in der



		betroffenen lokalen Patientenakte für die Benachrichtigungsfunktion kenntlich machen.
InvalidDocumentContent	Dokument oder seine Metadaten sind fehlerhaft, daher ist das Dokument nicht verfügbar	Dokument ist nicht verfügbar und in dieser Hinsicht als gelöscht anzusehen. Als Info über gelöschte Dokumente in der Benachrichtigungsfunktion verwenden.
XDSDocumentUniqueIdError	Dokument zur DokumentID ist nicht verfügbar.	

[<=]

### 5.3.1.6 Umsetzung

Die auch kombinierbaren Aktivitäten des Anwendungsfalles Benachrichtigungen erhalten sind:

#### Vorbedingung:

- Der Versicherte ist der Primärdokumentation im PS mit seiner Versicherten-ID und seinem `RecordIdentifier` bekannt

#### Auslöser:

- Die Primärdokumentation im PS zu dieser Versicherten-ID ist geöffnet
- anlassbezogene Abfrage oder Nutzerinteraktion

#### Aktivitäten:

- Auswerten der Auswahloptionen der Benachrichtigungsverwaltung
- Aufruf der für die Benachrichtigungsverwaltung hinterlegten `StoredQueries` auf die Akte des Versicherten
- Auswertung des Ergebnisses und ggf. Aktualisieren geänderter Werte in der Primärdokumentation

#### Resultat:

- Die aktualisierten Benachrichtigungsinformationen liegen zur Anzeige vor

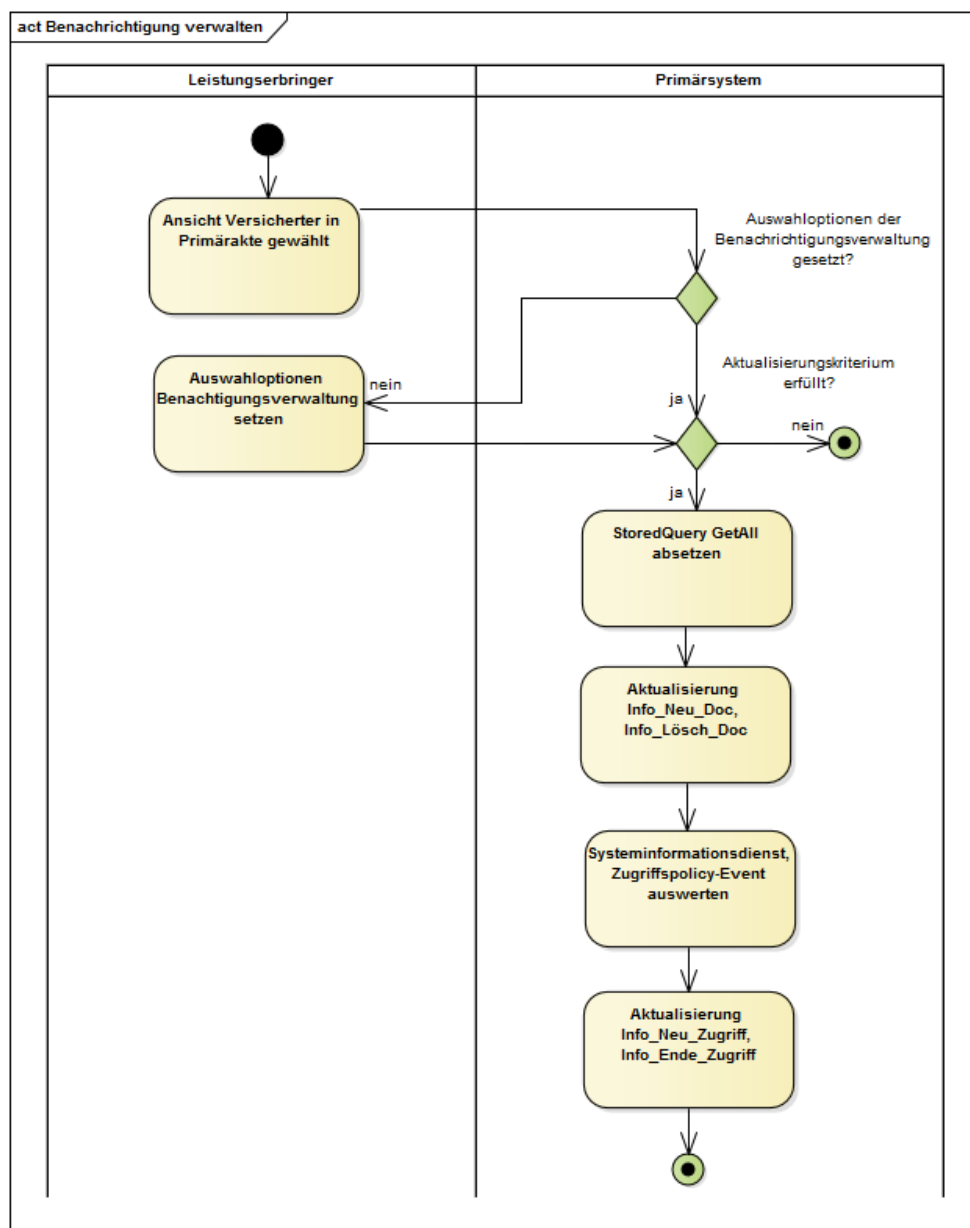


Abbildung 11: Abb\_ILF\_ePA\_Benachrichtigungen\_GetAll\_mit\_Zugriffspolicy-Event

### 5.3.1.7 Nutzung

#### A\_14659 - Speicherung RecordIdentifier in der lokalen Primärdokumentation des PS

Das PS MUSS den RecordIdentifier an der lokalen Patientenakte (Primärdokumentation) persistent speichern, falls eine neu vergebene Berechtigung für den LE ermittelt wurde. [ $\leq$ ]

#### A\_15100 - Auswahloptionen der Benachrichtigungsverwaltung

Das PS SOLL dem LE Auswahloptionen für die Benachrichtigungsverwaltung anbieten. [ $\leq$ ]

Der `StoredQuery GetDocuments` liefert aktuelle Metadaten für Dokumente, auf die ein LE zugriffsberechtigt ist. Durch Nutzung von `GetALL` [ITI-18#3.18.4.1.2.3.7.4] werden die Metadaten aller `XDSSubmissionSets` und `XSDocumentEntries` eines Versicherten in einer Akte erfragt.

Suchstrategien aus der Schnittstelle `Registry Stored Query` können `Info_Neu_Zugriff` und `Info_Ende_Zugriff` aktualisieren helfen, beispielsweise:

- Benachrichtigungen über durch andere Akteure hinzugefügte Dokumente in einer Akte ab einem Stichtag
- Ermitteln von Änderungen durch andere Akteure an Dokumenten, die ein LE selbst eingestellt hat

Die Suche erfolgt auf den Metadaten von Dokumenten, nicht auf den Dokumenteninhalten.

## 5.3.2 Übertragungsprotokolle speichern

*Das Primärsystem von Dr. Weber speichert die Übertragungsprotokolle zwischen dem Primärsystem und dem Konnektor, die darüber Auskunft geben, welche Aktenzugriffe er auf Frau Gundlachs ePA vollzogen hat.*

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, nicht jedoch des Fachmoduls ePA oder anderer Komponenten der TI. 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 Fachmodul ePA des Konnektors speichern, durchsuchbar und einsehbar machen. [ $\leq$ ]

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

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

Details zur Nutzung der Übertragungsprotokolle obliegen dem PS.

## 5.4 Status- und Fehlermeldungen

### 5.4.1 Statusinformationen

#### **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. [ $\leq$ ]

**Tabelle 33: Tab\_ILF\_ePA\_ErrorSeverity**

Wert	Beschreibung	Erläuterung	Beispiel Anzeigetext
W	Warning	Transaktion erfolgreich, jedoch gibt es Abweichungen	7402: Das Aktenkonto ist bereits eingerichtet
E	Error	Transaktion gescheitert	7409: Das Aktenkonto wurde aktiviert, aber die Wiederherstellungsschlüssel konnten nicht am Aktensystem hinterlegt werden.

[IHE-ITT-TF3] definiert, insbes. Table 4.2.4.2-3 und Table 4.2.4.2-4.

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

**Tabelle 34: Tab\_ILF\_ePA\_IHE\_Success\_and\_Error\_Reporting**

Wert	Beschreibung	Erläuterung	Beispiel Anzeigetext
urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success	[IHE-ITT-TF3]#Table 4.2.4.2-1, 4.2.4.2-3, 4.2.4.2-4	Transaktion erfolgreich	Transaktion erfolgreich
urn:ihe:iti:2007:ResponseStatusType:Partial Success	[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.
--	---	-------------------------	---

## 5.4.2 Fehlerbehandlung

Auftretende Fehlertypen unterscheiden sich je nach Architekturebene:

- `gematik-SOAP-Faults` bei Fehlern auf Transportebene mit `TelematikError` auf Anwendungsebene außerhalb des Dokumentenmanagements:
  - Fehler bei Abbruch der Verarbeitung
  - Error-Elemente als Teil der Status-Elemente bei abgeschlossener Verarbeitung
- Fehler auf Ebene des Dokumentenmanagements und der Aktenermittlung

**Tabelle 35: Tab\_ILF\_ePA\_DifferenzFehlerhandling**

Aspekt	TelematikError	IHE-Error
Fehlercodes	als Nummer	als String mit Kurzbeschreibung
Fehlerlisten	Fehler als Einzelobjekte ohne Trace	<code>RegistryErrorList</code>
Kritikalität Warning	<code>GERROR:Severity = "Warning"</code>	<code>RegistryErrorList.highestSeverity="Warning"</code>
Kritikalität Error	<code>GERROR:Severity = "Error", "Fatal"</code>	<code>RegistryErrorList.highestSeverity="Error"</code>
SOAP-Fehlertyp	SOAP 1.1	SOAP 1.2

### A\_14179 - Verständliche Fehlermeldung

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

Der Stacktrace der Fehler wird nicht an das PS weitergegeben.

#### 5.4.2.1 TelematikError

Im Falle von Nicht-IHE-Fehlern erhält das PS vom Fachmodul ePA einen Fehler gemäß [gemSpec\_OM#3.2.3], das ein einzelnes `GERROR:Trace`-Element enthält, das in der

GERROR-Struktur im Element GERROR:Trace einen von der gematik spezifizierten Fehler enthält.

Es gibt keinen Fehlertrace bei SOAP-Fehlern. Die Fehlerbehandlung durch das PS MUSS auf Basis der Fehlerstruktur erfolgen. Herstellerspezifische ePA-SOAP-Fehler sind nicht zulässig. Anforderungen an das PS zum Fehlerhandling bei SOAP-Fehlern finden sich in [gemILF\_PS#6].

Die vom FM geworfenen Fehler sind gelistet in Tab\_ILF\_ePA\_Fehlermeldungen des Fachmoduls ePA.

Daneben kann es Fehler des Basiskonnektors geben gemäß [gemSpec\_Kon], s. Übersicht in [gemILF\_PS#6.6]

#### **A\_16205 - Fehlertexte aus dem TelematikError zur Anzeige von Fehlertexten**

Das PS SOLL bei Auftreten eines `TelematikErrors` den `Code` und den `ErrorText` zur Anzeige der Fehlermeldungen verwenden.

[<=]

### **5.4.2.2 IHE-Error**

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

Das Vorhandensein einer Error-List ist prinzipiell vereinbar mit einer teilweise erfolgreichen Verarbeitung. Falls die `ErrorList` nur Warnings enthält (`RegistryError` elements mit `warning severity`, aber ohne `error severity`), kann die Verarbeitung als erfolgreich angesehen werden.

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

#### **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. [≤]

### **5.4.3 Handlungs-Empfehlungen in Fehlerfällen**

#### **A\_15632-02 - Empfehlungen zur Fehlerbehandlung**

Bei Auftreten der in Tab\_ILF\_ePA\_Handlungsanweisung\_im\_Fehlerfall aufgelisteten Fehlercodes SOLL das PS die geschilderten Handlungsweisen unterstützen.

**Tabelle 36: Tab\_ILF\_ePA\_Handlungsanweisung\_im\_Fehlerfall**

<b>Fehler- code</b>	<b>Fehlertext</b>	<b>Handlungsanweisung</b>

7207	PIN Verifikation gescheitert	Das PS soll den LE darüber informieren, dass der Versicherte seine PIN-Eingabe wiederholen soll. Wenn die PIN-Eingabe ein weiteres Mal scheitert, sollte darauf hingewiesen werden, dass nach dem dritten fehlerhaften Versuch die PIN gesperrt wird und nur über die PUK am ePA-Frontend des Versicherten freigeschaltet werden kann.
4063	PIN gesperrt	Das PS soll den LE darüber informieren, dass der Versicherte die PIN mit seiner PUK am ePA-Frontend des Versicherten entsperren soll.
7231	Die Abfrage getAuthorizationList wurde zu häufig gestellt	Das PS soll den Nutzer auffordern, die Anfrage nicht zu häufig zustellen oder den Administrator auffordern, das Anfrage-Intervall zu verlängern.
7403	Das Aktenkonto kann noch nicht verwendet werden.	Das PS soll das Aktenkonto des Versicherten aktivieren (s. Kap. 5.1.2).
7209	Keine Berechtigung für das Aktenkonto vorhanden	Aufruf von <code>getHomeCommunityID</code> zur Prüfung, ob die persistent im PS gespeicherte <code>HomeCommunityID</code> aktualisiert werden muss, weil der Versicherte seinen Aktenanbieter gewechselt hat. Falls bei Aktualisierung der <code>HomeCommunityID</code> die erneut aufgerufene Operation dennoch scheitert, gilt für Anwendungsfälle außer <i>Ad-hoc-Berechtigung erteilen</i> : Das PS soll den Ablauf der Zugriffsberechtigung in der betroffenen lokalen Patientenakte kenntlich machen. Wenn ein ePA-Zugriff ausgeführt werden soll, und der Versicherte ist einverstanden, eine Ad-hoc-Berechtigung auszuführen, soll die Ad-hoc-Berechtigung beim ihm eingeholt werden.
7205	Es konnte kein freigeschaltetes SM-B gefunden werden.	Das PS soll den Konnektoradministrator auffordern zu prüfen, ob eine SM-B im Konnektor konfiguriert ist, diese ggf.

		konfigurieren, freischalten (lassen) und Anwendungsfall wiederholen (lassen).
7401 7403, 7404, 7405	s. Tab_ILF_ePA_Fehlermeldungen des Fachmoduls ePA	Das PS soll den LE darüber informieren, dass der Versicherte den Anwendungsfall zu einem späteren Zeitpunkt wiederholen soll.

[<=]

## 5.4.4 Übersicht möglicher Fehlermeldungen

### 5.4.4.1 Fehlermeldungen aus dem Fachmodul ePA

Das Primärsystem können neben Fehlermeldungen des Basiskonnektors auch solche des Fachmoduls ePA erreichen:

**Tabelle 37: Tab\_ILF\_ePA\_Fehlermeldungen des Fachmoduls ePA**

Code	Fehlertext	Referenz
106	Zertifikat ungültig	[gemSpec_OM#Tab_Gen_Fehler]
114	DF.HCA gesperrt	[gemSpec_OM#Tab_Gen_Fehler]
4000	Syntaxfehler beim Aufruf einer Operation	[gemSpec_Kon#TAB_KON_567]
4008	Karte nicht gesteckt	[gemSpec_Kon#TAB_KON_515]
4063	PIN gesperrt	[gemSpec_Kon#TAB_KON_089], Tab_ILF_ePA_Handlungsanweisung_im_Fehlerfall
4065	PIN transportgeschützt	[gemSpec_Kon#TAB_KON_089]
4093	Karte bereits exklusiv verwendet	[gemSpec_Kon#TAB_KON_824]
7200	Lokalisierung des Aktensystems fehlgeschlagen	
7202	Verbindung zum Aktensystem fehlgeschlagen	
7203	Die gegenseitige Authentisierung von eGK und SMC-B (Card-to-Card-Authentisierung) ist gescheitert.	



		Tab_ILF_ePA_Handlungsanweisung_im_Fehlerfall
7205	Es konnte kein freigeschaltetes SM-B gefunden werden.	Tab_ILF_ePA_Handlungsanweisung_im_Fehlerfall
7206	Prüfung der Zugriffsberechtigung fehlgeschlagen	
7207	PIN-Verifikation gescheitert	Tab_ILF_ePA_Handlungsanweisung_im_Fehlerfall
7209	Keine Berechtigung für das Aktenkonto vorhanden	Tab_ILF_ePA_Handlungsanweisung_im_Fehlerfall
7211	Dokument überschreitet maximal zulässige Größe von 25 MB	
7212	Summe der Dokumente überschreitet maximal zulässige Größe von 250 MB	
7213	Sperrstatus des Zertifikats der eGK nicht ermittelbar	
7214	Das Schlüsselmaterial der Akte entspricht nicht den Sicherheitsanforderungen.	
7215	Fehler im Aktensystem - Die Operation konnte nicht durchgeführt werden.	
7217	Die Operation wurde am Kartenterminal abgebrochen.	
7220	Aktensystem nicht erreichbar	
7290	Die Patientenakte konnte nicht gefunden werden	Operation GetHomeCommunityID
7291	Die Patientenakte konnte nicht eindeutig identifiziert werden.	Operation GetHomeCommunityID

7231	Die Abfrage getAuthorizationList wurde zu häufig gestellt.	Info-Quelle Berechtigungs-Abfrage, Tab_ILF_ePA_Handlungsanweisung_im_Fehlerfall
7400	Fehler - Die Operation konnte nicht durchgeführt werden.	
7401	Operation konnte nicht durchgeführt werden - Akte vorübergehend nicht verfügbar.	Tab_ILF_ePA_Handlungsanweisung_im_Fehlerfall
7402	Das Aktenkonto ist bereits eingrichtet	Operation ActivateAccount
7403	Das Aktenkonto kann noch nicht verwendet werden.	Tab_ILF_ePA_Handlungsanweisung_im_Fehlerfall
7404	Das Aktenkonto existiert nicht (mehr) in diesem ePA- Aktensystem.	Tab_ILF_ePA_Handlungsanweisung_im_Fehlerfall
7405	Das Aktenkonto wurde bei diesem ePA-Aktensystem gekündigt, kann aber aktuell noch benutzt werden.	Tab_ILF_ePA_Handlungsanweisung_im_Fehlerfall
7406	Das Aktenkonto wurde bei diesem ePA-Aktensystem gekündigt und ist nur noch für einen Kontowechsel lesend zugreifbar.	

#### **5.4.4.2 Fehlermeldungen aus dem Aktensystem ePA**

Das Aktensystem kann mindestens die Fehler der Tabelle Tab\_ILF\_ePA\_IHE-Fehlermeldungen\_Aktensystem werfen, die an das PS durchgereicht werden.

**Tabelle 38: Tab\_ILF\_ePA\_IHE-Fehlermeldungen\_Aktensystem**

<b>Code</b>	<b>Hinweis</b>	<b>Referenz</b>
InvalidDocumentContent	Dokument passt nicht zu Metadaten	[IHE-ITI-TF3#4.2.4]

UnresolvedReferenceException	entryUUID kann nicht aufgelöst werden	[IHE-ITI-TF3#4.2.4]
XSDDocumentUniqueIdError	uniqueId kann nicht aufgelöst werden	[IHE-ITI-TF3#4.2.4]
XSDuplicateUniqueIdInRegistry	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]
XSPatientIdDoesNotMatch	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]
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]
XDSStoredQueryMissingParameter	Parameterfehler Stored Query	[IHE-ITI-TF3#4.2.4]
XDSStoredQueryParameterNumber	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.]
MAX_DOC_SIZE_EXCEEDED	Die max. Dokumentengröße wurde überschritten.	Bei Verletzung von A_16197, vgl. auch [gemSpec_Dokumentenverwaltung#Operation Cross-Gateway Document Provide#Technische Fehlermeldungen]
ACCESS_DENIED	Der Zugriff für diese Operation konnte nicht gewährt werden.	Der Nutzer hat nicht die erforderliche Berechtigung für die Operationen der [gemSpec_Dokumentenverwaltung]: <ul style="list-style-type: none"> <li>• Cross-Gateway Document Provide</li> <li>• Cross-Gateway Query</li> <li>• Remove Metadata</li> <li>• Cross-Gateway Retrieve</li> </ul>
MAX_PKG_SIZE_EXCEEDED	Die max. Paketgröße wurde überschritten.	Bei Verletzung von A_16519, vgl. auch [gemSpec_Dokumentenverwaltung#OperationCross-Gateway Retrieve#Technische Fehlermeldungen]

---

## 6 Informationsmodell

---

### 6.1 Metadaten

Beim Einstellen von Dokumenten in die ePA werden die dazu genutzten SubmissionSets und die Dokumente selbst, durch Metadaten angereichert die für Such- und Filterfunktionen nachgenutzt werden können. Metadaten liegen sowohl am SubmissionSet, als auch am ePA-Dokument selbst vor.

Das PS MUSS Metadaten unter Beachtung von [gemSpec\_DM\_ePA] möglichst automatisiert aus den Primärdaten der Versicherten übernehmen und erzeugen, ohne dass eine händische Eingabe von Metadaten zwingend erforderlich ist. Die manuelle Auszeichnung der Werte von Metadaten sollte auf ein Minimum begrenzt werden.

Als Codierung wird UTF-8 verwendet.

#### **A\_14940 - Festlegungen zu Metadaten im Datenmodells der ePA-Dokumente**

Das PS MUSS die Dokumententypen aus [gemSpec\_DM\_ePA#A\_14760] betreffenden Festlegungen zur Verwendung von Metadaten gemäß [gemSpec\_DM\_ePA#3.3] beachten.[<=]

### 6.2 Wertebereiche

Erforderliche Wertebereiche (Value Sets) für ePA-Dokumente werden je nach Festlegung von [gemSpec\_DM\_ePA] in [IHE-ITI-VS] angegeben.

#### **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.

#### **A\_15086-03 - Selbstauskunft der LE-Institution**

Das PS MUSS dem LE die Möglichkeit zur Konfiguration von Metadaten geben, in denen Leistungserbringer ihre LE-Institution und sich selbst als Akteure beschreiben. Diese LE-Selbstbeschreibungen MUSS zur Befüllung der Metadaten automatisiert herangezogen werden können und die in Tabelle Tab\_ILF\_ePA\_Datenfelder\_Selbstauskunft aufgeführten Felder gemäß [gemSpec\_DM\_ePA#A\_14760] umfassen. `SubmissionSet.authorPerson` MUSS mit Werten des Einstellers belegt werden. Für den Fall, dass der LE eigene Dokumente einstellt, MUSS die Selbstauskunft zusätzlich auch für die Belegung von `DocumentEntry.authorPerson` herangezogen werden. Da bei manchen einzustellenden Dokumenten auch mehrere Autoren angegeben werden, MUSS die Selbstauskunft mindestens mehrere Mitarbeiter der eigenen Institution umfassen können. Die Fachrichtung der erstellenden Einrichtung MUSS in der Selbstauskunft im Feld `practiceSettingCode` gespeichert werden mit einem zutreffenden Wert aus [IHE-ITI-VS].

Die Selbstauskunft MUSS einen einzelnen Code aus [Tab\_DM\_112:Codes in ValueSet für

Folder.codeList] setzen, um eine Voreinstellung für die fachrichtungsspezifische ePA-Berechtigung vorzunehmen. Dieser fachrichtungsspezifische Code beschreibt Daten zu Befunden, Diagnosen, durchgeführten und geplanten Therapiemaßnahmen, Früherkennungsuntersuchungen, zu Behandlungsberichten und sonstige untersuchungs- und behandlungsbezogene medizinische Informationen.

**Tabelle 39: Tab\_ILF\_ePA\_Datenfelder\_Selbstauskunft**

Metadatum (Dokumentenmanagement)	Schnittstellenparameter (ePA-Administration)	Mult.
DocumentEntry.authorPerson		[1..*]
DocumentEntry.authorInstitution	OrganizationName	1
DocumentEntry.authorRole		[0..*]
DocumentEntry.authorSpecialty		[0..*]
DocumentEntry.authorTelecommunication		[0..*]
DocumentEntry.healthcareFacilityTypeCode		1
DocumentEntry.practiceSettingCode		[1..*]
DocumentEntry.legalAuthenticator		[0..*]
DocumentEntry.languageCode		[1..*]
Folder.codeList		1

[<=]

### **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 gemäß [gemSpec\_DM#4.1] verkürzten Form zur Auswahl bringen.[<=]

### **A\_16206-02 - Empfehlungen zur sektorspezifischen Reduktion von Auswahllisten**

Beim Einstellen von Dokumenten SOLLEN sektorspezifische Empfehlungen zur Reduktion von Auswahllisten mögliche Werte für die Metadaten `authorRole` und `typeCode` beim Einstellen von Dokumenten gemäß [gemSpec\_DM\_ePA#5.2.3] beachtet werden. [<=]

### **Auslesen von Dokumenten**

Insoweit Metadaten zur Anzeige gebracht werden, muss das PS die Anzeigenamen der Metadaten in eine lesbare Form bringen. Die Anzeige von Metadaten ist insbesondere zu

dem Zwecke des Filterns großer Ergebnismengen erforderlich sowie zur Auswahl der gegebenenfalls herunterzuladenden Dokumente. Zum Filtern über Dokumentenmengen kann es nützlich sein, nicht nur Metadaten der `DocumentEntries`, sondern auch Metadaten der `SubmissionSets` anzuzeigen, um ein Ausblenden bestimmter Suchergebnisse zu ermöglichen.

## 6.3 Dokumentenformate der ePA

### A\_14245 - Unterstützung der Verarbeitung von Dokumentenformaten der ePA durch das PS

Das PS KANN über die Liste gültiger ePA-Formate gemäß [gemSpec\_DM\_ePA#Tab\_DM\_100: Code-System und Codes für XDS `formatCode` der ePA-Fachanwendung hinaus zusätzliche Dokumentenformate gemäß [gemSpec\_DM\_ePA#A\_14760] unterstützen, um sie zu verwalten. [`<=`]

**Tabelle 40: Tab\_ILF\_ePA\_Dokumentenformate (beispielhaft)**

<b>Dokumentenformate</b> <code>DocumentEntry.mimeType</code>	<b>Beispielwerte</b> <code>DocumentEntry.formatCode</code>
application/xml	"urn:gematik:ig:Notfalldatensatz:r3.1"
	"urn:gematik:ig:DatensatzPersoenlicheErklaerungen:r3.1"
	"urn:gematik:ig:Medikationsplan:r3.1"
	"urn:gematik:ig:Arztbrief:r3.1"
application/hl7-v3	„urn:ihe:iti:xds:2017:mimeTypeSufficient“
application/pdf	„urn:ihe:iti:xds:2017:mimeTypeSufficient“
image/jpeg	„urn:ihe:iti:xds:2017:mimeTypeSufficient“
image/tiff	„urn:ihe:iti:xds:2017:mimeTypeSufficient“
text/plain	„urn:ihe:iti:xds:2017:mimeTypeSufficient“
text/rtf	„urn:ihe:iti:xds:2017:mimeTypeSufficient“
application/fhir+xml oder /pkcs7-mime (für nicht signierte oder signierte Einträge)	"urn:gematik:ig:Impfausweis:r4.0"
	"urn:gematik:ig:Mutterpass:r4.0"
	"urn:gematik:ig:Kinderuntersuchungsheft:r4.0"
	"urn:gematik:ig:Zahnbonusheft:r4.0"
	"urn:gematik:ig:Arbeitsunfähigkeitsbescheinigung:r4.0"

application/json+xml	"urn:gematik:ig:VerordnungsdatensatzMedikation:r4.0"
----------------------	--

Falls Word- oder Openoffice-Dokumente in die ePA eingestellt werden sollen, müssen diese Dokumente vor ihrem Upload in ein PDF umgewandelt werden.

Das DPE-XML der eGK ist ein Beispiel eines XML-Dokumentes, dessen Metadaten gemäß [gemSpec\_DM\_ePA] in [IHE-ITI-VS] angereichert werden.

Ein ContentProfile zu einem einzelnen Dokumentenformat bzw. Inhaltstypen eines Dokumentenformates beschreibt die Befüllung der Metadaten im Sinne einer Best Practice zur Vermeidung von Interoperabilitätsproblemen.

Der `DocumentEntry.formatCode` von Dokumenten, bei denen es kein Contentprofile gibt, kann mit dem Wert "urn:ihe:iti:xds:2017:mimeTypeSufficient" automatisch vorbelegt werden. Eine manuelle Auswahl des `formatCodes` soll vermieden werden.

#### **A\_21651 - Verarbeitung strukturierter Dokumente der gesetzlich vorgegebenen Kategorien**

Das Primärsystem MUSS strukturierte Dokumente der Kategorien aus `Tab_DM_Dokumenten Kategorien` in `gemSpec_DM_ePA#A_19388-*` nicht nur anzeigen, sondern auch verarbeiten können, d.h. anlegen und bearbeiten können. Strukturierte Dokumente sind Dokumente, für die in `gemSpec_DM` Strukturdefinitionen aufgeführt werden oder aber Definitionen als Medizinische Informationsobjekte vorliegen. [`<=`]

#### **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`. [`<=`]

### **6.3.1 ContentProfile Notfalldatensatz und Datensatz Persönliche Erklärungen**

Der Notfalldatensatz, der in die ePA eingestellt werden soll, wird vom PS entweder zuvor gemäß [gemILF\_PS\_NFDM#5.1.2] von der eGK gelesen oder er wird gemäß den im XML-Schema des Infomodells NFDM festgelegten Regeln und den darüber hinaus gehenden in [gemSpec\_InfoNFDM] definierten Integritätsregeln erstellt, so dass der NFD gemäß [gemRL\_QES\_NFDM] signiert werden kann.

Ein Datensatz persönliche Erklärungen (DPE), der in die ePA eingestellt werden soll, wird vom PS entweder zuvor gemäß [gemILF\_PS\_NFDM#5.2.2] von der eGK gelesen oder er wird gemäß den im XML-Schema des Infomodells NFDM festgelegten Regeln und den darüber hinaus gehenden in [gemSpec\_InfoNFDM] definierten Integritätsregeln erstellt.

Im `<Icm:SubmitObjectsRequest>` des `<ProvideAndRegisterDocumentSetRequest>` referenziert das `<rim:ExtrinsicObject>` die `<rim:RegistryObjectList>` die ID des angehängten NFD-Objektes bzw. DPE-Objektes.

#### **A\_18690 - DPE-spezifische Metadatenbefüllung**



Das PS KANN die Werte der `SubmissionSet`-Metadaten für den Datensatz persönliche Erklärungen gemäß [gemSpec\_DM\_ePA] für das Dokumentenmanagement der ePA automatisiert befüllen und dabei die DPE-spezifischen Implementierungshinweise aus `Tab_ILF_ePA_Nutzungsvorgaben` für Metadaten NFD/DPE beachten. Datenquellen sind Daten des Einstellers und der DPE der eGK.[<=]

#### **A\_14504 - NFD-spezifische Metadatenbefüllung**

Das PS MUSS die Werte der `SubmissionSet`-Metadaten für den Notfalldatensatz gemäß [gemSpec\_DM\_ePA] für das Dokumentenmanagement der ePA automatisiert befüllen und dabei die NFD-spezifischen Implementierungshinweise aus `Tab_ILF_ePA_Nutzungsvorgaben` für Metadaten NFD/DPE beachten. Datenquellen sind Daten des Einstellers und die NFD der eGK.

**Tabelle 41: Tab\_ILF\_ePA\_Nutzungsvorgaben für Metadaten NFD/DPE**

Metadatum XDS.b	Op t	Nutzungsvorgabe (Wertvorgabe oder Implementierungsanweisung)
<b>Metadatenelement DocumentEntry</b>		
author	R	%
authorPerson	O	<p>Mögliche Quellen:</p> <ul style="list-style-type: none"> <li>NFD signed NFD_Document, darin: ds:X509Certificate.subject.commonName (Nur für NFD)</li> <li><code>SubmissionSet.authorPerson</code>, falls Autor identisch mit Einsteller des Dokumentes</li> </ul>
authorInstitution	O	<code>SubmissionSet.authorInstitution</code> , falls Autor identisch mit Einsteller des Dokumentes
authorRole	O	Einsteller des Dokumentes Verwendung gemäß [IHE-ITI-VS]
authorSpecialty	O	Einsteller des Dokumentes Verwendung gemäß [IHE-ITI-VS]
authorTelecommunication	O	Einsteller des Dokumentes = <code>SubmissionSet.authorTelecommunication</code>
classCode	R	<p>Codesystem, ID=1.2.276.0.76.11.32</p> <ul style="list-style-type: none"> <li>Code= AUS (Nur für NFD)</li> <li>Code=ADM (Nur für DPE)</li> </ul>
creationTime	R	Mögliche Quellen (Mehrfachnutzung möglich):

		<ul style="list-style-type: none"> <li>• Signaturzeitpunkt NFD=NFD signed NFD_Document.SignatureArzt, darin: xades:SigningTime (Nur für NFD)</li> <li>• Aktualisierungszeitpunkt DPE=Persoenliche Erklaerungen/DPE_letzte_Aktualisierung_time (Nur für DPE)</li> <li>• Zeitpunkt des Einstellens = submissionSet.submissionTime</li> </ul>
formatCode	R	Codesystem= 1.3.6.1.4.1.19376.3.276.1.5.6 Code=urn:gematik:ig:Notfalldatensatz:r3.1
healthcareFacilityTypeCode	R	Einsteller des Dokumentes Der Wert MUSS aus [IHE-ITI-VS], Value Set IHEXDShealthcareFacilityTypeCode gewählt werden.
contentType	R	application/xml
practiceSettingCode	R	Einsteller des Dokumentes Der Wert MUSS aus [IHE-ITI-VS], Value Set IHEXDShealthcareFacilityTypeCode gewählt werden.
sourcePatientId	R	NFD signed NFD_Document.Versicherter.Versicherten_ID, falls diese mit der Versicherten-ID der Primärdokumentation übereinstimmt, zur Übernahme gemäß [gemSpec_DM_ePA]#2.1.4.6
title	O	Notfalldatensatz (Nur für NFD) Datensatz persönliche Erklärungen (Nur für DPE)
typeCode	R	Codesystem-ID=1.3.6.1.4.1.19376.3.276.1.5.9 <ul style="list-style-type: none"> <li>• Code=BESC (Nur für NFD)</li> <li>• Code=PATD (Nur für DPE)</li> </ul>
<b>Metadatenelement SubmissionSet</b>		
contentTypeCode	R	Klinische Aktivität, die zum Einstellen des SubmissionSet geführt hat gemäß [IHE-ITI-VS]. Codesystem=1.3.6.1.4.1.19376.3.276.1.5.12 Code=8

[<=]

Der Notfalldatensatz wird im Base64-Format, wie er aus der eGK ausgelesen wird, in das Element <xds:Document> eingefügt, das ein Attribut @id enthält, das dem rim:ExtrinsicObject/@id übereinstimmt.

#### **A\_15058 - Anzeige (Rendering) ContentProfile NFD/DPE**

Das PS MUSS ePA-Daten im ContentProfile NFD/DPE in geeigneter Form zur Anzeige bringen können. Für die Anzeige der Inhaltsdaten SOLL die Anzeigefunktion der Notfalldaten bzw. des DPE nachgenutzt werden, die beim Auslesen der NFD/DPE von der eGK gemäß [gemILF\_PS\_NFDM] verwendet wird, sofern die Anzeigefunktion über die Anwendung NFDM verfügbar ist. [ $\leq$ ]

### **6.3.2 ContentProfile elektronischer Medikationsplan**

Der elektronische Medikationsplan, der in die ePA eingestellt werden soll, wird vom PS entweder zuvor gemäß [gemILF\_PS\_AMTS] von der eGK gelesen oder er wird gemäß den im XML-Schema des Infomodells eMP/AMTS festgelegten Regeln und den darüber hinaus gehenden in [gemSpec\_Info\_AMTS] definierten Integritätsregeln erstellt, so dass der eMP durch das PS gemäß [gemILF\_PS\_AMTS] zum Einstellen des eMP in die ePA vorbereitet ist.

#### **A\_21103 - Einstellen von eMP-Daten inklusive der Einwilligung**

Das PS MUSS dafür Sorge tragen, dass für den elektronischen Medikationsplan der eGK sowohl das XML-Artefakt zum Medikationsplan, als auch das XML-Artefakt zur Einwilligung des Versicherten gemäß [gemSpec\_Info\_AMTS#2.1] in einer aktuellen Fassung in die ePA hochgeladen wird, falls die genannten Artefakte dort fehlen oder nicht in einer aktuellen Version vorliegen. [ $\leq$ ]

#### **A\_21102-01 - eMP-spezifische Metadatenbefüllung**

Das PS MUSS die Werte der Metadaten für den elektronischen Medikationsplan und die zugehörige Einwilligung gemäß [gemSpec\_DM\_ePA] für das Dokumentenmanagement der ePA automatisiert befüllen und dabei die eMP-spezifischen Implementierungshinweise aus Tab\_ILF\_ePA\_Nutzungsvorgaben für Metadaten eMP sowie die ValueSetDefinition aus [IHE-ITI-VS] beachten. Datenquellen sind Daten des Einstellers oder eMP-Daten der eGK. [ $\leq$ ]

**Tabelle 42: Tab\_ILF\_ePA\_Nutzungsvorgaben für Metadaten eMP**

Metadatum XDS.b	Opt	Nutzungsvorgabe (Wertvorgabe oder Implementierungsanweisung)
<b>Metadatenelement DocumentEntry</b>		
classCode	R	Codesystem, ID: 1.2.276.0.76.11.32 Code: PLA
creationTime	R	element MP/A attribute MP/A/@t

healthcareFacilityTypeCode	R	Author des Dokumentes Der Wert MUSS aus [IHE-ITI-VS], Value Set IHEXDShealthcareFacilityTypeCode gewählt werden.
practiceSettingCode	R	Author des Dokumentes Der Wert MUSS aus [IHE-ITI-VS], Value Set practiceSettingCode gewählt werden.
sourcePatientId	R	Mögliche Quellen: KVNR des Versicherten = element MP/P attribute MP/P/@egk
<b>Metadatenelement SubmissionSet</b>		
contentTypeCode	R	Klinische Aktivität, die zum Einstellen des SubmissionSet geführt hat. Codesystem=1.3.6.1.4.1.19376.3.276.1.5.12 Code=8

#### **A\_15059-01 - Anzeige (Rendering) ContentProfile eMP**

Das PS MUSS ePA-Daten im ContentProfile elektronischer Medikationsplan in geeigneter Form zur Anzeige bringen können. Für die Anzeige der Inhaltsdaten SOLL die Anzeigefunktion des Medikationsplans und der zugehörigen Einwilligung nachgenutzt werden, die beim Auslesen des eMP von der eGK gemäß [gemILF\_PS\_AMTS] verwendet wird, sofern die Anzeigefunktion über die Anwendung eMP/AMTS verfügbar ist. [≤]

### **6.3.3 ContentProfile Arztbrief nach § 291f**

Falls ein Arztbrief im Format als HL7 CDA R2-Dokument vorliegt, ohne dass der Arztbrief eine PDF-Darstellung hat, soll er direkt im Format `contentType = application/xml` in der Dokumentenverwaltung der ePA verwaltet werden.

Ein Arztbrief, der als reines PDF-Dokument in die ePA eingestellt werden soll, soll direkt im Format `contentType = application/pdf` in der Dokumentenverwaltung der ePA verwaltet werden.

Der Arztbrief nach § 291f SGB V hat gemäß [Richtlinie eArztbrief] die verpflichtenden Teile PDF-Dokument und CDA-XML (nur der CDA-Header ist verpflichtend). Um diesen Arztbrief in die ePA einzustellen und wieder auszulesen, wird auf das XML-Containerformat `DischargeLetterContainer` (s. Abb\_ILF\_ePA\_eAB-XML-Containerformat aus `PHRManagementService.xsd`) zurückgegriffen.

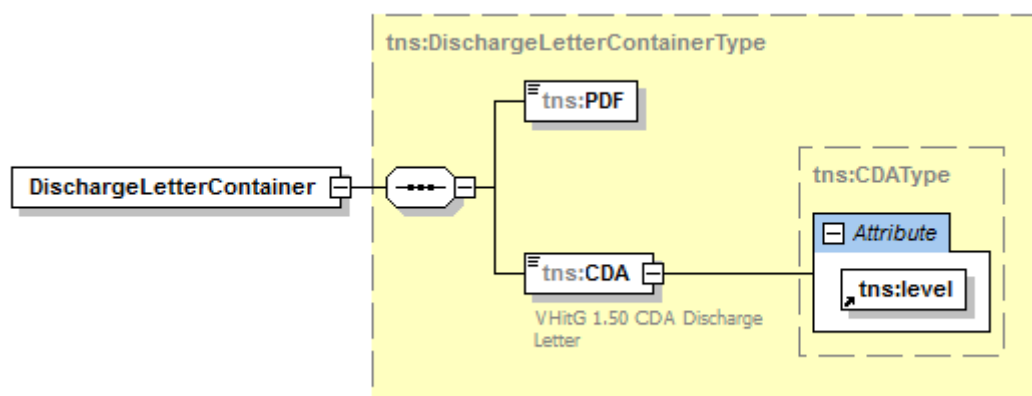


Abbildung 12: Abb\_ILF\_ePA\_eAB-XML-Containerformat

#### A\_14244 - ePA-Einstellung Verarbeitungsvorschrift für Arztbrief nach § 291f mit XML- und PDF-Anteil

Falls der Arztbrief nach § 291f in zwei Anteilen vorliegt (einem CDA-Anteil und einem PDF-Anteil), MUSS das PS beide Teile gemeinsam in eine XML-Container-Struktur gemäß [gemSpec\_DM\_ePA#4.2] einstellen und diesen in eine gemeinsamen SubmissionSet in die ePA einstellen. In diesem SubmissionSet MUSS das Metadatenelement

SubmissionSet.formatCode auf

Codesystem= 1.3.6.1.4.1.19376.3.276.1.5.6 und Code=urn:gematik:ig:Arztbrief :r3.1 gesetzt werden.[<=]

#### A\_14556 - eAB-spezifische Metadatenbefüllung

Das PS MUSS die Werte der SubmissionSet-Metadaten für den elektronischen Arztbrief gemäß [gemSpec\_DM\_ePA] für das Dokumentenmanagement der ePA automatisiert befüllen und dabei die eAB-spezifischen Implementierungshinweise aus Tab\_ILF\_ePA\_Nutzungsvorgaben für Metadaten eAB beachten.

Tabelle 43: Tab\_ILF\_ePA\_Nutzungsvorgaben für Metadaten eAB

Metadatum XDS.b	Opt	Nutzungsvorgabe (Wertvorgabe oder Implementierungsanweisung)
<b>Metadatenelement DocumentEntry</b>		
author	R	%
authorPerson	O	<p>Mögliche Quellen :</p> <ul style="list-style-type: none"> <li>eAB ClinicalDocument.author.person.name, falls eine Person der Autor ist</li> <li>SubmissionSet.authorPerson, falls Autor identisch mit Einsteller des Dokumentes</li> </ul>

authorInstitution	O	<p>Mögliche Quellen :</p> <ul style="list-style-type: none"> <li>eAB <code>ClinicalDocument.author.representedOrganization.name</code>, falls vorhanden</li> <li><code>SubmissionSet.authorInstitution</code>, falls Autor identisch mit Einsteller des Dokumentes</li> </ul>
authorRole	O	Einsteller des Dokumentes Verwendung gemäß [IHE-ITI-VS]
authorSpecialty	O	Einsteller des Dokumentes Verwendung gemäß [IHE-ITI-VS]
authorTelecommunication	O	Telekommunikationsdaten des Autors
classCode	R	Codesystem, ID: 1.2.276.0.76.11.32 Code: BRI
creationTime	R	<p>Mögliche Quellen:</p> <ul style="list-style-type: none"> <li>Erstellzeitpunkt eAB <code>ClinicalDocument.effectiveTime</code></li> <li>Einstellzeitpunkt des Dokumentes = Systemzeit</li> </ul>
formatCode	R	Codesystem= 1.3.6.1.4.1.19376.3.276.1.5.6 Code=urn:gematik:ig:Arztbrief:r3.1
healthcareFacilityTypeCode	R	Der Wert MUSS aus [IHE-ITI-VS], Value Set IHEXDShealthcareFacilityTypeCode gewählt werden. Wert des Einstellers
contentType	R	Für den eAB als XML: application/xml Für den eAB als PDF: application/pdf
practiceSettingCode	R	Der Wert MUSS aus [IHE-ITI-VS], Value Set practiceSettingCode gewählt werden. Wert des Einstellers
sourcePatientId	R	eAB Patient.id, falls vorhanden und eine Versicherten-ID, mit Versicherten-ID des Versicherten abgleichen. Falls die IDs nicht matchen, muss eine Warnung ausgegeben werden.
title	O	eAB <code>ClinicalDocument.title</code>
typeCode	R	Codesystem-ID=1.3.6.1.4.1.19376.3.276.1.5.9 Code=BERI

Metadatenelement SubmissionSet		
contentTypeCode	R	Klinische Aktivität, die zum Einstellen des SubmissionSet geführt hat. Codesystem=1.3.6.1.4.1.19376.3.276.1.5.12 Code=2,3,4,8,9 gemäß [IHE-ITI-VS]

[<=]

### A\_16246 - Auslesen des eArztbriefes nach § 291f SGB V

Beim Auslesen eines eArztbriefes mit `formatCode="Code=urn:gematik:ig:Arztbrief:r3.1"` MUSS das PS die zwei Anteile (den CDA-Anteil und den PDF-Anteil) aus der XML-Container-Struktur `DischargeLetterContainer` gemäß [gemSpec\_DM\_ePA#4.2] aus der ePA herauslesen und als eArztbrief nach § 291f SGB V gemäß [Richtlinie eArztbrief] weiterverarbeiten und den PDF-Anteil zur Anzeige bringen können. [<=]

## 6.3.4 Strukturierte Dokumente

In der ePA können strukturierte Dokumente verarbeitet werden. Strukturierte Dokumente und deren Zuordnung zu Sammlung und Sammlungstypen sind in [gemSpec\_DM\_ePA#[Kapitel 2.1.4.4](#)] beschrieben.

Zum Laden, Suchen und Einstellen von strukturierten Dokumenten gelten die Anwendungsfälle zum Laden, Suchen, Einstellen und Löschen von Dokumenten. Es kommen gemäß [gemSpec\_DM] weitere Kriterien zur Aufbereitung einer Sammlung hinzu. Sammlungen des Verwaltungstyps mixed werden durch Ordner gruppiert. Besteht der Bedarf nach mehreren Sammlungen des gleichen Typs (Beispiel Mutterpass) so wird jeweils ein Ordner (je Schwangerschaft) angelegt. Beim erstmaligen Erstellen einer Sammlung muss vom Primärsystem für diese Sammlung ein Ordner angelegt werden. Es wird empfohlen für den Titel des Ordners einen sprechenden Namen zu finden. Dadurch kann bei der Suche nach Sammlungen bereits durch den Titel auf deren Inhalt geschlossen werden. Da das Aktensystem die Ordner des Verwaltungstyps mixed löscht, wenn diese keine Dokumente mehr enthalten, ist das Löschen der Ordner durch das Primärsystem nicht erforderlich.

Die Erteilung der Berechtigung für eine Sammlung kann im Primärsystem im Rahmen der Berechtigung für eine Dokumentenkategorie (soweit für Pass definiert) erfolgen. Zusätzlich können Sammlungen grobgranular berechtigt werden, wenn die vergebene Berechtigungsstufe (normal oder erweitert) den Zugriff auf jedes einzelne Dokument der Sammlung gestattet.

Die Liste der strukturierten Dokumente wird sich im Laufe der Zeit erweitern. Die KBV liefert zu neu entwickelten MIOs Informationen über die interne Datenstruktur und fachliche Hintergründe, die gematik veröffentlicht Informationen darüber, um welchen Sammlungstyp es sich bei dem neuen strukturierten Dokument handelt, und welche Metadaten dieses strukturierte Dokument identifizieren.

Die Berechtigung zukünftiger strukturierter Dokumente wird über das Freigeben gemäß Vertraulichkeitsstufe geregelt, d.h. wenn ein neues, bisher noch nicht bekanntes strukturiertes Dokument vom Versicherten mit der Vertraulichkeitsstufe "normal" eingestellt wird, kann es über die genannte Vertraulichkeitsstufe für einen LE freigegeben werden.

#### **A\_19548 - Elektronischer Impfpass**

Das PS MUSS die Werte der `DocumentEntry`- und `SubmissionSet`-Metadaten für den elektronischen Impfpass gemäß `[gemSpec_DM_ePA]` für das Dokumentenmanagement der ePA automatisiert befüllen. [`<=`]

#### **A\_19549 - Elektronischer Mutterpass**

Das PS MUSS die Werte der `DocumentEntry`- und `SubmissionSet`-Metadaten für den elektronischen Mutterpass gemäß `[gemSpec_DM_ePA]` für das Dokumentenmanagement der ePA automatisiert befüllen. [`<=`]

#### **A\_19550 - Elektronisches Untersuchungsheft für Kinder**

Das PS MUSS die Werte der `DocumentEntry`- und `SubmissionSet`-Metadaten für das elektronische Untersuchungsheft für Kinder gemäß `[gemSpec_DM_ePA]` für das Dokumentenmanagement der ePA automatisiert befüllen. [`<=`]

#### **A\_19551 - Elektronisches Zahnbonusheft**

Das PS MUSS die Werte der `DocumentEntry`- und `SubmissionSet`-Metadaten für das elektronische Zahnbonusheft gemäß `[gemSpec_DM_ePA]` für das Dokumentenmanagement der ePA automatisiert befüllen. [`<=`]

#### **A\_19552 - Elektronische Verordnungen/Verordnungsdatensatz**

Das PS MUSS die Werte der `DocumentEntry`- und `SubmissionSet`-Metadaten für elektronische Verordnungen/den Verordnungsdatensatz gemäß `[gemSpec_DM_ePA]` für das Dokumentenmanagement der ePA automatisiert befüllen. [`<=`]

#### **A\_20197-01 - Arbeitsunfähigkeitsbescheinigung**

Das PS MUSS die Werte der `DocumentEntry`- und `SubmissionSet`-Metadaten für elektronische Arbeitsunfähigkeitsbescheinigungen gemäß `[gemSpec_DM_ePA]` für das Dokumentenmanagement der ePA automatisiert befüllen. [`<=`]

### **6.3.4.1 Signatur für strukturierte Dokumentenformate der ePA**

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

Im Folgenden wird das Vorgehen beschrieben, für den Fall, dass ein strukturiertes Dokumentenformat signiert wird.

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, z.B. Dokument elektronische Verordnungen/Verordnungsdatensatz, Impfpassdokument.
2. Primärsystem serialisiert die Daten zu einer Data to be Signed Representation (DTBSR).
3. Primärsystem übermittelt DTBSR an den Konnektor zur Signaturerstellung (Aufruf der Operation `SignDocument` gemäß `[gemILF_PS]`).
4. Konnektor erzeugt eine CADES Enveloping Signatur.



5. Signiertes Objekt enthält sowohl die Signatur als auch die ursprünglichen DTBSR bitgenau und in einem binären ASN.1 Format (PKCS#7).
6. Konnektor übermittelt signiertes Objekt an das Primärsystem.
7. Primärsystem stellt über das Funktionsmerkmal "Dokumente einstellen" (siehe Kap.5.2.1) 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. Primärsystem lädt Dokument aus dem ePA-Aktensystem.
2. Primärsystem erkennt, dass es sich dabei um ein medizinisches Objekt im Format im PKCS#7 handelt (`DocumentEntry.mimetype = application/pkcs7-mime`).
3. Primärsystem übermittelt das signierte Objekt an den Konnektor zur Signaturprüfung (Aufruf der Operation `VerifyDocument [gemILF_PS]`).
4. Konnektor prüft die Signatur.
5. 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.[<=]

Ein vom Arzt mit QES-signiertes E-Rezept darf nicht in den Besitz des Versicherten gelangen und wird ausschließlich im E-Rezept-Server gespeichert. Deshalb wird begrifflich unterschieden zwischen E-Rezept und Elektronische Verordnungen/Verordnungsdatensatz. Elektronische Verordnungen/Verordnungsdatensatz ist nicht QES signiert und kann in die Akte des Versicherten eingestellt werden.

#### **A\_19974 - Elektronische Verordnungen/Verordnungsdatensatz ohne QES**

Ein Primärsystem DARF NICHT Elektronische Verordnungen/Verordnungsdatensatz mit QES in die Akte des Versicherten einstellen. [**<=**]

---

## **7 Ergänzende Funktionalitäten**

---

### **7.1 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\_DM\_ePA#Tabelle Nutzungsvorgaben für Metadatenattribute XDS.b] aufgelistet sind, soweit sie für den Verarbeitungskontext relevant sind.

## 8 Anhang A – Verzeichnisse

### 8.1 Abkürzungen

Kürzel	Erläuterung
Versicherten-ID	Die Versicherten-ID ist der 10-stellige unveränderliche Teil der 30-stelligen Krankenversicherungsnummer.
BAG	Berufsausübungsgemeinschaft
DTBS	Data To Be Signed - zu signierende Daten
DTBSR	Data to be Signed Representation - maschinenlesbare Repräsentation der zu signierenden Daten.
KT	Kartenterminal

### 8.2 Glossar

Begriff	Erläuterung
Funktionsmerkmal	Der Begriff beschreibt eine Funktion oder auch einzelne, eine logische Einheit bildende Teilfunktionen der TI im Rahmen der funktionalen Zerlegung des Systems.
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.

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

### 8.3 Abbildungsverzeichnis

Abbildung 1: ILF_ePA_Element_Context .....	14
Abbildung 2: Abb_ILF_ePA_RecordIdentifier .....	16
Abbildung 3: Abb_ILF_ePA_Kombinierte_Anwendungsfälle_für_bereits_aktiviertes_Aktenkonto ..	20
Abbildung 4: Abb_ILF_ePA_getHomeCommunityRequest .....	24
Abbildung 5: Abb_ILF_PS_ePA_getHomeCommunityResponse .....	24

Abbildung 6: Abb_ILF_ePA_Eingabeparameter_ActivateAccount .....	28
Abbildung 7: Abb_ILF_ePA_RequestFacilityAuthorization .....	32
Abbildung 8: Abb_ILF_ePA_Ad-hoc-Berechtigung_erteilen .....	35
Abbildung 9: Abb_ILF_ePA_Eingabeparameter_GetAuthorizationList .....	70
Abbildung 10: Abb_ILF_ePA_GetAuthorizationListResponse .....	71
Abbildung 11: Abb_ILF_ePA_Benachrichtigungen_GetAll_mit_Zugriffspolicy-Event .....	74
Abbildung 12: Abb_ILF_ePA_eAB-XML-Containerformat .....	93

## 8.4 Tabellenverzeichnis

Tabelle 1: Tab_ILF_ePA_IHE-TransaktionenProfile .....	8
Tabelle 2: Tab_ILF_ePA_Identifizierung_für_Versicherte_und_Akten .....	15
Tabelle 3: Tab_ILF_ePA_Zugriffsberechtigungsstatus pro RecordIdentifier .....	16
Tabelle 4: Tab_ILF_ePA_Zugriffsberechtigungen.....	17
Tabelle 5: Tab_ILF_ePA_Funktionsmerkmale_Beteiligung_Versicherter .....	20
Tabelle 6: Tab_ILF_ePA_PHRManagementService .....	21
Tabelle 7: Tab_ILF_ePA_Operation_getHomeCommunityID .....	23
Tabelle 8: Tab_ILF_ePA_Operation_ActivateAccount .....	27
Tabelle 9: Tab_ILF_ePA_Operation_RequestFacilityAuthorization .....	31
Tabelle 10: Tab_ILF_ePA_Zugriffsberechtigungs-Endedatum.....	33
Tabelle 11: Tab_ILF_ePA_PHRService .....	36
Tabelle 12: Tab_ILF_ePA_DM_Profilierung .....	37
Tabelle 13: Tab_ILF_ePA_Einschränkungen_auf_XDS.b.....	37
Tabelle 14: Tab_ILF_ePA_ClientInformationen .....	38
Tabelle 15: Tab_ILF_ePA_Zugriffsinformation_Werte .....	39
Tabelle 16: Tab_ILF_ePA_IHE-Profilierung_ITI41.....	40
Tabelle 17: Tab_ILF_ePA_Operation_Dokument_einstellen .....	40
Tabelle 18: Tab_ILF_ePA_Fehlerbehandlung_Dokumente_einstellen .....	51
Tabelle 19: Tab_ILF_ePA_IHE-Profilierung_ITI18.....	52
Tabelle 20: Tab_ILF_ePA_Operation_Dokument_suchen.....	53
Tabelle 21: Tab_ILF_ePA_FindDocuments_Pflichtfelder .....	55
Tabelle 22: Tab_ILF_ePA_StoredQueries .....	56
Tabelle 23: Tab_ILF_ePA_Fehlerbehandlung_Dokumente_Suchen .....	59
Tabelle 24: Tab_ILF_ePA_IHE-Profilierung_ITI43.....	60
Tabelle 25: Tab_ILF_ePA_Operation_Dokumente_anzeigen .....	61

Tabelle 26: Tab_ILF_ePA_IHE-Profilierung_ITI86.....	64
Tabelle 27: Tab_ILF_ePA_Operation_Dokumente_löschen .....	65
Tabelle 28: Tab_ILF_ePA_Namensräume .....	66
Tabelle 29: Tab_ILF_ePA_Benachrichtigungsquellen .....	68
Tabelle 30: Tab_ILF_ePA_Benachrichtigungs_InfoModell .....	68
Tabelle 31: Tab_ILF_ePA_Operation_GetAuthorizationList .....	70
Tabelle 32: Tab_ILF_ePA_Infoquelle_Fehlermeldung .....	72
Tabelle 33: Tab_ILF_ePA_ErrorSeverity.....	76
Tabelle 34: Tab_ILF_ePA_IHE_Success_and_Error_Reporting .....	76
Tabelle 35: Tab_ILF_ePA_DifferenzFehlerhandling .....	77
Tabelle 36: Tab_ILF_ePA_Handlungsanweisung_im_Fehlerfall .....	78
Tabelle 37: Tab_ILF_ePA_Fehlermeldungen des Fachmoduls ePA.....	80
Tabelle 38: Tab_ILF_ePA_IHE-Fehlermeldungen_Aktensystem .....	82
Tabelle 39: Tab_ILF_ePA_Datenfelder_Selbstauskunft .....	86
Tabelle 40: Tab_ILF_ePA_Dokumentenformate (beispielhaft) .....	87
Tabelle 41: Tab_ILF_ePA_Nutzungsvorgaben für Metadaten NFD/DPE .....	89
Tabelle 42: Tab_ILF_ePA_Nutzungsvorgaben für Metadaten eMP .....	91
Tabelle 43: Tab_ILF_ePA_Nutzungsvorgaben für Metadaten eAB .....	93

## 8.5 Referenzierte Dokumente

### 8.5.1 Dokumente der gematik

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

<b>[Quelle]</b>	<b>Herausgeber: Titel</b>
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur
[gemSpec_FM_ePA]	gematik: Spezifikation Fachmodul ePA
[gemSpec_DM_ePA]	gematik: Datenmodell ePA

[gemSpec_OM]	gematik: Übergreifende Spezifikation Operations und Maintenance
[gemSysL_ePA]	gematik: Systemspezifisches Konzept ePA
[gemILF_PS_NFDM]	gematik: Implementierungsleitfaden Primärsysteme – Notfalldaten-Management (NFDM)
[gemSpec_InfoNFDM]	gematik: Informationsmodell Notfalldaten-Management (NFDM)
[gemRL_QES_NFDM]	gematik: Signaturreichtlinie QES Notfalldaten-Management (NFDM)
[gemSpec_Info_AMTS]	gematik: Informationsmodell eMP/AMTS-Datenmanagement
[gemILF_PS_AMTS]	gematik: Implementierungsleitfaden Primärsysteme – elektronischer Medikationsplan/AMTS-Datenmanagement (Stufe A)
[gemKPT_Arch_TIP]	gematik: Konzept Architektur der TI-Plattform
[gemSpec_PKI]	gematik: Spezifikation PKI

## 8.5.2 Weitere Dokumente

<b>[Quelle]</b>	<b>Herausgeber (Erscheinungsdatum): Titel</b>
[BasicProfile1.2]	Basic Profile Version 1.2 <a href="http://www.ws-i.org/Profiles/BasicProfile-1.2-2010-11-09.html">http://www.ws-i.org/Profiles/BasicProfile-1.2-2010-11-09.html</a>
[BasicProfile2.0]	Basic Profile Version 2.0 <a href="http://ws-i.org/Profiles/BasicProfile-2.0-2010-11-09.html">http://ws-i.org/Profiles/BasicProfile-2.0-2010-11-09.html</a>
[WSDL11]	W3C (2006): WSDL 1.1 Binding Extension for SOAP 1.2, <a href="https://www.w3.org/Submission/wsd11soap12/">https://www.w3.org/Submission/wsd11soap12/</a>
[SOAP12]	W3C (2007): SOAP Version 1.2 Part 1: Messaging Framework (Second Edition), <a href="https://www.w3.org/TR/soap12-part1/">https://www.w3.org/TR/soap12-part1/</a>
[ebRS]	ebXML Registry Services Specification Version 3.0 <a href="https://docs.oasis-open.org/regrep/regrep-rs/v3.0/regrep-rs-3.0-os.pdf">https://docs.oasis-open.org/regrep/regrep-rs/v3.0/regrep-rs-3.0-os.pdf</a>
[IHE-ITI-TF2a], enthält [ITI-18]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework, Volume 2a (ITI TF-2a) - Transactions Part A, Revision 15.0, <a href="http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2a.pdf">http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2a.pdf</a>

[IHE-ITI-TF2b], enthält [ITI-41], [ITI-43], [ITI-45]	IHE International (2017): IHE IT Infrastructure (ITI) Technical Framework, Volume 2b (ITI TF-2b) - Transactions Part B, Revision 14.0, <a href="http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2b.pdf">http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2b.pdf</a>
[IHE-ITI-TF2x]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework, Volume 2x (ITI TF-2x) – Volume 2 Appendices, Revision 15.1, <a href="http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2x.pdf">http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2x.pdf</a>
[IHE-ITI-TF3]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework, Volume 3 (ITI TF-3) - Cross-Transaction Specifications and Content Specifications, Revision 15.0, <a href="http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol3.pdf">http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol3.pdf</a>
[IHE-ITI-RMD], enthält [ITI-86]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework Supplement, Remove Metadata and Documents (RMD), Revision 1.2 – Trial Implementation, <a href="http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RMD.pdf">http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RMD.pdf</a>
[IHE-ITI-XCDR]	IHE International (2017): IHE IT Infrastructure (ITI) Technical Framework Supplement, Cross-Community Document Reliable Interchange (XCDR), Revision 1.4 – Trial Implementation, <a href="http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_XCDR.pdf">http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_XCDR.pdf</a>
[IHE-ITI-TF1]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework, Volume 1 (ITI TF-1) Integration Profiles <a href="http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol1.pdf">http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol1.pdf</a>
[ITI TF Supplement]	IHE IT Infrastructure 5 Technical Framework Supplement Remove Metadata and Documents 10 (RMD)
[MTOM]	W3C (2005): SOAP Message Transmission Optimization Mechanism, <a href="https://www.w3.org/TR/soap12-mtom/">https://www.w3.org/TR/soap12-mtom/</a>
[Richtlinie eArztbrief]	Kassenärztliche Bundesvereinigung (2017): Richtlinie über die Übermittlung elektronischer Briefe in der vertragsärztlichen Versorgung gemäß § 291f SGB V, Richtlinie Elektronischer Brief, Version: 10.0, <a href="https://www.kbv.de/media/sp/RL-eArztbrief.pdf">https://www.kbv.de/media/sp/RL-eArztbrief.pdf</a>
[KBV Portal]	Portal der Kassenärztliche Bundesvereinigung <a href="https://kbv.de">https://kbv.de</a>
[XPath]	XML Path Language (XPath) Version 1.0 <a href="http://www.w3.org/TR/xpath">http://www.w3.org/TR/xpath</a>
[IHE-ITI-VS]	IHE Deutschland (2018): Value Sets für Aktenprojekte im deutschen Gesundheitswesen, Implementierungsleitfaden, Version 2.0 <a href="http://www.ihe-d.de/projekte/xds-value-sets-fuer-deutschland/">http://www.ihe-d.de/projekte/xds-value-sets-fuer-deutschland/</a>



[OWASP Top 10]	OWASP (2017): OWASP Top 10 -- 2017 - The Ten Most Critical Web Application Security Risks <a href="https://github.com/OWASP/Top10/raw/master/2017/OWASP%20Top%2010-2017%20(en).pdf">https://github.com/OWASP/Top10/raw/master/2017/OWASP%20Top%2010-2017%20(en).pdf</a>
----------------	--