

Beim vorliegenden Dokument handelt es sich um einen Entwurf der gematik in Vorbereitung auf zukünftige normative Festlegungen als Grundlage entsprechender Zulassungs- und Bestätigungsverfahren. Die gematik veröffentlicht diesen Entwurf mit dem Ziel, dass sich Interessierte bereits frühzeitig einen Überblick über die mögliche Weiterentwicklung der Telematikinfrastruktur verschaffen können. Die gematik übernimmt keine Gewähr für die Aktualität, Richtigkeit und Vollständigkeit dieses Entwurfes und behält sich das Recht vor, ohne vorherige Ankündigung Änderungen oder Ergänzungen vorzunehmen oder von den Regelungen insgesamt bzw. teilweise Abstand zu nehmen.

## Elektronische Gesundheitskarte und Telematikinfrastruktur

# Spezifikation Fachmodul ePA

Version: 1.45.0 CC  
Revision: 198565230717  
Stand: 02.0330.04.2020  
Status: zur Abstimmung freigegeben  
Klassifizierung: öffentlich Entwurf  
Referenzierung: gemSpec\_FM\_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		freigegeben	gematik
1.1.0	15.05.19		Einarbeitung P18.1	gematik
1.2.0	28.06.19		Einarbeitung P19.1	gematik
			Einarbeitung P20.1	gematik
1.3.0	02.10.19		freigegeben	gematik
1.4.0	02.03.20		freigegeben	gematik
<a href="#">1.5.0 CC</a>	<a href="#">30.04.20</a>		<a href="#">Anpassungen gemäß Änderungsliste P22.1 und Scope-Themen aus Systemdesign R4.0.0</a>	<a href="#">gematik</a>

## Inhaltsverzeichnis

<b>1 Einordnung des Dokumentes</b>	<b>7</b>
1.1 Zielsetzung	7
1.2 Zielgruppe	7
1.3 Geltungsbereich	7
1.4 Abgrenzungen	8
1.5 Methodik	8
<b>2 Systemüberblick</b>	<b>9</b>
<b>3 Systemkontext</b>	<b>10</b>
<b>4 Zerlegung des Produkttyps</b>	<b>11</b>
<b>5 Technologien und Standards</b>	<b>12</b>
5.1 Webservices	12
5.2 Integrating the Healthcare Enterprise (IHE)	12
5.2.1 Relevante IHE Integrationsprofile	12
5.2.2 Überblick über IHE Akteure und assoziierte Transaktionen	14
<b>6 Übergreifende Festlegungen</b>	<b>16</b>
6.1 Allgemein	16
6.2 IHE	23
6.3 Lokalisierung von ePA Aktensystemen	26
6.4 Aufrufkontext und Auswahl eines SM-B	27
6.5 Login	30
6.5.1 Aktensession	30
6.5.2 Authentisierung mittels SM-B	33
6.5.3 Authentisierung mittels eGK	34
6.5.4 Autorisierung	36
6.5.5 Verbindung zur Dokumentenverwaltung	39
6.5.6 Schlüsselableitung	41
6.6 Logout	45
6.7 Datenschutz und Sicherheitsaspekte	46
6.8 Verwendung des Dienstverzeichnisdienstes	46
6.9 Protokollierung und Logging	47
6.10 Konfiguration	50
6.11 Fehlerbehandlung und Fehlermeldungen	51
<b>7 Funktionsmerkmale</b>	<b>55</b>

68	<b>7.1 PHRService</b>	<b>57</b>
69	7.1.1 Definition/Signatur	60
70	7.1.1.1 putDocuments	60
71	7.1.1.2 find	61
72	7.1.1.3 getDocuments	61
73	7.1.1.4 removeDocuments	62
74	7.1.1.5 updateDocumentSet	63
75	7.1.2 Umsetzung	64
76	7.1.2.1 putDocuments	65
77	7.1.2.2 find	66
78	7.1.2.3 getDocuments	67
79	7.1.2.4 removeDocuments	68
80	7.1.2.5 updateDocumentSet	69
81	<b>7.2 PHRManagementService</b>	<b>70</b>
82	7.2.1 Definition/Signatur	71
83	7.2.1.1 ActivateAccount	72
84	7.2.1.2 RequestFacilityAuthorization	72
85	7.2.1.3 GetHomeCommunityID	74
86	7.2.1.4 GetAuthorizationList	75
87	7.2.2 Umsetzung	76
88	7.2.2.1 ActivateAccount	76
89	7.2.2.2 RequestFacilityAuthorization	78
90	7.2.2.3 GetHomeCommunityID	92
91	7.2.2.4 GetAuthorizationList	93
92	<b>8 Anhang A – Verzeichnisse</b>	<b>96</b>
93	8.1 Abkürzungen	96
94	8.2 Glossar	97
95	8.3 Abbildungsverzeichnis	97
96	8.4 Tabellenverzeichnis	97
97	8.5 Referenzierte Dokumente	100
98	8.5.1 Dokumente der gematik	100
99	8.5.2 Weitere Dokumente	101
100	<b>1 Einordnung des Dokumentes</b>	<b>7</b>
101	1.1 Zielsetzung	7
102	1.2 Zielgruppe	7
103	1.3 Geltungsbereich	7
104	1.4 Abgrenzungen	8
105	1.5 Methodik	8
106	<b>2 Systemüberblick</b>	<b>9</b>
107	<b>3 Systemkontext</b>	<b>10</b>
108	<b>4 Zerlegung des Produkttyps</b>	<b>11</b>
109	<b>5 Technologien und Standards</b>	<b>12</b>

110	<b>5.1 Webservices .....</b>	<b>12</b>
111	<b>5.2 Integrating the Healthcare Enterprise (IHE) .....</b>	<b>12</b>
112	5.2.1 Relevante IHE-Integrationsprofile.....	12
113	5.2.2 Überblick über IHE-Akteure und assoziierte Transaktionen .....	14
114	<b>6 Übergreifende Festlegungen .....</b>	<b>16</b>
115	<b>6.1 Allgemein .....</b>	<b>16</b>
116	<b>6.2 IHE .....</b>	<b>23</b>
117	<b>6.3 Lokalisierung von ePA-Aktensystemen .....</b>	<b>26</b>
118	<b>6.4 Aufrufkontext und Auswahl eines SM-B.....</b>	<b>27</b>
119	<b>6.5 Login .....</b>	<b>30</b>
120	6.5.1 Aktensession .....	30
121	6.5.2 Authentisierung mittels SM-B .....	33
122	6.5.3 Authentisierung mittels eGK .....	34
123	6.5.4 Autorisierung.....	36
124	6.5.5 Verbindung zur Dokumentenverwaltung.....	39
125	6.5.6 Schlüsselableitung.....	41
126	<b>6.6 Logout .....</b>	<b>45</b>
127	<b>6.7 Datenschutz und Sicherheitsaspekte .....</b>	<b>46</b>
128	<b>6.8 Verwendung des Dienstverzeichnisdienstes .....</b>	<b>46</b>
129	<b>6.9 Protokollierung und Logging .....</b>	<b>47</b>
130	<b>6.10 Konfiguration .....</b>	<b>50</b>
131	<b>6.11 Fehlerbehandlung und Fehlermeldungen .....</b>	<b>51</b>
132	<b>7 Funktionsmerkmale .....</b>	<b>55</b>
133	<b>7.1 PHRService .....</b>	<b>57</b>
134	7.1.1 Definition/Signatur .....	60
135	7.1.1.1 putDocuments .....	60
136	7.1.1.2 find .....	61
137	7.1.1.3 getDocuments .....	61
138	7.1.1.4 removeDocuments .....	62
139	7.1.1.5 updateDocumentSet des WebService Version 1.x (abgekündigt) .....	63
140	7.1.1.6 putDocuments .....	65
141	7.1.1.7 find .....	66
142	7.1.1.8 getDocuments .....	67
143	7.1.1.9 removeDocuments .....	68
144	7.1.1.10 updateDocumentSet (abgekündigt).....	69
145	<b>7.2 PHRManagementService.....</b>	<b>70</b>
146	7.2.1 Definition/Signatur .....	71
147	7.2.1.1 ActivateAccount .....	72
148	7.2.1.2 RequestFacilityAuthorization .....	72
149	7.2.1.3 GetHomeCommunityID .....	74
150	7.2.1.4 GetAuthorizationList .....	75
151	7.2.2 Umsetzung.....	76
152	7.2.2.1 ActivateAccount .....	76
153	7.2.2.2 RequestFacilityAuthorization .....	78
154	7.2.2.3 GetHomeCommunityID .....	92

155	<a href="#">7.2.2.4 GetAuthorizationList .....</a>	93
156	<b><a href="#">8 Anhang A – Verzeichnisse .....</a></b>	<b>96</b>
157	<a href="#">8.1 Abkürzungen .....</a>	96
158	<a href="#">8.2 Glossar .....</a>	97
159	<a href="#">8.3 Abbildungsverzeichnis .....</a>	97
160	<a href="#">8.4 Tabellenverzeichnis .....</a>	97
161	<a href="#">8.5 Referenzierte Dokumente .....</a>	100
162	<a href="#">8.5.1 Dokumente der gematik .....</a>	100
163	<a href="#">8.5.2 Weitere Dokumente .....</a>	101
164		

ENTWURF

---

## 1 Einordnung des Dokumentes

---

### 1.1 Zielsetzung

Das Fachmodul ePA ist Teil der Fachanwendung ePA, die im Systemkonzept [gemSysL\_ePA] beschrieben wird. Als Teil des Konnektors kommt das Fachmodul ePA in der Leistungserbringerumgebung zum Einsatz und ist damit Bestandteil der dezentralen TI. Es bietet Primärsystemen Schnittstellen an, um medizinische Dokumente für Versicherte in einem ePA-Aktensystem zu verwalten.

Die vom Fachmodul ePA bereitzustellenden Schnittstellen basieren zu großen Teilen auf den Spezifikationen der IHE-Initiative. Insbesondere kommen IHE-Integrationsprofile aus der Familie XDS.b (Cross-Enterprise Document Sharing) zum Einsatz. Neben den Primärsystemen kommuniziert das Fachmodul ePA auch mit ePA-Aktensystemen, welche die Dokumente der Versicherten verwalten. ePA-Aktensysteme können von mehreren Anbietern zur Verfügung gestellt werden, wobei die Dokumente eines einzelnen Versicherten immer genau bei einem Anbieter ePA-Aktensystem hinterlegt werden.

Diese Spezifikation beschreibt Anforderungen an die Schnittstellen, die vom Fachmodul ePA selbst angeboten werden müssen und an die daraus resultierende Funktionalität. Dazu nutzt das Fachmodul ePA die Schnittstellen des ePA-Aktensystems und weiterer zentraler TI-Komponenten.

### 1.2 Zielgruppe

Das Dokument richtet sich an Hersteller des Produkttyps Konnektor sowie Hersteller und Anbieter von Produkttypen, die hierzu eine Schnittstelle besitzen.

### 1.3 Geltungsbereich

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

### **Schutzrechts-/Patentrechtshinweis**

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

## 202 1.4 Abgrenzungen

203 Spezifiziert werden in dem Dokument die von dem Fachmodul ePA bereitgestellten  
204 Schnittstellen. Benutzte Schnittstellen werden hingegen in der Spezifikation desjenigen  
205 Produkttypen beschrieben, der diese Schnittstelle bereitstellt. Auf die entsprechenden  
206 Dokumente wird referenziert (siehe auch Anhang 8.5).

207 Die vollständige Anforderungslage für den Konnektor ergibt sich aus weiteren  
208 Spezifikationsdokumenten, die im Produkttypsteckbrief verzeichnet sind.

## 209 1.5 Methodik

210 Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID  
211 sowie die dem RFC 2119 [RFC2119] entsprechenden, in Großbuchstaben geschriebenen  
212 deutschen Schlüsselworte MUSS, DARF NICHT, SOLL, SOLL NICHT, KANN  
213 gekennzeichnet.

214 Da in dem Beispielsatz „Eine leere Liste DARF NICHT ein Element besitzen.“ die Phrase  
215 „DARF NICHT“ semantisch irreführend wäre (wenn nicht ein, dann vielleicht zwei?), wird  
216 in diesem Dokument stattdessen „Eine leere Liste DARF KEIN Element besitzen.“  
217 verwendet. Die Schlüsselworte werden außerdem um Pronomen in Großbuchstaben  
218 ergänzt, wenn dies den Sprachfluss verbessert oder die Semantik verdeutlicht.

219 Anforderungen werden im Dokument wie folgt dargestellt:

220 **<AFO-ID> - <Titel der Afo>**

221 Text / Beschreibung

222 [**<=>**]

223 Dabei umfasst die Anforderung sämtliche zwischen Afo-ID und Textmarke

224 [**<=>**] angeführten Inhalte.



225

## 2 Systemüberblick

Die Fachanwendung ePA setzt im Rahmen der TI-Plattform eine elektronische Patientenakte (ePA), ein Aktenkonto des Versicherten um, in die Berechtigte wie der Versicherte oder autorisierte Leistungserbringer patientenbezogene Dokumentation aus verschiedenen Einrichtungen einstellen und verwalten können. Die Fachanwendung erlaubt das Einstellen, Suchen, Abrufen und Löschen von Dokumenten sowie die Aktualisierung von Metadaten bestehender Dokumente.

Die Fachanwendung ePA besteht aus Sicht dieser Spezifikation aus zwei Teilen: Einerseits dem dezentralen Fachmodul, das Teil des Konnektors ist und nach außen eine Schnittstelle für die Verwaltung der Dokumente bietet und andererseits dem zentralen Fachdienst ePA-Aktensystem, der die Dokumente innerhalb der TI-Plattform speichert, Berechtigungen verwaltet und durchsetzt usw. und den beiden Schlüsselgenerierungsdiensten (SGD). Das außerdem zur Fachanwendung gehörende „ePA-Modul Frontend des Versicherten“ ist für dieses Dokument nicht relevant und wird deshalb nicht weiter behandelt.

Diese Spezifikation beschreibt das Fachmodul ePA und dessen Außenschnittstelle, die von Primärsystemen (z. B. KIS und PVS) genutzt wird, um Dokumente zu verwalten. Um beim Leistungserbringer „ad hoc“ Zugriffsberechtigungen zu Dokumenten vom Patienten einzuholen, findet zudem bei Bedarf eine Kommunikation mit dem Kartenterminal statt. Zusätzlich beschreibt diese Spezifikation die Nutzung der Schnittstelle des ePA-Aktensystems, welches die eigentliche Dokumentenverwaltung, Autorisierung und weitere Details umsetzt.

Ein ePA-Aktensystem kann durch mehr als einen Anbieter angeboten werden. Die Akte des Versicherten wird zu einem Zeitpunkt jedoch immer nur exklusiv von einem einzigen Anbieter ePA-Aktensystem geführt, der alle Dokumente des Versicherten verwaltet und über das ePA-Aktensystem bereitstellt.

Über das ePA-Aktensystem hinaus interagiert das Fachmodul ePA unter Verwendung der Basisdienste des Konnektors mit dem Verzeichnisdienst der TI-Plattform, um Details zu Leistungserbringern und -institutionen abzurufen sowie anderen zentralen TI-Diensten (Zeitdienst, Namensdienst).

ePA-Aktensysteme speichern aus Datenschutzgründen alle Dokumente in verschlüsselter Form. Die Verschlüsselung beim Einstellen und die Entschlüsselung beim Herunterladen erfolgt immer im Fachmodul (nicht in den Primärsystemen). Um eine im ePA-Aktensystem eingehende Suchanfrage nach Dokumenten im ePA-Aktensystem trotz verschlüsselter Daten durchführen zu können, wird für jedes Dokument zusätzlich ein Satz an unverschlüsselten Metadaten gespeichert. Dazu gehören das Dokumentenformat (z. B. PDF), der Dokumententyp (z. B. Notfalldatensatz), Erstellungsdatum und -uhrzeit und der Autor des Dokuments.

Für den Zugriff auf Metadaten und Dokumente muss ein Nutzer (in diesem Dokument Leistungserbringerinstitutionen) sich über das Fachmodul ePA authentisieren und vom ePA-Aktensystem autorisiert werden. Um den Zugriff des Anbieters ePA-Aktensystem auf die im Klartext vorliegenden Metadaten zu verhindern, werden diese zusätzlich über eine vertrauenswürdige Ausführungsumgebung (VAU) geschützt.

268

---

### 3 Systemkontext

---

269 Das Fachmodul ePA ist eingebettet in den Produkttyp Konnektor. Die Beschreibung aller  
270 direkt mit dem Fachmodul kommunizierenden Akteure ist im vorgehenden Kapitel  
271 beschrieben. Eine weitere Beschreibung des Systemkontexts ist nicht erforderlich.

ENTWURF

272

---

## **4 Zerlegung des Produkttyps**

---

273

Eine weitere Untergliederung des Fachmoduls ePA in Komponenten ist nicht erforderlich.

ENTWURF

---

## 5 Technologien und Standards

---

Die Schnittstellen und die Verarbeitungslogik der Fachmoduls basiert auf Transaktionen des IHE ITI Technical Frameworks [IHE-ITI-TF]. Es werden soweit wie möglich Cross-Community Access-Profile angewendet.

Der Profilierung von IHE ITI-Transaktionen als Umsetzungsvorgabe für die Außenschnittstellen der Dokumentenverwaltung des ePA-Aktensystems liegt die folgende Herangehensweise zugrunde:

1. Auswahl relevanter IHE ITI-Integrationsprofile
2. Logische Gruppierung zwischen IHE ITI-Akteuren mit Auswahl relevanter IHE ITI-Transaktionen.
3. Übergreifende Einschränkung von IHE ITI-Transaktionen
4. Festlegung spezieller Umsetzungsvorgaben bzgl. einzelner Transaktionen

### 5.1 Webservices

#### **A\_15575 - FM ePA: Übergreifende Anforderung - SOAP für Webservices**

Das Fachmodul ePA MUSS für die Webservices PHRService und PHRManagementService den Standard [SOAP1.2] verwenden.  
[<=]

### 5.2 Integrating the Healthcare Enterprise (IHE)

#### 5.2.1 Relevante IHE-Integrationsprofile

Für die Umsetzung des Fachmoduls sind die folgenden Integrationsprofile relevant:

- Cross-Enterprise Document Sharing (XDS.b) Profile
- Cross-Community Access (XCA) Profile
- Cross-Community Document Reliable Interchange (XCDR) Profile
- Cross-Enterprise Document Reliable Interchange (XDR) Profile
- Remove Metadata and Documents (RMD) Profile
- ~~Restricted Metadata Update (RMU) Profile~~
- Cross-Enterprise User Assertion (XUA) Profile
- Advanced Patient Privacy Consents (APPC) Profile

Ihre Verwendung im Fachmodul wird im Folgenden kurz erläutert:

#### **XDS.b (Cross-Enterprise Document Sharing) Profile**

XDS.b [IHE-ITI-TF], im Weiteren nur als XDS bezeichnet, stellt die Grundlage für die Umsetzung von IHE-Patientenakten dar. Die mit dem Fachmodul verbundenen Primärsysteme bei den Leistungserbringern operieren als Akteure Document Source und

Document Consumer, während das ePA-Aktensystem die Akteure Document Repository und Document Registry bereitstellt.

Das Fachmodul ePA selbst muss zwischen Primärsystem und ePA-Aktensystem vermitteln, also die XDS-basierten Primärsystemnachrichten entgegennehmen, verarbeiten und an das ePA-Aktensystem weiterleiten; das Fachmodul ePA übernimmt also eine Art Proxyfunktionalität, nimmt die Anfragen von Primärsystemen (Document Source/Consumer) entgegen und leitet sie an den Anbieter ePA-Aktensystem mit der Akte des Patienten bzw. dessen Document Repository und Registry weiter. Aus diesem Grund wird auch eine Spezialisierung des XDS-Profiles verwendet: XCA (siehe unten).

### **XCA (Cross-Community Access) Profile**

XCA [IHE-ITI-TF] wird im engeren Sinne bei IHE dafür verwendet, um verschiedene „Home Communities“ miteinander zu vernetzen. Das Profil nimmt dazu geringe Änderungen an den bei XDS.b vorgesehenen Nachrichten und Akteuren zum Suchen und Herunterladen von Dokumenten vor.

Im Fachmodul ePA kommt es zum Einsatz, da XCA (zusammen mit dem XCDR-Profil, siehe unten) am besten die Proxy-artige Funktionalität des Fachmoduls darstellt, das zwischen Primärsystem und ePA-Aktensystem vermittelt und es ermöglicht, die unterschiedlichen Anbieter ePA-Aktensystem jeweils als eigene Home Community zu modellieren. Das Fachmodul ePA tritt dabei als IHE-Akteur „Initiating Gateway“ auf.

### **XCDR (Cross-Community Document Reliable Interchange) Profile**

XCDR [IHE-ITI-XCDR] wird für das Einstellen von Dokumenten verwendet, wenn der XCA-Ansatz (siehe oben) Anwendung findet und spezialisiert vor diesem Hintergrund die in XDS dafür vorgesehene Akteure und Transaktionen. Das Fachmodul ePA arbeitet auch hier als IHE-Akteur „Initiating Gateway“, der Anbieter ePA-Aktensystem als „Responding Gateway“.

### **XDR (Cross-Enterprise Document Reliable Interchange) Profile**

Die Verwendung des Profils XCDR erzwingt auch den gleichzeitigen Gebrauch des Profils XDR, welches leicht veränderte Anforderungen beim Einstellen von Dokumenten (bezüglich Metadaten) mit sich bringt.

### **RMD (Remove Metadata and Documents) Profile**

Gemäß [gemSysL\_ePA] muss die Akte auch das Löschen von Dokumenten ermöglichen. Da dies über die Möglichkeiten der oben genannten Integrationsprofile hinausgeht, greift die Fachanwendung zusätzlich auf das Profil RMD [IHE-ITI-RMD] zurück. Das Fachmodul ePA (als IHE-Akteur „Document Repository“) empfängt und verarbeitet dazu die entsprechenden Nachrichten des Primärsystems und leitet diese (als IHE-Akteur Document Administrator) an das ePA-Aktensystem weiter.

### **~~Restricted Metadata Update (RMU) Profile~~**

~~ePA unterstützt keine Versionierung von Dokumenten. Müssen ein Dokument oder seine Metadaten geändert werden, muss es gelöscht (RMD-Profil, s.o.) und neu eingestellt werden (XCDR-Profil, s.o.). Die einzige Ausnahme dieser Regel wird genutzt, um den Status eines Dokuments von einem reinen „Versichertendokument“ auf ein „leistungserbringeräquivalentes Dokument“ zu ändern, ohne das Dokument neu einstellen zu müssen.~~

### **XUA (Cross-Enterprise User Assertion) Profile**

Das XUA-Profil [IHE-ITI-TF] wird vom Fachmodul verwendet, um sich einerseits bei der Komponente Autorisierung des Anbieters ePA-Aktensystem und andererseits beim Zugriff auf die Akte eines Versicherten bei der Dokumentenverwaltung mit Authentifizierungsinformationen des anfragenden Nutzers auszuweisen.

### **APPC (Advanced Patient Privacy Consents)**

Das APPC-Profil [IHE-ITI-APPC] dient der Durchsetzung von Zugriffsregeln (Autorisierung) in der Fachanwendung. Das Fachmodul ePA erzeugt bei Bedarf das technische Dokument (gemäß APPC) und hinterlegt es in der Akte des Versicherten. Das ePA-Aktensystem verwendet die hinterlegten Zugriffsregeln dann, um zu entscheiden, ob der anfragende Nutzer (gemäß mitgelieferter XUA-Zusicherung) die entsprechende Operation (z. B. Herunterladen eines bestimmten Dokuments) unter Berücksichtigung der Dokumentenmetadaten durchführen darf oder die Anfrage abgelehnt werden muss.

## **5.2.2 Überblick über IHE-Akteure und assoziierte Transaktionen**

Die Abbildung in Abschnitt [gemSpec\_DM\_ePA#2.1.3] zeigt, welche IHE ITI-Akteure insgesamt in der Fachanwendung ePA wie gruppiert sind und welche zugehörigen Transaktionen angewendet werden.

Die folgenden Schilderungen beschreiben beispielhaft die drei häufigsten Anwendungsfälle, das Einstellen, Suchen und Herunterladen von Dokumenten aus Sicht des Fachmoduls ePA.

Gemäß der Nutzung von Cross-Community-Profilen, ist die IHE-basierte Nachrichtenübermittlung durch Transaktionen gekennzeichnet, um ein Dokument durch den Mitarbeiter einer Leistungserbringerinstitution in die elektronische Patientenakte eines Versicherten zu speichern. Ein Primärsystem in der Consumer Zone erzeugt ein Dokument, das vom System als XDR-Akteur „Document Source“ in die Akte eines Versicherten gespeichert werden soll. Beim Einstellen kommen anschließend die folgenden IHE ITI-Transaktionen zum Tragen:

1. Provide & Register Document Set-b [ITI-41]: Das Primärsystem bzw. der XDR-Akteur „Document Source“ sendet eine Nachricht zum Speichern ein oder mehrerer Dokumente an den XDR-Akteur „Document Recipient“ bzw. den gruppierten XCDR-Akteur „Initiating Gateway“, welcher durch das Fachmodul ePA umgesetzt wird.
2. Cross-Gateway Document Provide [ITI-80]: das Fachmodul ePA nimmt einige Transformationen an der Nachricht vor (z. B. Verschlüsselung des Dokuments) und leitet sie als XCDR „Initiating Gateway“ an das XCDR „Responding Gateway“ des Anbieters ePA-Aktensystem weiter.
3. Es erfolgt das akteninterne Registrieren und Speichern der Dokumente. Die Umsetzungsdetails werden zu großen Teilen den Anbietern ePA-Aktensystem überlassen.

Für das Suchen von Dokumenten werden die folgenden IHE-Transaktionen eingesetzt:

1. Registry Stored Query [ITI-18]: Das Primärsystem bzw. der XDS-Akteur „Document Consumer“ sucht Dokumente anhand gewünschter Suchkriterien, in dem es eine entsprechende Nachricht an den XCA-Akteur „Initiating Gateway“ sendet, der vom Fachmodul repräsentiert wird.
2. Cross-Gateway Query [ITI-38]: das Fachmodul ePA bzw. der XCA-Akteur „Initiating Gateway“ leitet die Suchanfrage an den Anbieter ePA-Aktensystem weiter, der den XCA-Akteur „Responding Gateway“ umsetzt.

400 3. Die Suche innerhalb der Akte wird vom Anbieter ePA-Aktensystem durchgeführt  
401 und Suchergebnisse über „Responding Gateway“ und „Initiating Gateway“ an das  
402 Primärsystem zurückgeliefert.

403 Das Herunterladen von Dokumenten wird über die folgenden Transaktionen umgesetzt:

404 1. Retrieve Document Set [ITI-43]: Das Primärsystem stößt als XDS-Akteur  
405 „Document Consumer“ den Download eines oder mehrerer Dokumente an.

406 2. Cross-Gateway Retrieve [ITI-39]: das Fachmodul ePA als XCA-Akteur „Initiating  
407 Gateway“ nimmt die Anfrage entgegen und leitet sie an den Anbieter ePA-  
408 Aktensystem (XCA-Akteur „Responding Gateway“) weiter.

409 3. Die angefragten Dokumente werden vom Anbieter ePA-Aktensystem über XCA  
410 „Responding Gateway“ und „Initiating Gateway“ an das Primärsystem  
411 zurückgeliefert.

412 Das Fachmodul ePA muss alle Anfragen an denjenigen Anbieter ePA-Aktensystem  
413 weiterleiten, der die Akte für den jeweiligen Versicherten führt. Dazu nutzt es die vom  
414 Primärsystem bei jeder Anfrage mit bereitgestellte HomeCommunityID, die den Anbieter  
415 ePA-Aktensystem eindeutig identifiziert. Um die HomeCommunityID verlässlich  
416 verwenden zu können, geht die Fachmodulspezifikation an einigen Stellen über die  
417 Anforderungen von IHE hinaus (z.B. Ermittlung der HomeCommunityID über den  
418 Namensdienst der TI).

## 6 Übergreifende Festlegungen

### 6.1 Allgemein

Die folgenden Anforderungen gelten für das gesamte Fachmodul. Im Gegensatz dazu gibt es auf der Ebene der Webservices Festlegungen, die dann jeweils nur für dessen Operationen greifen.

#### Übergreifende Festlegung für die Kommunikation mit ePA-Aktensystemen

##### **A\_14400 - FM ePA: Übergreifende Anforderung - Server nicht erreichbar - Fehler**

Falls jeweils alle zur Durchführung einer Operation benötigten Komponenten und Diensten

- Zugangsgateway des Versicherten oder
- Autorisierung,
- Dokumentenverwaltung,  
SGD 1 und  
SGD 2

für die Zeitdauer von EPA\_SERVER\_TIMEOUT nicht erreichbar sind, MUSS das Fachmodul ePA die Operation mit den Code 7220 gemäß Tab\_FM\_ePA\_011 abbrechen.

[<=]

Eine Operation, die nur mit einem ePA-Aktensystem kommunizieren muss, bricht demnach ab, falls eine der genannten Komponenten zwingend benötigt wird und nicht zur Verfügung steht. Eine Operation, die mit mehreren ePA-Aktensystemen kommunizieren muss, bricht erst ab wenn eine der Komponenten zwingend benötigt wird und in allen ePA-Aktensystemen nicht zur Verfügung steht. Sonderfälle, falls z.B. ein ePA-Aktensystem komplett ausfällt, werden in den Operationen unterschiedlich behandelt (vgl. auch Kapitel 6.11).

##### **A\_15647 - FM ePA: Übergreifende Anforderung - Konfigurationsparameter des Fachmoduls ePA**

Das Fachmodul ePA MUSS es einem Administrator ermöglichen, Konfigurationsänderungen gemäß Tabelle Tab\_FM\_ePA\_008 vorzunehmen:

**Tabelle 1: Tab\_FM\_ePA\_008 Konfigurationswerte des Fachmoduls ePA**

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
EPA_TLS_HS_TIMEOUT	X Sekunden	Der Administrator MUSS die Anzahl Sekunden eingeben können, die der Konnektor auf den TLS-Verbindungsaufbau zum Aktensystem wartet (Handshake-Timeout).



		Wertebereich:5-30 Default-Wert=10
EPA_KEEP_ALIVE_TRY_COUNT	Anzahl der Versuche	Anzahl von aufeinander folgenden, nicht beantworteten Keep-Alive-Nachrichten, nach denen ein Timeout der TLS-Verbindung festgestellt wird.  Wertebereich:3-10 Default-Wert=3
EPA_SERVER_TIMEOUT	X Sekunden	Der Administrator MUSS die Anzahl Sekunden eingeben können, die der Konnektor maximal auf den TCP-Verbindungsaufbau zum Aktensystem/SGD wartet.  Wertebereich:5-30 Default-Wert=10

452  
453 [ $\leq$ ]

454 **A\_15648 - FM ePA: Übergreifende Anforderung - Timeout bei TLS-**  
455 **Verbindungsaufbau - Fehler**

456 Falls beim TLS-Verbindungsaufbau zu jeweils allen zur Durchführung einer Operation  
457 benötigten Komponenten und Diensten

- 458 • Zugangsgateway des Versicherten oder
- 459 • Autorisierung oder
- 460 • Dokumentenverwaltung oder
- 461 • SGD 1 oder
- 462 • SGD 2

463 der Wert von EPA\_TLS\_HS\_TIMEOUT überschritten wird, MUSS das Fachmodul ePA den  
464 TLS-Verbindungsaufbau abbrechen und die vom Primärsystem aufgerufene Operation mit  
465 dem Code 7202 gemäß Tab\_FM\_ePA\_011 abbrechen.

466 [ $\leq$ ]

467 **A\_15649 - FM ePA: Übergreifende Anforderung - Aktensystem antwortet nicht -**  
468 **Fehler**

469 Falls beim TLS-Verbindungsaufbau zu jeweils allen zur Durchführung einer Operation  
470 benötigten Komponenten und Diensten

- 471 • Zugangsgateway des Versicherten oder
- 472 • Autorisierung oder
- 473 • Dokumentenverwaltung oder
- 474 • SGD 1 oder
- 475 • SGD 2

476 die Antworten nach der Anzahl von EPA\_KEEP\_ALIVE\_TRY\_COUNT Versuchen ausbleibt,  
477 MUSS das Fachmodul ePA die Netzwerkverbindungen beenden und die vom Primärsystem

478 aufgerufene Operation mit dem Code 7220 gemäß Tab\_FM\_ePA\_011 abbrechen.  
479 [ $\leq$ ]

#### 480 **A\_17948 - FM ePA: Authentisierung mit eGK - TLS-Verbindung - Fehler**

481 Falls beim Aufbau der TLS-Verbindung zu jeweils allen zur Durchführung einer Operation  
482 benötigten Komponenten und Diensten

- 483 • Zugangsgateway des Versicherten oder
- 484 • Autorisierung oder
- 485 • Dokumentenverwaltung oder
- 486 • SGD 1 oder
- 487 • SGD 2

488 ein Fehler auftritt, MUSS das Fachmodul ePA die Operation mit dem Code 7202 gemäß  
489 Tab\_FM\_ePA\_011 abbrechen.  
490 [ $\leq$ ]

491 Für Operationen, die mit genau einem Aktensystem kommunizieren, wird die Operation  
492 mit dem Fehler abgebrochen, wenn die Fehlersituation beim Zugangsgateway des  
493 Versicherten oder bei der Komponente Autorisierung oder bei der Komponente  
494 Dokumentenverwaltung auftritt.

495 Für Operationen, die mit mehr als einem Aktensystem kommunizieren, wird die  
496 Operation nur dann mit dem Fehler abgebrochen, wenn die Fehlersituation zu allen  
497 Zugangsgateways des Versicherten oder bei allen Komponenten Autorisierung oder bei  
498 allen Komponenten Dokumentenverwaltung auftritt. Treten Fehler an verschiedenen  
499 Komponenten auf, so wird im Kontext der Operation entschieden, ob mit einem Fehler  
500 (und mit welchem Code) abgebrochen wird (vgl. auch Kapitel 6.11).

#### 501 **Status des Aktenkontos**

#### 502 **A\_17744-01 - FM ePA: Übergreifende Anforderung - Status des Aktenkontos -** 503 **Fehlerbehandlung**

504 Das Fachmodul ePA MUSS in Abhängigkeit des Status des Aktenkontos und der  
505 ausgeführten Operation mit den nachfolgend zugeordneten Codes als Fehler oder  
506 Warnung abbrechen:  
507

508 **Tabelle 2: Tab\_FM\_ePA\_053 - Übersicht der Fehlerfälle nach Status des Status eines**  
509 **Aktenkontos**

Operation	Status des Aktenkontos	Abbruch oder Warnung mit Fehlercode gemäß Tab_FM_ePA_011
Alle Operationen des Webservices PHRService	UNKNOWN	7404
	REGISTERED_MIGRATION	7403
	REGISTERED	7403

Operationen getDocuments, putDocuments, findDocuments, removeDocuments und updateDocumentSet des Webservices PHRService	SUSPENDED	7406
ActivateAccount	UNKNOWN	7404
	REGISTERED_MIGRATION	7403
	ACTIVATED	7402
	DISMISSED	7405
	SUSPENDED	7406
RequestFacilityAuthorization	UNKNOWN	7404
	REGISTERED_MIGRATION	7403
	SUSPENDED	7406

510 **[<=]**

511 Hinweise:

- 512 • Eine Auflistung und Erläuterung aller Status befindet sich in  
513 [gemSpec\_AktenSystem].
- 514 • Ein Aktenkonto kann nur aktiviert werden, falls es sich im Status REGISTERED  
515 befindet.
- 516 • Berechtigungen für LEI können auch bei einem Aktenkonto hinzugefügt werden,  
517 das sich im Status DISMISSED befindet.
- 518 • Falls RequestFacilityAuthorization mit einem Aktenkonto aufgerufen wird, das sich  
519 im Status REGISTERED befindet, führt das Fachmodul vorher implizit die  
520 Operation ActivateAccount durch, um das Aktenkonto zu aktivieren.

521 Da die Operationen GetHomeCommunityID und GetAuthorizationList mit mehreren ePA-  
522 Aktensystemen kommunizieren müssen, findet die Behandlung der Status in den  
523 jeweiligen Unterkapiteln statt.

524 Der Status und die Existenz eines Aktenkontos kann mit Hilfe der Operation  
525 I\_Authorization\_Management::checkRecordExists der Komponente Autorisierung eines  
526 ePA-AktenSystems ermittelt werden. Für manche Operationen müssen alle bekannten  
527 ePA-AktenSysteme angefragt werden, die jeweils mit verschiedenen Fehlern antworten  
528 können. Das Fachmodul zeigt mit dem Fehlercode 7215 eindeutig ein Problem auf Seite  
529 der Aktensysteme an, Fehlercode 7400 hingegen deutet auf ein Problem im Konnektor  
530 hin, bedarf aber einer genaueren Analyse der Log-Dateien.

**A\_17133 - FM ePA: PHRManagementService - Statusprüfung Aktenkonto - Fehler**

Falls alle zur Durchführung einer Operation benötigten Statusprüfungen von Aktenkonten mittels `I_Authorization_Management::checkRecordExists` den Fehler `TECHNICAL_ERROR` zurückgeben, MUSS das Fachmodul ePA die aufgerufene Operation mit dem Code 7400 gemäß `Tab_FM_ePA_011` abbrechen.  
[<=]

**Übergreifende Festlegungen für beteiligte Smartcards****A\_14241 - FM ePA: Übergreifende Anforderung - Unterstützte Generationen der eGK**

Das Fachmodul ePA MUSS alle Versionen der eGK der Generationen G2 und höher unterstützen.[<=]

**A\_14412 - FM ePA: Übergreifende Anforderung - Unterstützung unbekannter Generationen der eGK**

Falls die Version einer eGK der Generation G2 oder höher entspricht, dem Fachmodul ePA aber unbekannt ist, MUSS das Fachmodul ePA die unbekannte Version als die aktuellste ihm bekannte Version interpretieren und versuchen, die Anfrage zu bearbeiten.  
[<=]

**A\_14221 - FM ePA: Übergreifende Anforderung - Unterstützte Generationen der eGK - Fehler**

Falls zur Durchführung einer Operation eine eGK kleiner der Generation G2 verwendet wird, MUSS das Fachmodul ePA mit dem Code 115 gemäß `Tab_FM_ePA_011` abbrechen.  
[<=]

**A\_14414 - FM ePA: Übergreifende Anforderung - Fehlende Smartcard**

Falls auf eine zur Durchführung einer Operation benötigte Smartcard nicht zugegriffen werden kann, MUSS das Fachmodul ePA die Operation mit dem Code 4008 gemäß `Tab_FM_ePA_050` abbrechen.[<=]

**A\_14759 - FM ePA: Übergreifende Anforderung - Gesperrter Ordner DF.HCA auf der eGK**

Falls der Ordner DF.HCA einer beteiligten eGK nicht aktiv ist, MUSS das Fachmodul ePA die aufgerufene Operation mit dem Code 114 gemäß `Tab_FM_ePA_051` abbrechen.[<=]

**A\_15137 - FM ePA: Übergreifende Anforderung - Unterbindung paralleler Zugriffe auf die eGK**

Falls der Zugriffsversuch auf eine exklusiv verwendete eGK erfolgt, MUSS das Fachmodul ePA die aufgerufene Operation mit dem Code 4093 gemäß `Tab_FM_ePA_050` abbrechen.  
[<=]

**A\_14767 - FM ePA: Übergreifende Anforderung - Gesperrtes Zertifikat auf der eGK**

Falls das Zertifikat C.CH.AUT einer beteiligten eGK gesperrt ist, MUSS das Fachmodul ePA die aufgerufene Operationen mit dem Code 106 gemäß `Tab_FM_ePA_051` abbrechen.[<=]

**A\_16211 - FM ePA: Übergreifende Anforderung - Zertifikat auf der eGK nicht prüfbar**

Falls der Sperrstatus des Zertifikats C.CH.AUT einer beteiligten eGK nicht ermittelt werden konnte, MUSS das Fachmodul ePA die aufgerufene Operation mit dem Code 7213 gemäß `Tab_FM_ePA_011` abbrechen.  
[<=]

**A\_15215 - FM ePA: Übergreifende Anforderung - Prüfung von Authentizität und Echtheit der beteiligten Smartcards (C2C)**

Falls das Fachmodul ePA zum Zugriff auf einen Bereich der eGK gemäß [gemSpec\_eGK\_ObjSys\*] ein C2C gegen eine SM-B benötigt, so MUSS es das per gegenseitigem C2C durchführen. [≤]

**A\_15216 - FM ePA: Übergreifende Anforderung - Fehlerbehandlung bei nicht erfolgreicher C2C-Prüfung**

Falls eine C2C-Prüfung fehlschlägt, MUSS das Fachmodul ePA die Operation mit dem Code 7203 gemäß Tabelle Tab\_FM\_ePA\_011 abbrechen. [≤]

**Übergreifende Festlegungen zur Verwendung von kryptographischen Verfahren****A\_17483 - FM ePA: Übergreifende Anforderung - Kryptographische Verfahren für Smartcards der Generation 2**

Das Fachmodul ePA MUSS bei Smartcards der Generation 2 für alle kryptographischen Operationen RSA-basiertes Schlüsselmaterial verwenden.

[≤]

Die Authentisierungsbestätigungen mittels einer eGK der Generation 2 wird z.B. mit C.CH.AUT.R2048 erstellt, vgl [gemSpec\_Kon#TAB\_KON\_858].

**A\_17484 - FM ePA: Übergreifende Anforderung - Kryptographische Verfahren für Smartcards ab Generation 2.1**

Das Fachmodul ePA MUSS bei Smartcards ab Generation 2.1 für alle kryptographischen Operationen ECC-basiertes Schlüsselmaterial verwenden.

[≤]

Die Authentisierungsbestätigungen mittels einer eGK ab Generation 2.1 wird z.B. mit C.CH.AUT.E256 erstellt, vgl [gemSpec\_Kon#TAB\_KON\_858].

**Übergreifende Festlegungen zur Verwendung von Schlüsseln****A\_16193 - FM ePA: Übergreifende Anforderung - Vorgaben Aktenschlüssel und Kontextschlüssel - Fehler**

Falls die Vorgaben aus [A\\_15705](#)#1 hinsichtlich der geforderten Schlüssellänge nicht erfüllt werden, MUSS das Fachmodul ePA die aufgerufene Operation mit dem Code 7214 gemäß Tab\_FM\_ePA\_011 abbrechen.

[≤]

**Übergreifende Festlegungen zur Performanz**

Die für das Fachmodul ePA relevanten Vorgaben zur Performanz befinden sich in dem Dokument [gemSpec\_Perf#4.1.2.1].

**Übergreifende Festlegung zur Nutzung der Basisfunktionalität des Konnektors****A\_15867 - FM ePA: Übergreifende Anforderung - Verwendung der Basisfunktionalität des Konnektors zur Schlüsselerzeugung**

Das Fachmodul ePA MUSS zur Erzeugung von Schlüsseln die Basisfunktionalität des Konnektors verwenden. [≤]

Zur Erzeugung von Schlüsseln kann TUC\_KON\_072 „Daten symmetrisch verschlüsseln“ verwendet werden, welcher als Rückgabewert einen symmetrischen Schlüssel liefert.

**A\_18165 - FM ePA: Übergreifende Anforderung - Verwendung der Basisfunktionalität des Konnektors zur Kommunikation mit einem SGD**

Das Fachmodul ePA MUSS bei der Kommunikation mit einem SGD für die Schlüsselableitung gemäß A\_17777 die Basisfunktionalität des Konnektors verwenden. [≤]

**A\_15894 - FM ePA: Übergreifende Anforderung - Verwendung der Basisfunktionalität des Konnektors zur Kommunikation mit der VAU bei Schlüsselaushandlung**

Das Fachmodul ePA MUSS bei der Kommunikation mit der VAU für die Schlüsselaushandlung gemäß [A\\_15549](#) die Basisfunktionalität des Konnektors verwenden. [≤]

**A\_15895 - FM ePA: Übergreifende Anforderung - Verwendung der Basisfunktionalität des Konnektors zur Kommunikation mit der VAU bei Schlüsselableitung**

Das Fachmodul ePA MUSS zur Kommunikation mit der VAU bei der Schlüsselableitung gemäß [A\\_15549](#) die Basisfunktionalität des Konnektors verwenden. [≤]

**A\_14748 - FM ePA: Übergreifende Anforderung - Verwendung des Verschlüsselungsdienstes**

Das Fachmodul ePA MUSS zur Ver- und Entschlüsselung von Dokumenten und Dokumenten-, Akten- und Kontextschlüssel den Verschlüsselungsdienst des Konnektors nutzen. [≤]

Die fachlichen Schnittstellen zur Nutzung des Verschlüsselungsdienstes im Konnektor sind in [gemSpec\_Kon#4.1.7] beschrieben.

**A\_15891 - FM ePA: Übergreifende Anforderung - Verwendung des Zertifikatsdienstes**

Das Fachmodul ePA MUSS zur Prüfung von Zertifikaten den Zertifikatsdienst des Konnektors verwenden. [≤]

Die fachlichen Schnittstellen zur Nutzung des Zertifikatsdienstes im Konnektor sind in [gemSpec\_Kon#4.1.9] beschrieben.

**A\_15892 - FM ePA: Übergreifende Anforderung - Verwendung des Signaturdienstes**

Das Fachmodul ePA MUSS zur Erstellung und Prüfung von Signaturen den Signaturdienst des Konnektors verwenden. [≤]

Die fachlichen Schnittstellen zur Nutzung des Signaturdienstes im Konnektor sind in [gemSpec\_Kon#4.1.8] beschrieben.

**A\_15135 - FM ePA: Übergreifende Anforderung - Verwendung des Namensdienstes**

Das Fachmodul ePA MUSS für DNS-Abfragen den Namensdienst des Konnektors nutzen. [≤]

Die fachlichen Schnittstellen zur Nutzung des Namensdienstes im Konnektor sind in [gemSpec\_Kon#4.2.6] beschrieben.

**A\_15136 - FM ePA: Übergreifende Anforderung - Verwendung des Zugriffsberechtigungsdienstes**

Das Fachmodul ePA MUSS zur Prüfung der Berechtigungen zum Zugriff auf vom Konnektor verwaltete Ressourcen den Zugriffsberechtigungsdienst des Konnektors nutzen. [≤]

Die fachlichen Schnittstellen zur Nutzung des Zugriffsberechtigungsdienstes im Konnektor sind in [gemSpec\_Kon#4.1.1] beschrieben.

#### **A\_14710 - FM ePA: Übergreifende Anforderung - Verwendung des Protokollierungsdienstes**

Das Fachmodul ePA MUSS für Log-Einträge den Protokollierungsdienst des Konnektors nutzen.[<=]

Die fachlichen Schnittstellen zur Nutzung des Protokollierungsdienstes im Konnektor sind in [gemSpec\_Kon#4.1.10] beschrieben.

#### **A\_15194 - FM ePA: Übergreifende Anforderung - Verwendung des Kartendienstes**

Das Fachmodul ePA MUSS für Interaktion mit Smartcards den Kartendienst des Konnektors nutzen.[<=]

Die fachlichen Schnittstellen zur Nutzung des Kartendienstes im Konnektor sind in [gemSpec\_Kon#4.1.5] beschrieben.

#### **A\_15535 - FM ePA: Übergreifende Anforderung - Verwendung des TLS-Dienstes des Konnektors**

Das Fachmodul ePA MUSS zum Aufbau und Abbau einer TLS-Verbindung den TLS-Dienst des Konnektors nutzen.  
[<=]

Die fachlichen Schnittstellen zur Nutzung des TLS-Dienstes sind in [gemSpec\_Kon#4.1.11] beschrieben.

#### **A\_15677 - FM ePA: Übergreifende Anforderung - Verwendung des Zeitdienstes des Konnektors**

Das Fachmodul ePA MUSS zur Ermittlung der Systemzeit den Zeitdienst des Konnektors nutzen.[<=]

Die fachlichen Schnittstellen zur Nutzung des Zeitdienstes sind in [gemSpec\_Kon#4.2.5] beschrieben.

## **6.2 IHE**

Das Aktensystem, mit dem die Operationen des Fachmoduls kommunizieren, wird durch die HomeCommunityID festgelegt. Diese wird als Teil des RecordIdentifier entweder über Aufrufparameter oder SOAP-Header übertragen. Kapitel 6.2 beschreibt alle IHE-Akteure der Fachanwendung ePA.

#### **A\_14374-01A~~14374~~ - FM ePA: Übergreifende Anforderung IHE - Profile, Akteure und Optionen**

Das Fachmodul ePA MUSS die in der folgenden Tabelle gelisteten Profile, Akteure und Optionen unterstützen:

**Tabelle 3: Tab\_FM\_ePA\_002 Profile, Akteure und Optionen des Webservices PHRService**

Profil	Akteur	IHE-Option	Erläuterung
XCA gemäß [IHE-ITI-TF]	Initiating Gateway	XDS Affinity Domain Option	Die Option wird benötigt, um IHE-konformes Suchen [ITI-18] und Herunterladen



			von Dokumenten [ITI-43] zu ermöglichen.
RMD gemäß [IHE-ITI-RMD]	Document Repository	Keine	Keine Optionen benötigt.
	Document Administrator* (ggü. ePA-Aktensystem)	Remote Repository Option	Option wird benötigt, damit das Fachmodul ePA die Löschanfrage an das ePA-Aktensystem weiterreichen kann.
RMU gemäß [IHE-ITI-RMU]	Update Responder	Forward Update	Option <del>wird</del> <u>wurde in ePA 1.1</u> benötigt, um Update-Nachricht weiterzuleiten an XCA Responding Gateway der Dokumentenverwaltung. Die Option erzwingt eine Gruppierung mit einem RMU Update Initiator. <u>Die Funktion wird in ePA 2.0 nicht mehr unterstützt und mit einem Fehler beendet.</u>
	<del>Update Initiator</del>	<del>Keine</del>	<del>Keine Optionen benötigt.</del>
APPC gemäß [IHE-ITI-APPC]	Content Creator*	Keine	Keine Optionen benötigt.
XCDR gemäß [IHE-ITI-XCDR]	XCDR Initiating Gateway	<del>Keine</del> <u>Document Replacement Option, Document Addendum Option gemäß einer XDS.b Document Source</u>	<del>Keine Option benötigt.</del> <u>Die Document Replacement Option wird benötigt, um Dokumente durch eine neue Version zu ersetzen. Document Addendum Option wird benötigt, um Dokumente verschiedener Formate als Ergänzung bestehender Dokumente unter Verwendung der „Append“-</u>



			<a href="#">Association zu kennzeichnen.</a>
XDR gemäß [IHE-ITI-TF]	Document Recipient	Keine	Keine Optionen benötigt.
XUA gemäß [IHE-ITI-TF]	X-Service User (ggü. ePA-Aktensystem)*	Keine	Keine IHE Optionen benötigt. Erweiterung um die SAML-Attribute Subject-ID, Organization-ID, Organization

Legende: Mit "\*" gekennzeichnete Akteure haben keine Auswirkungen auf die Außenschnittstelle zu Primärsystemen, sondern nur auf Umsetzung der einzelnen Operationen durch das Fachmodul

【<=】

*Hinweis: Alle spezifizierten Anforderungen der IHE ITI-Akteure in Abschnitt 6.2. definieren das zu implementierende Verhalten an den Außenschnittstellen `PHRService` sowie `PHRManagementService`. Dies schließt keine zusätzlichen implementierten IHE-Funktionalitäten innerhalb des ePA-Fachmoduls aus. Um die Anforderungen an den Datenschutz zu gewährleisten, dürfen auch bei der Verwendung weiterer IHE-Funktionalitäten weder medizinische noch personenbezogene Daten geloggt werden, d.h. es gilt A\_14155*

#### **A\_17879 - FM ePA: Übergreifende Anforderung IHE - Außenverhalten der IHE ITI-Implementierung**

Falls über die in Tab\_FM\_ePA\_002 genannten IHE ITI-Akteure und Optionen zusätzliche IHE ITI-Akteure und Optionen implementiert werden, DARF das Fachmodul ePA NICHT von der Definition des Außenverhaltens von `PHRService` und `PHRManagementService` abweichen oder anderweitig Nachrichten an Komponenten außerhalb des Fachmoduls ePA kommunizieren.

【<=】

*Hinweis: Sofern zusätzliche Funktionalität im Fachmodul ePA implementiert ist, muss diese vollständig dokumentiert werden (inkl. Begründung, warum sie nicht ausführbar ist), um eine Prüfung nach der Technischen Richtlinie zu ermöglichen.*

**A\_14354 - FM ePA: Übergreifende Anforderung IHE - Keine Prüfung der Metadaten-Profilierung**

Das Fachmodul ePA DARF die Metadaten von IHE-Transaktionen nach [gemSpec\_DM\_ePA#2.1.4] über das XML-Schema ihrer zugehörigen WSDL-Datei hinaus NICHT prüfen.

[<=]

Eine Schemaprüfung der Metadaten als übergebenen Parameter findet nur im Rahmen der Schemaprüfung der Nachricht durch den zugehörigen Webservice PHRService statt. Die darüberhinausgehende, Prüfung der Metadaten gemäß der IHE-Profilierung in [gemSpec\_DM\_ePA#2.1.4] erfolgt im ePA-Aktensystem.

**A\_16220 - FM ePA: Übergreifende Anforderung IHE - Dokumenten-Codierung**

Das Fachmodul ePA MUSS gemäß den Anforderungen von [IHE-ITI-TF2x#V.3.6] zur Übertragung von Dokumenten eine Kodierung mittels MTOM/XOP [MTOM] verwenden.

[<=]

## 6.3 Lokalisierung von ePA-Aktensystemen

Die Versicherten haben das Recht, sich ihr Aktensystem frei unter den am Markt bestehenden Anbietern ePA-Aktensystem auszuwählen und zu wechseln. Dies bedeutet, dass vor dem Zugriff auf eine Akte immer der passende Anbieter inklusive der URL des Aktendienstes und der Endpunkte über den Namensdienst der zentralen TI abgefragt werden muss.

Das ePA-Aktensystem wird durch die HomeCommunityID adressiert, welche Bestandteil des `RecordIdentifier` (siehe [gemSpec\_DM\_ePA#2.2]) ist.

**A\_13839 - FM ePA: Lokalisierung - ePA-Aktensystem und Komponenten**

Das Fachmodul ePA MUSS die zur Kommunikation mit den Komponenten

- Zugangsgateway des Versicherten,
- Autorisierung ,
- Dokumentenverwaltung,
- SGD 1 und
- SGD 2

eines ePA-Aktensystems notwendigen Lokalisierungsinformationen per DNS-Abfrage nach den in [gemSpec\_Aktensystem#Tab\_ePA\_Service Discovery] und [gemSpec\_Aktensystem#Tab\_ePA\_FQDN] dargestellten Parametern ermitteln.

[<=]

**A\_14025 - FM ePA: Lokalisierung - ePA-Aktensystem und Komponenten - Fehler**

Fallsalle zur Durchführung einer Operation benötigten Lokalisierungsinformationen nicht vorliegen, MUSS das Fachmodul ePA die aufgerufene Operation mit dem Code 7200 gemäß Tab\_FM\_ePA\_011 abrechnen.[<=]

Das Fachmodul ePA kann die Lokalisierungsinformationen unabhängig von der Nutzung seiner Schnittstellen abrufen, zwischenspeichern und wiederverwenden. Es ist z.B. denkbar, dass das Fachmodul ePA die Lokalisierungsinformationen in der Bootup-Phase des Konnektors abruft.

779

## 780 6.4 Aufrufkontext und Auswahl eines SM-B

781 Die Operationen des Fachmoduls ePA werden von Mandanten mit unterschiedlichen  
 782 Berechtigungen aufgerufen und benötigen Zugriff auf vom Konnektor verwaltete  
 783 Ressourcen, wie z.B. Kartenterminals und SM-Bs. Daher muss bei jedem Aufruf vom  
 784 Clientsystem ein Aufrufkontext übergeben werden, anhand dessen der Konnektor die  
 785 Zugriffsberechtigung gegen das vom Administrator konfigurierte Informationsmodell  
 786 prüfen kann. Falls die Operation einen Login im ePA-Aktensystem mittels SM-B erfordert,  
 787 wird diese durch den Mandanten, den der Aufrufkontext bestimmt, ebenfalls über das  
 788 Informationsmodell ermittelt.

789 Der Aufrufkontext wird üblicherweise im Request als Parameter übertragen (vgl.  
 790 [PHRManagementService.wsdl]). Um die Verwendung bereits vorhandener IHE-  
 791 Funktionalität in Primärsystemen zu erleichtern bzw. sogar ohne Anpassungen zu  
 792 unterstützen, bietet das Fachmodul folgende Möglichkeiten:

- 793 • In weniger komplexen Einsatzumgebungen kann bei der Nutzung des Webservices  
 794 PHRService auf die Übertragung des Aufrufkontexts verzichtet und stattdessen ein  
 795 Default-Aufrufkontext verwendet werden. Dieser wird vorab auf dem Konnektor  
 796 eingerichtet und bezieht sich immer genau auf einen Mandanten, ein Clientsystem  
 797 und einen Arbeitsplatz.
- 798 • In Einsatzumgebungen, welche verschiedene Aufrufkontexte benötigen, wird der  
 799 zu verwendende Aufrufkontext ~~als SAML-Token~~ im SOAP-Header ~~unter Nutzung~~  
 800 ~~des IHE Profils "XUA" als SAML-Token~~ übertragen.

### 801 **A\_14947 - FM ePA: Login - Ermittlung des Aufrufkontexts via Aufrufparameter**

802 Der Webservice PHRManagementService MUSS den Aufrufkontext gemäß  
 803 [ConnectorContext.xsd] anhand des im Aufruf übergebenen Parameters Context  
 804 bestimmen. [ $\leq$ ]

### 805 **A\_15142 - FM ePA: Login - Ermittlung des Aufrufkontexts via SOAP-Header**

806 Der Webservice PHRService MUSS den Aufrufkontext gemäß [ConnectorContext.xsd]  
 807 anhand der nach Tab\_FM\_ePA\_005 übertragenen SOAP-Header bestimmen.  
 808 [ $\leq$ ]

### 809 **A\_15142-01 - FM ePA: Login - Ermittlung des Aufrufkontexts via SOAP-Header -** 810 **PHRService Version 2.x**

811 Der Webservice PHRService Version 2.x MUSS den Aufrufkontext gemäß  
 812 [ConnectorContext.xsd] anhand der nach Tab\_FM\_ePA\_005 2.x übertragenen SOAP-  
 813 Header bestimmen. [ $\leq$ ]

### 814 **Default-Aufrufkontext**

### 815 **A\_14084 - FM ePA: Login - Bereitstellung Default-Aufrufkontext**

816 Das Fachmodul ePA MUSS im Informationsmodell des Konnektors einen Default-  
 817 Aufrufkontext für die Nutzung des Webservices PHRService bereitstellen mit:

- 818 • MandantId = "Mandant\_ePA\_Default"
- 819 • ClientsystemId = "Clientsystem\_ePA\_Default"
- 820 • WorkplaceId = "Workplace\_ePA\_Default"

821 [ $\leq$ ]

### A\_14103 - FM ePA: Login - Konfiguration Default-Aufrufkontext

Der Hersteller des Fachmoduls ePA MUSS im Handbuch die Konfiguration des Default-Aufrufkontexts durch den Administrator beschreiben. [≤]

### A\_14948 - FM ePA: Login - Verwendung des Default-Aufrufkontexts bei fehlenden SOAP-Headern

Falls keine SOAP-Header übergeben wurden, MUSS der Webservice PHRService als Aufrufkontext den Default-Aufrufkontext aus dem Informationsmodell des Konnektors auswählen. [≤]

Für die IHE-Schnittstelle (PHRService) wird die Komfortfunktion eines Default-Aufrufkontexts angeboten, um die Verwendung bereits vorhandener IHE-Funktionalität in Primärsystemen zu erleichtern bzw. sogar ohne Anpassungen zu unterstützen. Der Webservice PHRManagement hingegen folgt der in den anderen Fachmodulen des Konnektors üblichen Vorgehensweise zur Übertragung des Aufrufkontexts durch die Primärsysteme via Aufrufparameter.

### Prüfung der Zugriffsberechtigung auf vom Konnektor verwaltete Ressourcen

#### A\_13941 - FM ePA: Login - Zugriffsberechtigung auf vom Konnektor verwaltete Ressourcen

Das Fachmodul ePA MUSS vor Durchführung einer fachlichen Operation die Zugriffsberechtigung des aufrufenden Primärsystems anhand des Aufrufkontexts prüfen. [≤]

#### ~~A\_14107-02A\_14107-01~~ - FM ePA: Login - Zugriffsberechtigung auf vom Konnektor verwaltete Ressourcen - Fehler

Falls bei der Prüfung der Zugriffsberechtigung auf ~~das ausgewählte SM-B~~ oder die durch cardHandle adressierte eGK ein Fehler zurückgegeben wird, MUSS das Fachmodul ePA die Operation mit dem Code 7206 gemäß Tab\_FM\_ePA\_011 abbrechen. [≤]

### Auswahl eines SM-B

Alle Operationen, außer GetHomeCommunityID, benötigen in ihrem Ablauf ein oder auch mehrere SM-Bs für die folgende Funktionalität:

**Tabelle 4: Tab\_FM\_ePA\_034 Übersicht der Funktionen, die ein SM-B benötigen, mit Zuordnung zu den aufrufenden Operationen und ob die SM-B eine Berechtigung zum Zugriff haben muss**

Funktion (Wofür wird ein SM-B benötigt?)	Operation (Welche Operationen benötigen die Funktionalität?)
<b>Authentisierung am ePA-Aktensystem</b> Zur Erstellung (Signatur) einer AuthenticationAssertion benötigt das Fachmodul ePA ein gültiges SM-B.	Alle Operationen des Webservices PHRService und die Operation GetAuthorizationList
<b>Autorisierung am ePA-Aktensystem</b> Zum Abruf des Chiffrats, welches Akten- und Kontextschlüssel enthält, benötigt das Fachmodul ePA eine AuthenticationAssertion	Alle Operationen des Webservices PHRService

<p>für ein gültiges SM-B, dessen Telematik-ID zuvor zum Zugriff auf die Patientenakte berechtigt wurde.</p> <p>Zum Abruf der Schlüssel gemäß [gemSpec_SGD_ePA], mit denen das Chiffprat entschlüsselt werden kann, benötigt das Fachmodul ePA ein gültiges SM-B, dessen Telematik-ID zuvor zum Zugriff auf die Patientenakte berechtigt wurde.</p>	
<p><b>C2C mit eGK</b></p> <p>Zur Freischaltung von PrK.CH.AUT (eGK) bei der Authentisierung wird ein beliebiges SM-B benötigt.</p>	<p>ActivateAccount, RequestFacilityAuthorization</p>
<p><b>Berechtigungsvergabe</b></p> <p>Die Berechtigungsvergabe an eine LEI erfolgt für die Telematik-ID des ausgewählten SM-B.</p>	<p>RequestFacilityAuthorization</p>

856

857 Die folgenden Anforderungen beziehen sich auf die Auswahl eines SM-B zur  
 858 Authentisierung, zur Berechtigungsvergabe und zur Durchführung eines C2C mit einer  
 859 eGK. Die Auswahl eines SM-B zur Autorisierung wird im Kapitel 6.5.4 behandelt.

860

861 **A\_15614-01A\_15614 - FM ePA: Übergreifende Anforderung - Ermittlung eines**  
 862 **SM-B**

863 Das Fachmodul ePA MUSS zu jedem Aufrufkontext ein im Informationsmodell des  
 864 Konnektors konfiguriertes, freigeschaltetes und zugriffsberechtigtes SM-B des Mandanten  
 865 ermitteln.

866 [**<=**]

867 **A\_17928-01A\_17928 - FM ePA: Übergreifende Anforderung - Ermittlung eines**  
 868 **SM-B - Prüfung OID**

869 Das Fachmodul ePA MUSS eine SM-B ermitteln, welche im Zertifikat C.HCI.OSIG im Feld  
 870 `ProfessionOID` der ZertifikatsExtension `Admission` mindestens eine der zulässigen  
 871 Autorisierungsempfänger-Rollen gemäß [gemSpec\_OID#Tab\_PKI\_402] und  
 872 [gemSpec\_OID#Tab\_PKI\_403]

- 873 • oid\_praxis\_arzt
- 874 • oid\_zahnarztpraxis
- 875 • oid\_praxis\_psychotherapeut
- 876 • oid\_krankenhaus
- 877 • oid\_oeffentliche\_apotheke
- 878
- 879 • oid\_krankenhausapothekeinstitution\_pflege
- 880 • oid\_bundeswehrapothekegeburtshilfe
- 881 • ~~oid\_mobile\_einrichtung\_rettungsdienst~~
- 882 • oid\_praxis\_physiotherapeut

- [oid\\_gesundheitsdienst](#)
- [oid\\_arbeitsmedizin](#)
- [oid\\_vorsorge\\_reha](#)
- [oid\\_sanitaetsdienst\\_bundeswehr](#)

enthalten ist.

[<=]

#### **A\_15615 - FM ePA: Übergreifende Anforderung - Ermittlung eines SM-B - Fehler**

Falls bei der Ermittlung eines SM-B ein Fehler auftritt, MUSS das Fachmodul ePA die Operation mit dem Code 7205 gemäß Tab\_FM\_ePA\_011 abbrechen.

[<=]

Ein SM-B wird als freigeschaltet betrachtet, wenn sich das Objekt PIN.SMC im erhöhten Sicherheitszustand befindet.

## **6.5 Login**

Der Login nach [gemSysL\_ePA#3.4.2] in ein ePA-Aktensystem erfolgt bei Bedarf durch das Fachmodul ePA und beinhaltet die Vorbereitungen zur Durchführung von Fachoperationen. Dazu gehören das Abrufen der Authentifizierungs- und Autorisierungsbestätigungen sowie das Initialisieren und Öffnen des Aktenkontextes. Für den aufrufenden Akteur ist die Login-Funktionalität nicht explizit nutzbar, sondern wird implizit innerhalb anderer Operationsaufrufe ausgeführt. Dies bedeutet, dass eventuelle Fehlersituationen beim Login in den Rückgabewerten der jeweiligen Fachoperationen sichtbar werden.

Das Ergebnis eines vollständigen Logins ist

1. das Anlegen einer neuen oder die Nutzung einer vorhandenen Aktensession,
2. die Authentisierung des Nutzers (LEI oder Versicherter/Vertreter) gegenüber dem ePA-Aktensystem,
3. die Autorisierung des Nutzers gegenüber dem ePA-Aktensystem und
4. das Starten und die Initialisierung einer vertrauenswürdigen Ausführungsumgebung (VAU) im ePA-Aktensystem.

Punkt 4 ist insofern optional, als dass die Verbindung zur Dokumentenverwaltung nicht zur Durchführung aller Operationen erforderlich ist.

### **6.5.1 Aktensession**

Eine Aktensession umfasst die zur Kommunikation mit dem ePA-Aktensystem notwendigen Daten eines Operationsaufrufes (Abläufe, Parameter, Rückgabewerte, interne Variablen und Zustände, Referenzen auf Smartcards, Schlüsselmaterialien, Token, etc.). Je nach Komponenten und Art der Authentisierung des Nutzers (via SM-B oder eGK) werden die folgenden Daten benötigt:

921 **Tabelle 5: Tab\_FM\_ePA\_001 Daten zur Kommunikation mit den Komponenten des ePA-**  
 922 **Aktensystems (abhängig vom Nutzer)**

Datenfeld	Herkunft	Beschreibung
RecordIdentifier	Primärsystem (als Parameter übergeben)	Kennung der Akte des Versicherten beim jeweiligen Anbieter ePA-Aktensystem im Format von RecordIdentifier gemäß [gemSpec_DM_ePA#2.2]
Aufrufkontext	Primärsystem (als Parameter übergeben)	MandantId, CsId, WorkplaceId, UserId (optional)
Telematik-ID	Informationsmodell des Konnektors	Identität einer LEI in einem SM-B
SM-B (falls Authentisierung via SM-B)	Informationsmodell des Konnektors	SM-B, die zur Authentifizierung gegenüber dem ePA-Aktensystem verwendet wird
eGK (falls Authentisierung via eGK)	Primärsystem (als Parameter übergeben)	eGK, die zur Authentifizierung gegenüber dem ePA-Aktensystem verwendet wird
AuthenticationAssertion	Authentisierung via <ul style="list-style-type: none"> <li>• SM-B: Fachmodul</li> <li>• eGK: Komponente Zugangsgateway für Versicherte des ePA-Aktensystems</li> </ul>	Authentifizierungsbestätigung als Voraussetzung für die Autorisierung
AuthorizationAssertion	Komponente Autorisierung des ePA-Aktensystems (I_Authorization::getAuthorizationKey)	Die AuthorizationAssertion ist eine signierte Autorisierungsbestätigung für einen Nutzer und enthält Informationen über die Art und den Umfang der in der Komponente Autorisierung hinterlegten Autorisierung. Sie ist Base64-codiert und wird



		innerhalb des Fachmoduls nicht ausgewertet.
RecordKey	Komponente Autorisierung des ePA-Aktensystems (I_Authorization::getAuthorizationKey)	entschlüsselter Aktenschlüssel
ContextKey	Komponente Autorisierung des ePA-Aktensystems (I_Authorization::getAuthorizationKey)	entschlüsselter Kontextschlüssel
VAU-Assets	Kryptographische Geheimnisse (z.B. Ableitungsschlüssel, Authentisierungstoken), die beim Aufbau der sicheren Verbindung zur VAU ( <a href="#">A_17225</a> ) erzeugt bzw. ausgetauscht werden.	z.B. Ableitungsschlüssel, Authentisierungstoken
SGD-Assets	Kryptographische Geheimnisse, die beim Aufbau der sicheren Verbindung zu einem SGD ( <a href="#">A_17777</a> ) erzeugt bzw. ausgetauscht werden.	z.B. kurzlebige ECIES-Schlüssel

923

#### 924 **A\_13677 - FM ePA: Aktensession - Trennung von Operation**

925 Das Fachmodul ePA MUSS alle Operationsaufrufe sowie die den Operationen zugehörige  
926 Aktensession voneinander trennen. [ $\leq$ ]

#### 927 **A\_15143 - FM ePA: Aktensession - Temporäre Speicherung und Wiederverwendung (SM-B)**

928 Das Fachmodul ePA KANN auf Basis des Tupels (Telematik-ID der zur Authentisierung  
929 verwendeten SM-B, RecordIdentifier) eine Aktensession temporär speichern und  
930 wiederverwenden. [ $\leq$ ]

#### 932 **A\_15144 - FM ePA: Aktensession - Temporäre Speicherung und Wiederverwendung (eGK)**

933 Das Fachmodul ePA KANN auf Basis des Tupels (Versicherten-ID einer zur  
934 Authentisierung verwendeten eGK, RecordIdentifier) eine Aktensession temporär  
935 speichern und wiederverwenden.

936

937

938 [ $\leq$ ]

939 Sowohl der Aufruf der Operation EjectCard als auch das Ziehen der Karte aus dem  
940 Kartenterminal führt zum Entfernen der eGK aus dem Kartenterminal.



**A\_17949-01 - FM ePA: Aktensession - Löschen der Aktensession bei Entfernen der eGK**

Falls die eGK aus dem Kartenterminal entfernt wird, MUSS das Fachmodul ePA die Aktensession der eGK beenden, die Operation `I_Document_Management_Connect::CloseContext` gemäß `[I_Document_Management_Connect_Service.wsdl]` des zugehörigen ePA-Aktensystems aufrufen und alle dazugehörigen Daten löschen.[<=]

**6.5.2 Authentisierung mittels SM-B**

Die Authentisierung mittels SM-B findet für die folgenden Operationen statt:

- `PHRService`
  - `putDocuments`
  - `find`
  - `getDocuments`
  - `removeDocuments`
  - `updateDocumentSet`
- `PHRManagementService`
- `GetAuthorizationList`

Die Authentisierung LEI mit dem ausgewählten SM-B erfolgt durch das Fachmodul ePA. Hierzu erzeugt das Fachmodul ePA ein SAML-Token, welches dem IHE-Profil "XUA" [IHE-ITI-TF] genügt und als `AuthenticationAssertion` bezeichnet wird. Das Token wird mit dem für LEI ausgewählten SM-B signiert.

Die Authentisierung LEI im Fachmodul ePA muss nur einmalig erfolgen, auch wenn die LEI auf verschiedene Akten zugreifen möchte. Aus diesem Grunde kann die `AuthenticationAssertion` außerhalb einer Aktensession gespeichert und wiederverwendet werden.

**Ermittlung der Karte für die Authentisierung**

Die Ermittlung der SM-B für die Authentisierung wird in Kapitel 6.4 beschrieben.

**Erstellung der AuthenticationAssertion****A\_14927 - FM ePA: Authentisierung mit SM-B - Erstellung des SAML-Token**

Das Fachmodul ePA MUSS für die Authentisierung mit einem SM-B als Authentifizierungsbestätigung eine SAML2-Assertion gemäß dem IHE-Profil "XUA" [IHE-ITI-TF] und `[gemSpec_TBAuth#TAB_TBAuth_03]` erstellen und dabei folgende Vorgaben beachten:

- das *Issuer* Element muss als Aussteller des Token den Wert `"urn:epa:telematik:fmePA"` enthalten
- die eingebettete Signatur *ds:Signature* wird mit dem C.HCI.OSIG Zertifikat der ausgewählten SM-B unter Verwendung des Signatordienstes des Konnektors erstellt. Die Signatur enthält im *ds:KeyInfo* Element das verwendete Signaturzertifikat.
- das Element *saml2:Subject/saml2:NameID* muss auf Basis des C.HCI.OSIG Zertifikats gebildet werden

- das Attribut *saml2:Subject/saml2:SubjectConfirmation/@Method* muss auf den Wert "urn:oasis:names:tc:SAML:2.0:cm:bearer" gesetzt werden
- das Attribut *saml2:Conditions/@NotBefore* muss auf die Systemzeit gesetzt werden
- das Attribut *saml2:Conditions/@NotOnOrAfter* muss auf (Systemzeit+24 Stunden) gesetzt werden
- das Element *saml2:Conditions/saml2:AudienceRestriction/saml2:Audience* muss auf die FQDN des Anbieters des Aktensystems gesetzt werden
- das Element *saml2:AuthnStatement/saml2:AuthnContext/saml2:AuthnContextClassRef* muss auf den Wert "urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard" gesetzt werden

[<=]

#### **A\_15638 - FM ePA: Authentisierung mit SM-B - Behauptungen im SAML-Token**

Das Fachmodul ePA MUSS die für die Authentisierung mit einem SM-B als Authentifizierungsbestätigung erstellte SAML2-Assertion im Element *AttributeStatement* mit den Behauptungen gemäß [gemSpec\_TBAuth#TAB\_TBAuth\_02\_1] befüllen und dabei folgende Vorgaben beachten:

- die Behauptungen müssen auf Basis des C.HCI.OSIG Zertifikats gebildet werden
- die in der Tabelle angegebenen Behauptungen müssen enthalten sein, sofern sie aus dem zugrundeliegenden Zertifikat entnommen werden können
- die Behauptung "urn:gematik:subject:organization-id" muss enthalten sein und basierend auf der RegistrationNumber (Telematik-ID) gebildet werden. Das Attribut *Attribute/@NameFormat* muss dabei den Wert "urn:oasis:names:tc:SAML:2.0:attrname-format:uri" haben.

[<=]

Die SAML2-Assertion gemäß A\_14927 wird auch zur Kommunikation mit der Komponente Dokumentenverwaltung verwendet.

#### **A\_15202 - FM ePA: Authentisierung mit SM-B - Wiederverwendung der AuthenticationAssertion**

Das Fachmodul ePA KANN die AuthenticationAssertion zur Authentisierung einer LEI über ihre gesamte Gültigkeitsdauer hinweg auch außerhalb einer Aktensession zwischenspeichern und wiederverwenden.[<=]

#### **A\_15203 - FM ePA: Authentisierung mit SM-B - Löschen der AuthenticationAssertion**

Das Fachmodul ePA MUSS die AuthenticationAssertion zur Authentisierung einer LEI spätestens nach Ablauf ihrer Gültigkeitsdauer löschen.[<=]

### **6.5.3 Authentisierung mittels eGK**

Die Authentisierung mittels eGK findet für die folgenden Operationen statt:

- PHRManagementService
  - ActivateAccount
  - RequestFacilityAuthorization

Für die Anmeldung des Versicherten oder seines berechtigten Vertreters mit seiner eGK wird eine 2-Faktor-Authentisierung (eGK + PIN) verwendet. Das Fachmodul ePA baut anschließend eine TLS-Verbindung zur Komponente Zugangsgateway für Versicherte auf. Durch Nutzung des Interfaces `I_Authentication_Insurant::login` an der Komponente wird eine Authentifizierungsbestätigung (`AuthenticationAssertion`) angefordert. Bei dieser Form der Authentisierung wird kryptographisches Material der eGK verwendet. Hierfür ist eine Freischaltung der eGK durch PIN-Eingabe erforderlich.

### Freischaltung der eGK

#### **A\_14928 - FM ePA: Authentisierung mit eGK - PIN-Eingabe**

Falls für die Authentisierung mittels eGK die PIN.CH nicht freigeschaltet ist, MUSS das Fachmodul ePA die PIN-Verifikation der durch `EhcHandle` adressierten eGK durchführen. [ $\leq$ ]

#### **A\_14945-01 - FM ePA: Authentisierung mit eGK - PIN-Eingabe - Fehler**

Falls die Verifikation von PIN.CH fehlschlägt, MUSS das Fachmodul ePA die aufgerufene Operation mit einem Fehlercode gemäß `Tab_FM_ePA_033` abbrechen.

**Tabelle 6: Tab\_FM\_ePA\_033 Fehlermeldungen bei der Authentisierung mittels eGK**

Code	Bedeutung (informativ)	Ursache/Auslöser nach [gemSpec_Kon#TAB_KON_089]
7207	PIN-Verifikation gescheitert	<ul style="list-style-type: none"> <li>• 4043, 4049</li> <li>• Alle weiteren Fehlercodes, die der Kartendienst zurückgibt</li> </ul>
4063	PIN gesperrt	4063
4065	PIN transportgeschützt	4065

Die vollständige Definition des Fehlers bezeichnet durch Code ist in `Tab_FM_ePA_011` und `Tab_FM_ePA_050` beschrieben.

[ $\leq$ ]

### Aufbau der TLS-Verbindung zur Komponente Zugangsgateway für Versicherte

#### **A\_14929 - FM ePA: Authentisierung mit eGK - TLS-Verbindung zur Komponente Zugangsgateway aufbauen**

Das Fachmodul ePA MUSS zur Kommunikation mit der Komponente Zugangsgateway für Versicherte eine TLS-Verbindung aufbauen bzw. eine bestehende TLS-Verbindung nutzen. [ $\leq$ ]

#### **A\_16951 - FM ePA: Authentisierung mit eGK- Verwendung der lokalisierten URI**

Das Fachmodul ePA MUSS beim Aufbau der TLS-Verbindung zur Komponente Zugangsgateway für Versicherte deren lokalisierte Adresse verwenden. [ $\leq$ ]

#### **A\_14930 - FM ePA: Authentisierung mit eGK - TLS mit Zertifikats- und Rollenprüfung**

Das Fachmodul ePA MUSS beim Aufbau der TLS-Verbindung zur Komponente Zugangsgateway für Versicherte eine Zertifikats- und Rollenprüfung für das Zertifikatsprofil C.FD.TLS-S gemäß [gemSpec\_PKI] mit der Rolle `oid_epa_authn` gemäß [gemSpec\_OID#[GS-A 4446](#)] durchführen.

[ $\leq$ ]

## Authentifizierungsbestätigung erstellen

Das Fachmodul erstellt eine Authentifizierungsbestätigung für einen Versicherten auf der Basis des Zertifikats C.CH.AUT der eGK. Das Vorgehen und die Schnittstelle hierzu ist in [gemSpec\_Authentisierung\_Vers] beschrieben.

### A\_14838 - FM ePA: Authentisierung mit eGK - Authentifizierungsbestätigung erstellen

Das Fachmodul ePA MUSS die Erstellung einer AuthenticationAssertion gemäß Tab\_FM\_ePA\_030 umsetzen.

**Tabelle 7: Tab\_FM\_ePA\_030 Authentifizierungsbestätigung erstellen**

Schritt
1. Aufruf der Operation AuthInsurantService::LoginCreateChallenge der Komponente Zugangsgateway des Aktensystems ePA gemäß [gemSpec_Authentisierung_Vers#5.1.1.1.1 Operation login]
2. Signatur des Versicherten bzw. Vertreters (eGK) über die von der Komponente "Authentisierung Versicherter" erstellte Challenge
3. Aufruf von AuthInsurantService::LoginCreateToken der Komponente Zugangsgateway des Aktensystems ePA gemäß [gemSpec_Authentisierung_Vers#5.1.1.1.1 Operation login]

[<=]

Das Interface I\_Authentication\_Insurant::login ist in [gemSpec\_Authentisierung\_Vers#6.1 beschrieben].

### A\_14935 - FM ePA: Authentisierung mit eGK - Fehler im Aktensystem

Falls bei der Kommunikation mit der Komponente Zugangsgateway zur Authentisierung des Versicherten der Fehler "wst:RequestFailed" auftritt, MUSS das Fachmodul ePA die Operation mit dem Code 7215 gemäß Tab\_FM\_ePA\_011 abbrechen.[<=]

### A\_17123 - FM ePA: Authentisierung mit eGK - Fehler beim Aufruf Aktensystem

Falls bei der Kommunikation mit der Komponente Zugangsgateway zur Authentisierung des Versicherten ein anderer Fehler als "wst:RequestFailed" auftritt, MUSS das Fachmodul ePA die Operation mit dem Code 7400 gemäß Tab\_FM\_ePA\_011 abbrechen.[<=]

Weitere Fehlerrückgaben der Operationen AuthInsurantService::LoginCreateChallenge und AuthInsurantService::LoginCreateToken werden in [gemSpec\_Authentisierung\_Vers] spezifiziert.

## 6.5.4 Autorisierung

Die Komponente Autorisierung des lokalisierten ePA-Aktensystems prüft, ob der Zugriff auf die mit dem RecordIdentifier referenzierte Akte erlaubt ist. Dazu schickt das Fachmodul ePA die im Rahmen der Authentisierung (s.o.) ausgestellte AuthenticationAssertion an die Komponente Autorisierung und erhält nach erfolgreicher Prüfung ein Chiffprat mit Akten- und Kontextschlüssel sowie eine Autorisierungsbestätigung (AuthorizationAssertion) zur Kommunikation mit der Dokumentenverwaltung ausgehändigt. Das Chiffprat wird mit zwei gemäß

1095 [gemSpec\_SGD\_ePA] abgeleiteten Schlüsseln der SGD's entschlüsselt. Der Ablauf gliedert  
1096 sich in die folgenden Schritte:

- 1097 1. TLS-Verbindung zur Komponente Autorisierung aufbauen
- 1098 2. Aufruf der Operation `I_Authorization::getAuthorizationKey` der Komponente  
1099 Autorisierung, Übergabe der `AuthenticationAssertion` und entsprechender  
1100 Signatur im SOAP-Header gemäß [WSS-SAML]
- 1101 3. Verbindungsaufbau zu zwei SGD's und Abruf jeweils eines AES-Schlüssels
- 1102 4. Entschlüsselung von Akten- und Kontextschlüssel zur Nutzung in der Aktensession

1103

#### 1104 **Verbindungsaufbau zur Komponente Autorisierung**

1105 Im Konnektor baut das Fachmodul ePA mit Hilfe von TUC\_KON\_110 „Kartenbasierte TLS-  
1106 Verbindung aufbauen“ gemäß [gemSpec\_Kon#4.1.11.4.1] die TLS-Verbindung ohne  
1107 Clientauthentisierung und mit Rollenprüfung auf.

#### 1108 **A\_14105 - FM ePA: Autorisierung - TLS-Verbindung zur Komponente** 1109 **Autorisierung aufbauen**

1110 Das Fachmodul ePA MUSS zur Kommunikation mit der Komponente Autorisierung eine  
1111 TLS-Verbindung aufbauen bzw. eine bestehende TLS-Verbindung nutzen. [`<=`]

#### 1112 **A\_14223 - FM ePA: Autorisierung - Verbindung mit Zertifikats- und** 1113 **Rollenprüfung**

1114 Das Fachmodul ePA MUSS beim Aufbau der TLS-Verbindung zur Komponente  
1115 Autorisierung eine Zertifikats- und Rollenprüfung für das Zertifikatsprofil C.FD.TLS-S  
1116 gemäß [gemSpec\_PKI] mit der Rolle `oid_epa_authz` gemäß [gemSpec\_OID#[GS-A 4446](#)]  
1117 durchführen.  
1118 [`<=`]

#### 1119 **A\_14222 - FM ePA: Autorisierung - Verwendung der lokalisierten URI**

1120 Das Fachmodul ePA MUSS beim Aufbau der TLS-Verbindung zur Komponente  
1121 Autorisierung deren lokalisierte Adresse verwenden. [`<=`]

1122

#### 1123 **Abruf des Chiffrats für den authentisierten Nutzer (LEI oder Versicherter /** 1124 **Vertreter)**

#### 1125 **A\_14014 - FM ePA: Autorisierung Aktensession - Request SAML**

1126 Das Fachmodul ePA MUSS zur Autorisierung der Aktensession die Operation  
1127 `I_Authorization::getAuthorizationKey` gemäß [gemSpec\_Autorisierung] mit folgenden  
1128 Parametern aufrufen:  
1129

1130 **Tabelle 8: Tab\_FM\_ePA\_026 Aufrufparameter der Operation**  
1131 **`I_Authorization::getAuthorizationKey`**

Parameter	Inhalt	Beschreibung
RecordIdentifizier	[RecordIdentifizier der Aktensession]	Kennung der Versichertenakte, auf die zugegriffen werden soll
SAML:Assertion	[AuthenticationAssertion der Aktensession]	SAML2-Token zur Authentifizierung des Nutzers (LEI oder

		Versicherter) beim ePA-Aktensystem
--	--	------------------------------------

1132 [ $\leq$ ]

1133 Legende:

- 1134 • Inhalte in eckigen Klammern ([...]) sind ihrer Beschreibung nach zu ersetzen.
- 1135 • Die Parameter sind der Spezifikation [gemSpec\_Autorisierung] entnommen.

1136

1137 **A\_14243 - FM ePA: Autorisierung Aktensession - Fehler - keine Autorisierung**  
 1138 **vorhanden**

1139 Falls beim Aufruf der Operation `I_Authorization::getAuthorizationKey` eines Aktendienstes  
 1140 des Versicherten keine Berechtigung für den Nutzer im Aktenkonto hinterlegt ist  
 1141 (ACCESS\_DENIED, KEY\_ERROR), MUSS das Fachmodul ePA die Operation mit dem Code  
 1142 7209 gemäß Tab\_FM\_ePA\_011 abbrechen. [ $\leq$ ]

1143 **A\_14024 - FM ePA: Autorisierung Aktensession - Fehler**

1144 Wurde die Operation `I_Authorization::getAuthorizationKey` eines Aktendienstes des  
 1145 Versicherten mit einem anderen Fehler als ACCESS\_DENIED, oder KEY\_ERROR beendet,  
 1146 dann MUSS das Fachmodul ePA die Operation mit dem Code 7400 gemäß  
 1147 Tab\_FM\_ePA\_011 abbrechen. [ $\leq$ ]

1148 Weitere Fehlerrückgaben der Operation `I_Authorization::getAuthorizationKey` werden in  
 1149 [gemSpec\_Autorisierung] spezifiziert.

1150 **Schlüsselableitung und Entschlüsselung von Akten- und Kontextschlüssel**

1151 Die Schlüsselableitung und Entschlüsselung von Akten- und Kontextschlüssel ist in  
 1152 Kap. 6.5.6- Schlüsselableitung beschrieben.

1153 **Benachrichtigung des Primärsystem über bestehende Berechtigungen zum**  
 1154 **Zugriff auf ein Aktenkonto**

1155 **A\_15134 - FM ePA: Autorisierung Aktensession - Benachrichtigung an das**  
 1156 **Primärsystem**

1157 Wurde die Operation `I_Authorization::getAuthorizationKey` zur Autorisierung der LEI  
 1158 erfolgreich aufgerufen MUSS das Fachmodul ePA unter Verwendung des  
 1159 Systeminformationsdienstes des Konnektors ein Event mit folgendem Inhalt erzeugen:

Parameter	Inhalt
Topic	FM_EPA/POLICY_LEI
Type	Operation
Severity	Info
TelematikID	[Telematik-ID der Aktensession]
RecordID	[RecordIdentifier der Aktensession]



ValidTo	[Inhalt aus Attribut validTo von AuthorizationKey. Die Zeit wird mit dem Datentyp <code>DateTime</code> in folgendem Format angegeben: <code>yyyy-mm-ddThh:mm:ss+hh:mm</code> Es ist – gemäß ISO 8601 [ISO8601] – die lokale Zeit und die Differenz zur UTC anzugeben.]
---------	--

1160  
1161

[<=]

1162 Das Element validTo macht eine Aussage über die zeitliche Gültigkeit der übertragenen  
 1163 Schlüssel. Somit kann das Event bei einer Abonnieung durch ein Primärsystem  
 1164 verwendet werden, um Informationen über die zeitliche Gültigkeit der Berechtigung der  
 1165 LEI durch den Versicherten zu erhalten.

1166

## 1167 6.5.5 Verbindung zur Dokumentenverwaltung

1168 Alle Operationen des Webservices PHRService sowie die Operation  
 1169 RequestFacilityAuthorization benötigen einen initialisierten Aktenkontext in der  
 1170 Dokumentenverwaltung, d.h. eine Verbindung zum Verarbeitungskontext der  
 1171 Vertrauenswürdigen Ausführungsumgebung (VAU) des Versicherten wie in  
 1172 [gemSpec\_Dokumentenverwaltung#4.4] beschrieben. Das Fachmodul ePA muss dafür  
 1173 eine TLS-Verbindung zur Komponente Dokumentenverwaltung des Aktensystems, in  
 1174 welchem das Aktenkonto des Versicherten liegt, aufbauen. Die Dokumente des  
 1175 Aktenkontos werden zwischen dem Fachmodul ePA und dem Verarbeitungskontext der  
 1176 VAU in einem sicheren Kanal auf HTTP-Anwendungsschicht gemäß  
 1177 [gemSpec\_Krypt#6.4] übertragen.

1178 Die Schnittstelle der Dokumentenverwaltung wird in  
 1179 [gemSpec\_Dokumentenverwaltung#5.4] spezifiziert.

### 1180 Aufbau der TLS-Verbindung

#### 1181 A\_15531 - FM ePA: Dokumentenverwaltung - TLS-Verbindung zur Komponente 1182 Dokumentenverwaltung aufbauen

1183 Das Fachmodul ePA MUSS zur Kommunikation mit der Komponente  
 1184 Dokumentenverwaltung eine TLS-Verbindung aufbauen bzw. eine bestehende TLS-  
 1185 Verbindung nutzen.[<=]

#### 1186 A\_15532 - FM ePA: Dokumentenverwaltung - TLS mit Zertifikats- und 1187 Rollenprüfung

1188 Das Fachmodul ePA MUSS beim Aufbau der TLS-Verbindung zur Komponente  
 1189 Dokumentenverwaltung eine Zertifikats- und Rollenprüfung für das Zertifikatsprofil  
 1190 C.FD.TLS-S gemäß [gemSpec\_PKI] mit der Rolle oid\_epa\_dvw gemäß  
 1191 [gemSpec\_OID#GS-A 4446] durchführen.[<=]

#### 1192 A\_15533 - FM ePA: Dokumentenverwaltung - Verwendung der lokalisierten URI

1193 Das Fachmodul ePA MUSS beim Aufbau der TLS-Verbindung zur Komponente  
 1194 Dokumentenverwaltung deren lokalisierte Adresse verwenden.[<=]

### 1195 Aufbau eines sicheren Kanals auf HTTP-Anwendungsschicht zum 1196 Verarbeitungskontext der VAU

**A\_15199-01A\_15199 - FM ePA: Dokumentenverwaltung - sichere Verbindung zur VAU - Verfahren**

Das Fachmodul ePA MUSS für die Kommunikation mit der Schnittstelle I\_Document\_Management\_Connect der Komponente Dokumentenverwaltung eine sichere Verbindung zum Verarbeitungskontext der VAU aufbauen, gemäß den Vorgaben aus [gemSpec\_Krypt#3.15 und #6].-+-[<=]

**A\_15200 - FM ePA: Dokumentenverwaltung - sichere Verbindung zur VAU - Aufrufparameter**

Das Fachmodul ePA MUSS beim Aufbau der sicheren Verbindung zum Verarbeitungskontext der VAU die `AuthorizationAssertion` aus der Aktensession der vom Primärsystem aufgerufenen Operation als Parameter gemäß [A\\_15592](#) übergeben. [<=]

**A\_15210 - FM ePA: Dokumentenverwaltung - sichere Verbindung zur VAU mit Zertifikats- und Rollenprüfung**

Das Fachmodul ePA MUSS beim Aufbau der sicheren Verbindung zum Verarbeitungskontext der VAU eine Zertifikats- und Rollenprüfung für das vom Verarbeitungskontext empfangene Zertifikat C.FD.AUT gemäß [gemSpec\_PKI] mit der Rolle `oid_epa_vau` gemäß [gemSpec\_OID#[GS-A\\_4446](#)] durchführen. [<=]

**A\_15211 - FM ePA: Dokumentenverwaltung - sichere Verbindung zur VAU - Fehler**

Falls beim Aufbau der sicheren Verbindung zum Verarbeitungskontext der VAU ein Fehler auftritt, MUSS das Fachmodul ePA die Operation mit dem Code 7202 gemäß `Tab_FM_ePA_011` abrechnen. [<=]

Wie der Aufbau der sicheren Verbindung zum Verarbeitungskontext der VAU erfolgt, ist in [gemSpec\_Krypt#3.15] beschrieben.

**A\_14647 - FM ePA: Dokumentenverwaltung - Initialisierung des Aktenkontexts**

Das Fachmodul ePA MUSS vor Nutzung der Schnittstelle I\_Document\_Management der Komponente Dokumentenverwaltung sicherstellen, dass der entsprechende Aktenkontext mittels der Operation `I_Document_Management_Connect::OpenContext` initialisiert wurde. [<=]

**A\_14649 - FM ePA: Dokumentenverwaltung - Verwendung des Kontextschlüssels**

Das Fachmodul ePA MUSS beim Aufruf der Operation `I_Document_Management_Connect::OpenContext` der Komponente Dokumentenverwaltung den entschlüsselten Kontextschlüssel aus der Aktensession der vom Primärsystem aufgerufenen Operation als Parameter übergeben. [<=]

Nach dem erfolgreichen Aufruf der Operation `OpenContext` für ein Aktenkonto, kann das Fachmodul mittels IHE-Transaktionen auf Dokumente im ePA-Aktensystem zugreifen. Im Falle einer Aktivierung des Aktenkontos (Aufruf der Operation `ActivateAccount`) sind Akten- und Kontextschlüssel noch nicht vorhanden und müssen vor der Initialisierung erzeugt werden (vgl. Operation `ActivateAccount` im Webservice `PHRManagementService`).



**A\_14650-01 - FM ePA: Dokumentenverwaltung - Initialisierung des Aktenkontexts - Fehler in der Dokumentenverwaltung**

Falls bei der Kommunikation mit der Komponente Dokumentenverwaltung zur Initialisierung des Aktenkontexts ein Fehler auftritt, MUSS das Fachmodul ePA die Operation mit dem Code 7215 gemäß Tab\_FM\_ePA\_011 abbrechen. [`<=`]

Weitere Fehlerrückgaben der Operation `I_Document_Management_Connect::OpenContext` werden in [`gemSpec_Autorisierung`] spezifiziert.

Dies trifft auch zu, falls kein Schlüsselmaterial vorhanden ist.

## 6.5.6 Schlüsselableitung

Akten- und Kontextschlüssel werden doppelt symmetrisch verschlüsselt in der Komponente Autorisierung des Aktensystems hinterlegt. Die symmetrischen Schlüssel zur Ver- und Entschlüsselung von Akten- und Kontextschlüssel werden über die Schlüsselableitungsfunktion der SGD 1 und 2 ermittelt. Die Funktionsweise der Schlüsselgenerierung, die die Basis für die Ver- und Entschlüsselung von Akten- und Kontextschlüssel ist, wird in [`gemSpec_SGD_ePA`] beschrieben.

Das Element `phrs:AuthorizationKey/phrs:EncryptedKeyContainer` enthält das Chifftrat mit dem doppelt verschlüsselten Akten- und Kontextschlüssel sowie `AssociatedData`.

Die Datenstruktur für `EncryptedKeyContainer` und die Klartextpräsentation für Akten- und Kontextschlüssel ist in [[gemSpec\\_SGD\\_ePA#8 - Interoperables Austauschformat](#)] beschrieben.

### Aufbau der TLS-Verbindung

**A\_18011 - FM ePA: Schlüsselableitung - TLS-Verbindung zu SGD 1 und 2 aufbauen**

Das Fachmodul ePA MUSS zur Kommunikation mit SGD 1 und 2 jeweils eine TLS-Verbindung aufbauen bzw. eine bestehende TLS-Verbindung nutzen. [`<=`]

**A\_18012 - FM ePA: Schlüsselableitung- TLS mit Zertifikats- und Rollenprüfung**

Das Fachmodul ePA MUSS beim Aufbau der TLS-Verbindung zu SGD 1 und 2 eine Zertifikats- und Rollenprüfung für das Zertifikatsprofil C.FD.TLS-S gemäß [`gemSpec_PKI`] mit der Rolle `oid_sgd` gemäß [`gemSpec_OID#GS-A 4446`] durchführen. [`<=`]

**A\_17966 - FM ePA: Schlüsselableitung - Ablauf**

Zur Schlüsselableitung MUSS das Fachmodul ePA den in [`gemSpec_SGD_ePA#2.3`] festgelegten Ablauf durchführen. [`<=`]

In den Schritten 12 und 18 des Basisablaufs erfolgt der Aufruf für `KeyDerivation` abhängig vom Anwendungsfall.

**A\_17870 - FM ePA:Schlüsselableitung - Fehler im Schlüsselgenerierungsdienst**

Falls beim Abruf der AES-Schlüssel von SGD 1 bzw. 2 gemäß [`gemSpec_SGD_ePA`] einer der Fehler "certificate not valid" oder "signature not valid" auftritt, MUSS das Fachmodul ePA die aufgerufene Operation in Abhängigkeit der beim Login verwendeten Karte mit folgendem Code abbrechen:

- 1288 • Login (Authentisierung) mit eGK: Code 106 gemäß Tab\_FM\_ePA\_051
- 1289 • Login (Authentisierung) mit SM-B: Code 7221 gemäß Tab\_FM\_ePA\_011.

1290 [ $\leq$ ]

1291 **A\_17871 - FM ePA: Schlüsselableitung - Fehler an der Schnittstelle zum**  
 1292 **Schlüsselgenerierungsdienst**

1293 Falls beim Abruf der AES-Schlüssel gemäß [gemSpec\_SGD\_ePA] ein anderer Fehler als  
 1294 "certificate not valid" oder "signature not valid" auftritt, MUSS das Fachmodul ePA die  
 1295 aufgerufene Operation mit dem Code 7215 gemäß Tab\_FM\_ePA\_011 abbrechen. [ $\leq$ ]

1296 Als Ergebnis bei einer erfolgreichen Schlüsselableitung zum Verschlüsseln erhält das  
 1297 Fachmodul ePA von jedem der beiden SGD eine Antwortnachricht für KeyDerivation im  
 1298 Format: "OK-KeyDerivation "+Key+" "+a.

1299 *Key* ist der für die Verschlüsselung zu verwendende symmetrische Schlüssel und *a*  
 1300 entspricht AssociatedData für den entsprechenden SGD.  
 1301

1302 **Festlegungen zur Verschlüsselung von Akten- und Kontextschlüssel**

1303 **A\_17992 - FM ePA: Schlüsselableitung - Ermittlung von AssociatedData**

1304 Falls bei der Erteilung einer Berechtigung (Operation ActivateAccount, Operation  
 1305 RequestFacilityAuthorization) der Aufruf der Operation KeyDerivation beim SGD zur  
 1306 Schlüsselableitung erfolgreich war MUSS das Fachmodul ePA den Wert  
 1307 *phrs:AuthorizationKey/phrs:EncryptedKeyContainer/phrs:AssociatedData* gemäß  
 1308 [gemSpec\_SGD\_ePA#8 ] mit dem Inhalt aus 'a' der Antwortnachrichten befüllen.  
 1309 [ $\leq$ ]

1310 Zur Erteilung einer Berechtigung unter Verwendung der Operation ActivateAccount wird  
 1311 der Anwendungsfall [gemSpec\\_SGD\\_ePA#2.4](#) betrachtet.

1312 Zur Erteilung einer Berechtigung unter Verwendung der Operation  
 1313 RequestFacilityAuthorization werden die Anwendungsfälle  
 1314 [gemSpec\\_SGD\\_ePA#2.6](#) und [gemSpec\\_SGD\\_ePA#2.8](#) betrachtet.

1315 Die konkrete Verwendung der Schlüsselableitung zur Verschlüsselung von Akten- und  
 1316 Kontextschlüssel ist in den Kapiteln zur Umsetzung der Operationen ActivateAccount und  
 1317 RequestFacilityAuthorization beschrieben.

1318 **A\_18007 - Schlüsselableitung bei Verschlüsselung - Verschlüsselung mit**  
 1319 **Verschlüsselungsdienst**

1320 Das Fachmodul ePA MUSS beim Erstellen eines AuthorizationKeys den Akten- und  
 1321 Kontextschlüssel mit den von der Schlüsselableitung mit SGD 1 und SGD 2 erhaltenen

1322 symmetrischen Schlüssel unter Berücksichtigung der Strukturen in  
 1323 [[gemSpec\\_SGD\\_ePA#8](#)] unter Berücksichtigung der Reihenfolge wie folgt verschlüsseln:

<p>1. Verschlüsseln mit symmetrischem Schlüssel von SGD 1 durch Aufruf von TUC_KON_075</p>	<p>Eingangsdaten:</p> <ul style="list-style-type: none"> <li>• dataToBeEncrypted = Klartextpräsentation von Akten- und Kontextschlüssel gemäß gemSpec_SGD_ePA#Tab_Austauschformat Akten- und Kontextschlüssel</li> <li>• symmetricKey = aus SGD 1 abgeleiteter symmetrischer Schlüssel</li> <li>• associatedData = Anteil 'a' aus KeyDerivation Response des SGD 1</li> </ul> <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> <li>• encryptedData</li> </ul> <p>Mit encryptedData und aus SGD 1 abgeleiteter symmetrischer Schlüssel wird eine Struktur [gemSpec_SGD_ePA#Tab_erste_Verschlüsselungsschicht] gebildet.</p>
<p>2. Verschlüsseln mit symmetrischem Schlüssel von SGD 2 durch Aufruf von TUC_KON_075</p>	<p>Eingangsdaten:</p> <ul style="list-style-type: none"> <li>• dataToBeEncrypted = im vorangegangenen Schritt gebildete Struktur [gemSpec_SGD_ePA#Tab_erste_Verschlüsselungsschicht]</li> <li>• symmetricKey = aus SGD 2 abgeleiteter symmetrischer Schlüssel</li> <li>• associatedData = Anteil 'a' aus KeyDerivation Response des SGD 2</li> </ul> <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> <li>• encryptedData</li> </ul> <p>Mit encryptedData, associatedData von SGD 1 und associatedData von SGD 2 wird der phrs:EncryptedKeyContainer gemäß [gemSpec_SGD_ePA#Tab_erste_Verschlüsselungsschicht] des AuthorizationKey gebildet.</p>

1324 [**<=**]

## 1325 Festlegungen zur Entschlüsselung von Akten- und Kontextschlüssel

1326 I\_Authorization::getAuthorizationKey liefert abhängig von der Telematik-ID bzw. KVN  
 1327 der übertragenen AuthenticationAssertion das Chifftrat für einen berechtigten Nutzer mit  
 1328 Akten- und Kontextschlüssel, die Information durch wen die Berechtigung erfolgte  
 1329 und eine dazu passende AuthorizationAssertion. Das Fachmodul ePA kann im nächsten  
 1330 Schritt das Chifftrat entschlüsseln und Akten- und Kontextschlüssel liegen im Klartext vor  
 1331 und können verwendet werden.

## 1332 **A\_17869 - FM ePA: Schlüsselableitung bei Entschlüsselung - Entschlüsselung mit Verschlüsselungsdienst**

1333 Falls AuthorizationKey für den authentisierten Nutzer von der Komponente Autorisierung  
 1334 abgerufen werden konnte, MUSS das Fachmodul ePA die AES-Schlüssel von den beiden  
 1335 SGD abrufen und damit Akten- und Kontextschlüssel unter Berücksichtigung der  
 1336

1337 Strukturen in [[gemSpec\\_SGD\\_ePA#8](#)] wie folgt unter Berücksichtigung der Reihenfolge  
1338 entschlüsseln:

<p>1. Entschlüsseln mit symmetrischem Schlüssel von SGD 2 durch Aufruf von TUC_KON_076</p>	<p>Eingangsdaten:</p> <ul style="list-style-type: none"> <li>• encryptedData = phrs:AuthorizationKey/phrs:EncryptedKeyContainer/phrs:Ciphertext</li> <li>• symmetricKey = aus SGD 2 abgeleiteter symmetrischer Schlüssel</li> <li>• associatedData = phrs:AuthorizationKey/phrs:EncryptedKeyContainer/phrs:AssociatedData [1]</li> </ul> <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> <li>• plainData als einfach symmetrisch verschlüsselter Akten- und Kontextschlüssel (siehe gemSpec_SGD_ePA#Tab_erste_Verschlüsselungsschicht)</li> </ul>
<p>2. Entschlüsseln mit symmetrischem Schlüssel von SGD 1 durch Aufruf von TUC_KON_076</p>	<p>Eingangsdaten:</p> <ul style="list-style-type: none"> <li>• encryptedData = phrs:EncryptedKeyContainer\phrs:Ciphertext aus plainData (Schritt 1)</li> <li>• symmetricKey = aus SGD 1 abgeleiteter symmetrischer Schlüssel</li> <li>• associatedData = phrs:EncryptedKeyContainer/phrs:AssociatedData aus plainData (Schritt 1)</li> </ul> <p>Ausgangsdaten:</p> <ul style="list-style-type: none"> <li>• plainData als Klartextpräsentation von Akten- und Kontextschlüssel (siehe gemSpec_SGD_ePA#Tab_Austauschformat Akten- und Kontextschlüssel)</li> </ul>

1339  
1340 [**<=**]

1341 **A\_17986 - FM ePA: Schlüsselableitung bei Entschlüsselung- Abhängigkeit von**  
1342 **der Rolle**

1343 Bei der Entschlüsselung von Akten- und Kontextschlüssel MUSS das Fachmodul ePA bei  
1344 Durchführung der Schlüsselableitung die Operation KeyDerivation gemäß  
1345 Anwendungsfall gemSpec\_SGD\_ePA#2.5,2.7,2.9 aufrufen.

1346 [**<=**]

1347 **A\_17993 - FM ePA: Schlüsselableitung bei Entschlüsselung - Verwendung von**  
1348 **AssociatedData**

1349 Bei der Entschlüsselung von Akten- und Kontextschlüssel MUSS das Fachmodul ePA das  
1350 Element `phrs:AuthorizationKey/phrs:EncryptedKeyContainer/phrs:AssociatedData`  
1351 des ermittelten AuthorizationKey für den Aufruf der Operation KeyDerivation beim SGD  
1352 wie folgt verwenden:  
1353 KeyDerivation <Teilstring aus AssociatedData als Ableitungsinformationen für den  
1354 entsprechenden SGD>

1355 [**<=**]

1356 Die Ermittlung der Ableitungsinformation für SGD1 und SGD2 ist in  
1357 [gemSpec\_SGD\_ePA#8 ] beschrieben.

1358 Zur Optimierung der Performance muss das Fachmodul die Schlüsselableitung für SGD 1  
1359 (Basisablauf Schritt 1) und SGD 2 (Basisablauf Schritt 3) und das Erzeugen eines  
1360 ephemeren ECDH-Schlüsselpaares (Basisablauf Schritt 5) parallel ausführen. Der Request  
1361 an SGD 1 und der Request an SGD 2 in Basisablauf Schritt 7 können ebenfalls  
1362 parallelisiert werden (siehe [gemSpec\_SGD\_ePA#A\_17925 ] ). Die bei einer  
1363 Schlüsselableitung für eine Entschlüsselung im Request für KeyDerivation zu  
1364 übermittelnden Informationen werden sowohl für SGD 1 als auch SGD 2 dem Element  
1365 phrs:AuthorizationKey/phrs:EncryptedKeyContainer/phrs:AssociatedData  
1366 entnommen.

1367 **A\_17736 - FM ePA: Schlüsselableitung bei Entschlüsselung - Fehler bei der**  
1368 **Entschlüsselung**

1369 Falls der Basiskonnektor bei der Entschlüsselung von Akten- und Kontextschlüssel einen  
1370 Fehler zurückgibt, MUSS das Fachmodul ePA die aufgerufene Operation mit dem Code  
1371 7400 gemäß Tab\_FM\_ePA\_011 abbrechen.  
1372 [**<=**]

1373 **6.6 Logout**

1374 Das Fachmodul ePA stellt einen impliziten Logout für die Aktensession bereit, welcher  
1375 nach einem Timeout bei Inaktivität bzgl. der Nutzung einer Aktensession ausgeführt wird.  
1376 Es veranlasst die Löschung der zur Aktensession gehörenden Verbindungsdaten in der  
1377 VAU und löscht anschließend die Aktensession. Falls noch weitere Verbindungen anderer  
1378 Aktensessions in die VAU bestehen, bleiben diese aktiv (vgl.  
1379 I\_Document\_Management\_Connect::CloseContext gemäß  
1380 [gemSpec\_Dokumentenverwaltung]).

1381 **A\_14651 - FM ePA: Logout Aktensession - Löschung der Aktensession**

1382 Falls auf eine Aktensession länger als 20 Minuten nicht zugegriffen wird, MUSS das  
1383 Fachmodul ePA die Aktensession beenden und alle dazugehörigen Daten löschen.[**<=**]

1384 Das Fachmodul hat die Option, eine vom Zugangsgateway abgerufene  
1385 AuthenticationAssertion zu erneuern und muss daher, falls ein Logout erfolgt, als  
1386 zusätzliche Sicherheitsmaßnahme die Möglichkeit zur Erneuerung der aktuellen  
1387 AuthenticationAssertion mittels der Operation AuthInsurantService::LogoutToken  
1388 verhindern.

1389 **A\_17450-01 - FM ePA: Logout Aktensession - Unterbindung der Erneuerung der**  
1390 **AuthenticationAssertion**

1391 Falls eine Aktensession der eGK beendet wird, MUSS das Fachmodul ePA die Operation  
1392 AuthInsurantService::LogoutToken der Komponenten Zugangsgateway aufrufen.[**<=**]

1393 Da die Löschung der Aktensession nicht innerhalb einer vom Clientsystem aufgerufenen  
1394 Operation ausgeführt wird, kann ein aufgetretener Fehler auch nicht an das Clientsystem  
1395 zurückgegeben werden. Der Fehler muss dennoch protokolliert werden.

1396 **A\_17451 - FM ePA: Logout Aktensession - Unterbindung der Erneuerung der**  
1397 **AuthenticationAssertion - Fehler**

1398 Falls die Operation AuthInsurantService::LogoutToken gemäß  
1399 [gemSpec\_Authentisierung\_Vers] einen Fehler zurückgibt, MUSS das Fachmodul ePA  
1400 diesen Fehler im Sicherheitsprotokoll eintragen.

1401  
1402 [**<=**]

1403 **A\_17142 - FM ePA: Logout Aktensession - Löschung der Verbindung zur VAU -**  
 1404 **Fehler**  
 1405 Falls die Operation I\_Document\_Management\_Connect::CloseContext einen Fehler  
 1406 zurückgibt, MUSS das Fachmodul ePA diesen Fehler im Sicherheitsprotokoll eintragen.  
 1407 [ $\leq$ ]

## 1408 6.7 Datenschutz und Sicherheitsaspekte

1409 **A\_14173 - FM ePA: Sicherheit - Keine persistente Speicherung von**  
 1410 **personenbezogenen Daten**  
 1411 Das Fachmodul ePA DARF personenbezogene Daten NICHT persistent speichern. [ $\leq$ ]

1412 **A\_14722 - FM ePA: Sicherheit - Keine persistente Speicherung von Dokumenten**  
 1413 **und Metadaten**  
 1414 Das Fachmodul ePA DARF Dokumente und Metadaten der Patientenakte NICHT persistent  
 1415 speichern. [ $\leq$ ]

1416 **A\_14174 - FM ePA: Sicherheit - Keine Speicherung von privaten Schlüsseln**  
 1417 Das Fachmodul ePA DARF symmetrische und private asymmetrische Schlüssel (z.B.  
 1418 Dokumentenschlüssel, Aktenschlüssel) NICHT persistent speichern. [ $\leq$ ]

1419 **A\_14175 - FM ePA: Sicherheit - Keine Weitergabe vertraulicher**  
 1420 **Informationsobjekte an das PS**  
 1421 Das Fachmodul ePA DARF Schlüsselmaterial und Daten der Aktensession NICHT an das  
 1422 PS weitergeben. [ $\leq$ ]

1423

1424 **Regelungen aus [gemSpec\_Krypt]**  
 1425 Für die Erzeugung von Schlüsselmaterial gilt übergreifend [gemSpec\_Krypt#GS-  
 1426 A\_4368].

1427 **Regelungen für TLS-Verbindungen**  
 1428 Für TLS-Verbindungen gelten die Regelungen aus [gemSpec\_Krypt#3.3.2].

## 1429 6.8 Verwendung des Dienstverzeichnisdienstes

1430 **A\_13828 - FM ePA: Service-Informationen für Dienstverzeichnisdienste**  
 1431 Während der Bootup-Phase des Konnektors MUSS das Fachmodul ePA die in  
 1432 Tab\_FM\_ePA\_007 gemäß dem XML-Schema [ServiceInformation.xsd] definierten  
 1433 Services in den Dienstverzeichnisdienst des Konnektors [gemSpec\_Kon#4.1.3]  
 1434 einbringen.  
 1435

1436 **Tabelle 9: Tab\_FM\_ePA\_007 Service-Informationen der Services des Fachmoduls ePA**

Element/Attribut	PHRService	PHRManagementService
ServiceInformation/Service/@Name	PHRService	PHRManagementService



ServiceInformation/Service/Abstract	IHE-Schnittstelle zur Dokumentenverwaltung	Schnittstelle zur Administration und Rechtevergabe der Akte
ServiceInformation/Service/Version/Version/@TargetNamespace	aktueller Namensraumbezeichner gemäß Tab_FM_ePA_005 bzw. <a href="#">Tab FM ePA 005 2.x</a>	aktueller Namensraumbezeichner gemäß Tab_FM_ePA_003
ServiceInformation/Service/Version/Version/@Version	aktuelle Versionsnummer gemäß Tab_FM_ePA_005 bzw. <a href="#">Tab FM ePA 005 2.x</a>	aktuelle Versionsnummer gemäß Tab_FM_ePA_003
ServiceInformation/Service/Version/Version/Abstract	Initiale Version	Initiale Version
ServiceInformation/Service/Version/Version/Endpoint/@Location	Absoluter URL des über Hypertext Transfer Protocol (HTTP) erreichbaren Dienstes	Absoluter URL des über Hypertext Transfer Protocol (HTTP) erreichbaren Dienstes
ServiceInformation/Service/Version/Version/EndpointTLS/@Location	Absoluter URL des über HTTP Secure (HTTPS) erreichbaren Dienstes	Absoluter URL des über HTTP Secure (HTTPS) erreichbaren Dienstes
ServiceInformation/Service/Version/Version/WSDL/@Location	<leer>	<leer>

[&lt;=]

## 6.9 Protokollierung und Logging

Während die Protokollierung der Zugriffe nach §291a im ePA-Aktensystem erfolgt, legt das Fachmodul ePA Log-Informationen im Konnektor ab, die eine Analyse technischer Vorgänge erlauben. Diese Dateien sind dafür vorgesehen, aufgetretene Fehler zu identifizieren, die Performance zu analysieren und interne Abläufe zu beobachten. Um die Anforderungen an den Datenschutz zu gewährleisten, dürfen weder medizinische noch personenbezogene Daten geloggt werden.

**A\_14154 - FM ePA: Verbot des Logging von Schlüsselmaterial**

Das Fachmodul ePA DARF symmetrisches und privates Schlüsselmaterial NICHT loggen. [ <= ]

**A\_14155 - FM ePA: Verbot des Logging von medizinischen und personenbezogenen Daten**

Das Fachmodul ePA DARF medizinische und personenbezogene Daten NICHT loggen. [ <= ]

Die Log-Dateien folgen einem einheitlichen Format, das vom Hersteller festgelegt und dokumentiert wird. Es muss geeignet sein, um automatische Auswertungen mit wenig Aufwand durch Dritte zu ermöglichen. Ein Vorbild ist das Weblog des Apache Webserver. Um mehrere Protokolleinträge korrelieren zu können, soll beim Aufruf einer Operation an den Schnittstellen eine Vorgangsnummer gebildet werden. Diese Vorgangsnummer wird in allen Protokolleinträgen dieses Operationsaufrufs genutzt. Die Vorgangsnummer wird vom Konnektor pseudozufällig gebildet.

**A\_14156 - FM ePA: Einheitliches Log-Format**

Das Fachmodul ePA MUSS Log-Dateien in einem einheitlichen, dokumentierten Format erstellen, das eine automatisierte Auswertung ermöglicht. [ <= ]

**A\_14157 - FM ePA: Korrelation von Log-Einträgen**

Das Fachmodul ePA MUSS sicherstellen, dass sich alle zu einem Operationsaufruf zugehörigen Log-Einträge über eine Vorgangsnummer korrelieren lassen. [ <= ]

Der Zugriff auf Log-Dateien muss auf autorisierte Personen durch angemessene technische oder organisatorische Maßnahmen eingeschränkt werden. Zur besseren Auswertung können die Log-Dateien auf ein separates Speichermedium kopiert werden (siehe [gemSpec\_Kon#TIP1-A\_4716]).

**A\_14711 - FM ePA: Fachmodulprotokoll**

Das Fachmodul ePA MUSS ein Fachmodulprotokoll gemäß dem Protokollierungsdienst des Konnektors führen. [ <= ]

**A\_14712 - FM ePA: Fachmodul-Performance-Protokoll**

Das Fachmodul ePA MUSS ein Fachmodul-Performance-Protokoll gemäß dem Protokollierungsdienst des Konnektors führen. [ <= ]

**A\_17228 - FM ePA: Fachmodulprotokoll (Fehler)**

Das Fachmodul ePA MUSS unabhängig vom ErrorType alle lokal erkannten und Remote-Fehler der Severity „Warning“, „Error“ oder „Fatal“ im Fachmodulprotokoll mit mindestens den folgenden Parametern erfassen:

**Tabelle 10: Tab\_FM\_ePA\_014 Parameter des Fehlerprotokolls**

Feld	Beschreibung
eventType	„Op“
Schwere	„Warning“, „Error“, „Fatal“
Vorgangsnummer	Zeichenkette zur Korrelation der zugehörigen Protokolleinträge
Zeitpunkt	Zeitpunkt der Erstellung des Protokolleintrags



Fehlercode	Fehlercode des aufgetretenen Fehlers
CardHandle	CardHandle der betroffenen eGK
Fehlerdetails	Weiterführende Details zum Fehler

1484 [ $\leq$ ]

1485 **A\_17229-01 - FM ePA: Fachmodulprotokoll (Debug)**

1486 Falls nicht im Produktivbetrieb laufend, KANN das Fachmodul ePA für Testzwecke im  
1487 Fachmodulprotokoll Debug-Einträge mit mindestens den folgenden Parametern erfassen:  
1488

1489 **Tabelle 11: Tab\_FM\_ePA\_015 Parameter des Debug-Protokolls**

Feld	Beschreibung
eventType	„Op“
Schwere	„Debug“

1490 [ $\leq$ ]

1491

1492 **A\_17230 - FM ePA: Sicherheitsprotokoll**

1493 Das Fachmodul ePA MUSS sicherheitsrelevante Fehler und Ereignisse über den  
1494 Protokollierungsdienst des Konnektors im Sicherheitsprotokoll des Konnektors  
1495 mindestens mit den folgenden Parametern erfassen:

1496

1497 **Tabelle 12: Tab\_FM\_ePA\_022 Parameter des Sicherheitsprotokolls**

Feld	Beschreibung
eventType	„Sec“
Schwere	„Info“, „Warning“, „Error“, „Fatal“
Vorgangsnummer	Zeichenkette zur Korrelation der zugehörigen Protokolleinträge
Name der Operation	Name der untersuchten Operation
Bezeichnung	Bezeichnung des sicherheitsrelevanten Fehlers oder Ereignisses
Beschreibung	Details des sicherheitsrelevanten Fehlers oder Ereignisses

1498 [ $\leq$ ]

1499

**A\_17231 - FM ePA: Performanceprotokoll**

Das Fachmodul ePA MUSS alle zur Kontrolle der Performancevorgaben benötigten, mindestens aber die nachfolgenden, Parameter der Operationsaufrufe im Performanceprotokoll erfassen:

**Tabelle 13: Tab\_FM\_ePA\_024 Parameter des Performanceprotokolls**

Feld	Beschreibung
eventType	„Perf“
Vorgangsnummer	Zeichenkette zur Korrelation der zugehörigen Protokolleinträge
Name der Operation	Name der untersuchten Operation
Startzeitpunkt	Startzeitpunkt der Operation
Dauer	Dauer der Operation in ms
Beschreibung	Ergänzende Informationen zur gemessenen Aktion

[&lt;=]

Hinweis: Der Parameter „Schwere“ wird für einen Eintrag im Performanceprotokoll nicht verwendet.

**6.10 Konfiguration****A\_17227 - FM ePA: Übergreifende Konfigurationsparameter**

Das Fachmodul ePA MUSS die in Tabelle Tab\_FM\_ePA\_010 genannten Parameter dem Administrator über die Managementschnittstelle des Konnektors zur Konfiguration anbieten.

**Tabelle 14: Tab\_FM\_ePA\_010 Übergreifende Konfigurationsparameter des Fachmodules ePA**

ReferenzID	Belegung	Bedeutung
FM_EPA_LOG_LEVEL	Debug, Info, Warning, Error, Fatal	Kleinster Level der zu schreibenden Einträge im Fachmodulprotokoll (d.h., kleinere Level werden nicht geschrieben) Default-Wert: Warning
FM_EPA_LOG_DAYS	X Tage	Anzahl an Tagen, wie lange Protokolleinträge gespeichert werden müssen; Protokolleinträge dürfen nicht länger gespeichert werden. Dabei darf der eingestellte Wert nicht unter der Mindestgröße von 10 Tagen oder über der Maximalgröße von einem Jahr (365 Tage) liegen. Default-Wert: 180

FM_EPA_LOG_PERF	Boolean	Gibt an, ob das Performance-Protokoll für das Fachmodul ePA geführt werden soll. Default-Wert: false
-----------------	---------	---

1517 [**<=**]

1518 Die Einsicht von Protokolldateien und Administration der Konfigurationsparameter  
1519 erfolgen über die Managementschnittstelle des Konnektors (vgl. [gemSpec\_Kon#4.3.4]).

## 1520 6.11 Fehlerbehandlung und Fehlermeldungen

### 1521 Fehlerkonzept

1522 Einige Operationen des Fachmoduls müssen möglicherweise mehrere oder sogar alle  
1523 ePA-Aktensysteme anfragen, um ihre Funktionalität durchführen zu können.  
1524 GetHomeCommunityID iteriert beispielsweise über alle bekannten ePA-Aktensysteme, bis  
1525 ein ePA-Aktensystem gefunden wird, dass die Akte zur angefragten KVNR führt. Dabei  
1526 könnten die ePA-Aktensysteme verschiedene Fehler zurückgeben oder aufgrund eines  
1527 technischen Problems nicht erreichbar sein. Die einzelnen Operationen reagieren fachlich  
1528 nicht einheitlich auf diese Situation. Während ein nicht erreichbares ePA-Aktensystem für  
1529 GetHomeCommunity nicht zwingend ein Problem darstellt, falls etwa ein anderes ePA-  
1530 Aktensystem die Akte führt, gibt GetAuthorizationList in diesem Falle eine Warnung aus,  
1531 da möglicherweise nicht alle Berechtigungen der LEI abgerufen werden konnten.

1532 Die Methodik in diesem Dokument sieht in diesem Kapitel eine übergreifende Behandlung  
1533 der Fehler vor, falls alle Anfragen an das ePA-Aktensystem oder seine Komponenten, die  
1534 zwingend zur Durchführung einer Operation oder Funktionalität benötigt werden,  
1535 fehlschlagen. Diese Anforderungen greifen also auch, falls nur die Kommunikation mit  
1536 einem einzigen ePA-Aktensystem notwendig ist. Alle weiteren Situationen werden jeweils  
1537 in den Unterkapiteln der Operationen behandelt. Falls unterschiedliche Probleme  
1538 innerhalb einer Operation auftreten, liefert diese Operation dann ggfs. einen allgemeinen  
1539 Fehler an das aufrufende System zurück, da eine Differenzierung der Fehlersituationen  
1540 schnell unübersichtlich und für den Nutzer nicht hilfreich ist. Jeder Fehlercode wird dann  
1541 aber im Fachmodulprotokoll abgelegt und erlaubt so eine genaue Analyse.

### 1542 Übergreifende Festlegungen zu Fehlermeldungen

1543 Treten bei der Ausführung einer Operation Fehler auf, die zum Abbruch der Operation  
1544 führen, so werden diese an das aufrufende System über eine SOAP-Fault-Nachricht  
1545 gemeldet. Im Erfolgsfalle oder bei Fehlern, die nicht zum Abbruch der Operation führen,  
1546 wird ein Status-Element gemäß [gemSpec\_Kon#3.5.2] zurückgegeben.

1547 Für das Fehlermanagement gelten neben den hier aufgeführten spezifischen  
1548 Anforderungen die Anforderungen aus Kapitel 3 der übergreifenden Spezifikation  
1549 [gemSpec\_OM#3].

### 1550 **A\_14405 - FM ePA: Übergreifende Anforderung - Fehlermeldungen des** 1551 **Webservice PHRManagementService (SOAP-Fault)**

1552 Das Fachmodul ePA MUSS Fehler, die bei Operationen des Webservice  
1553 PHRManagementService auftreten, mittels gematik-SOAP-Fault an das aufrufende  
1554 System melden.**[<=]**

1555 Details zu gematik-SOAP-Faults finden sich in [gemSpec\_OM#3.2.3]. Der Code 7400  
1556 wird für Fehlerfälle verwendet, die technisch bedingt sind und durch den Nutzer nicht  
1557 behoben werden können. Diese Fehlerfälle erfordern eine Analyse und Behebung durch  
1558 den Anbieter.

**A\_14406 - FM ePA: Übergreifende Anforderung - Allgemeine Fehlerbehandlung**

Falls nicht durch andere Anforderungen geregelt, MUSS das Fachmodul ePA einen Operationsaufruf im Fehlerfall mit dem Code 7400 gemäß Tab\_FM\_ePA\_011 abbrechen.[<=]

**A\_15675 - FM ePA: Übergreifende Anforderung - Syntaxprüfung bei Aufrufen von Webservices - Fehler**

Falls bei Aufruf einer Operation der Webservices PHRManagementService oder PHRService die Syntaxprüfung fehlschlägt, MUSS das Fachmodul ePA den Operationsaufruf mit dem Code 4000 gemäß Tab\_FM\_ePA\_050 abbrechen.[<=]

Hinweis: Die Syntaxprüfung der Operationsaufrufe von PHRService und PHRManagementService ist durch die normative Beschreibung mittels WSDL-Dateien bedingt (Kapitel 7.1 PHRService und 7.2 PHRManagementService).

**A\_17724 - FM ePA: Übergreifende Anforderung - Verbot der Rückgabe von Implementierungsdetails**

Das Fachmodul ePA DARF in Fehlermeldungen KEINE Informationen über die Implementierung schreiben, z.B. Teile des Programm-Stack-Traces.[<=]

**Übergreifende Fehlercodes**

Die nachfolgenden Tabellen enthalten

- Fehlermeldungen der übergreifenden Festlegungen des Fachmoduls ePA,
- Fehlermeldungen zu Situationen, die in mehreren Operationen auftreten (und in den entsprechenden Unterkapiteln behandelt werden),
- Fehlermeldungen, die aus anderen Spezifikationen nachgenutzt werden.

**Tabelle 15: Tab\_FM\_ePA\_011 Übergreifende Fehlermeldungen des Fachmoduls ePA**

Code	ErrorType	Severity	Fehlertext
7200	Technical	ERROR	Lokalisierung des Aktensystems fehlgeschlagen
7202	Security	ERROR	Verbindung zum Aktensystem fehlgeschlagen
7203	Security	ERROR	Die gegenseitige Authentisierung von eGK und SMC-B (Card-to-Card-Authentisierung) ist gescheitert.
7205	Technical	ERROR	Es konnte kein freigeschaltetes SM-B mit einem zulässigen Institutionstyp gefunden werden.
7206	Technical	ERROR	Prüfung der Zugriffsberechtigung fehlgeschlagen
7207	Technical	ERROR	PIN-Verifikation gescheitert
7209	Technical	ERROR	Keine Berechtigung für das Aktenkonto vorhanden
7211	Technical	ERROR	Dokument überschreitet maximal zulässige Größe von 25 MB

7212	Technical	ERROR	Summe der Dokumente überschreitet maximal zulässige Größe von 250 MB
7213	Technical	ERROR	Sperrstatus des Zertifikats der eGK nicht ermittelbar
7214	Security	ERROR	Das Schlüsselmateriale der Akte entspricht nicht den Sicherheitsanforderungen.
7215	Technical	ERROR	Fehler im Aktensystem - Die Operation konnte nicht durchgeführt werden.
7217	Technical	ERROR	Die Operation wurde am Kartenterminal abgebrochen.
7220	Infrastructure	ERROR	Aktensystem nicht erreichbar
7221	Security	ERROR	Zertifikat auf SMC-B ungültig
7400	Technical	ERROR	Fehler - Die Operation konnte nicht durchgeführt werden.
7402	Technical	WARNING	Das Aktenkonto ist bereits eingerichtet.
7403	Technical	ERROR	Das Aktenkonto kann noch nicht verwendet werden.
7404	Technical	ERROR	Das Aktenkonto existiert nicht (mehr) in diesem ePA-Aktensystem.
7405	Technical	WARNING	Das Aktenkonto wurde bei diesem ePA-Aktensystem gekündigt, kann aber aktuell noch benutzt werden.
7406	Technical	WARNING	Das Aktenkonto wurde bei diesem ePA-Aktensystem gekündigt und ist nur noch für einen Kontowechsel lesend zugreifbar.

**Tabelle 16: Tab\_FM\_ePA\_050 Wiederverwendete Fehlermeldungen aus der Konnektorspezifikation**

Code	Referenz	Bedeutung (informativ)
4008	[gemSpec_Kon#TAB_KON_515]	Karte nicht gesteckt
4063	[gemSpec_Kon#TAB_KON_089]	PIN gesperrt
4065	[gemSpec_Kon#TAB_KON_089]	PIN transportgeschützt
4093	[gemSpec_Kon#TAB_KON_824]	Karte bereits exklusiv verwendet

4000	[gemSpec_Kon#TAB_KON_567]	Syntaxfehler beim Aufruf einer Operation
------	---------------------------	--

1587

1588

1589

**Tabelle 17: Tab\_FM\_ePA\_051 Wiederverwendete Fehlermeldungen aus der Übergreifenden Spezifikation Operations und Maintenance**

Code	Referenz	Bedeutung (informativ)
106	[gemSpec_OM#Tab_Gen_Fehler]	Zertifikat auf eGK ungültig
114	[gemSpec_OM#Tab_Gen_Fehler]	DF.HCA gesperrt
115	[gemSpec_OM#Tab_Gen_Fehler]	Leseversuch von veralteter eGK

## 7 Funktionsmerkmale

ePA 2.0 führt ein neues Berechtigungskonzept ein. Es wird in feingranulare, mittelgranulare und grobgranulare Berechtigung unterschieden. In der LEI wird bei der ad-Hoc Berechtigung die mittelgranulare und grobgranulare Berechtigung unterstützt. Um die Interoperabilität mit bisherigen Primärsystemen sicherzustellen wird in der Migrationsphase sowohl die in früheren Versionen bereits unterstützte ad-Hoc Berechtigung auf Basis der 3 Kategorien Versicherter, Arzt und Kasse als auch die neue Art der Berechtigung (mittelgranular und grobgranular) unterstützt. Das Kennzeichnen von Dokumenten, die ein Versicherter eingestellt hat in LE-äquivalente Dokumente wird nicht mehr unterstützt. Die Webservices PHRService und PHRManagementService werden mit jeweils 2 Versionen unterstützt. "Version 2.x" kennzeichnet die WebServices, die das neue Berechtigungskonzept von ePA 2.0 unterstützen.

Das Fachmodul ePA wird in zwei Funktionsmerkmale unterteilt, die je über eine Schnittstelle realisiert werden:

**Tabelle 18: Tab\_FM\_ePA\_004 Schnittstellenübersicht des Fachmoduls ePA**

Schnittstelle	Beschreibung und Operationen	
PHRService <a href="#">Version 1.x</a>	IHE-Schnittstelle zur Dokumentenverwaltung	
	<b>Logische Operation</b>	<b>Beschreibung</b>
	putDocuments	Dokumente einstellen
	find	Dokumente suchen
	getDocuments	Dokumente herunterladen
	removeDocuments	Dokumente löschen
	updateDocumentSet	Metadaten von Dokumenten ändern
<a href="#">PHRService Version 2.x</a>	<a href="#">IHE-Schnittstelle zur Dokumentenverwaltung Version 2.x</a>	
	<b><a href="#">Logische Operation</a></b>	<b><a href="#">Beschreibung</a></b>
	<a href="#">putDocuments</a>	<a href="#">Dokumente einstellen</a>
	<a href="#">find</a>	<a href="#">Dokumente suchen</a>
	<a href="#">getDocuments</a>	<a href="#">Dokumente herunterladen</a>

	<a href="#">removeDocuments</a>	<a href="#">Dokumente löschen</a>
PHRManagementService <a href="#">Version 1.x</a>	Schnittstelle zur Aktivierung und Rechtevergabe	
	<b>Logische Operation</b>	<b>Beschreibung</b>
	ActivateAccount	Aktivierung eines Aktenkontos
	RequestFacilityAuthorization	Berechtigungsvergabe für eine LEI
	<a href="#">GetHomeCommunityID</a>	<a href="#">Identifizierung eines ePA-Aktensystems</a>
	<a href="#">GetAuthorizationList</a>	<a href="#">Abruf aller Berechtigungen einer LEI</a>
<a href="#">PHRManagementService Version 2.x</a>	<a href="#">Schnittstelle zur Aktivierung und Rechtevergabe</a>	
	<b><a href="#">Logische Operation</a></b>	<b><a href="#">Beschreibung</a></b>
	<a href="#">ActivateAccount</a>	<a href="#">Aktivierung eines Aktenkontos</a>
	<a href="#">RequestFacilityAuthorization</a>	<a href="#">Berechtigungsvergabe für eine LEI Version 2.x</a>
	GetHomeCommunityID	Identifizierung eines ePA-Aktensystems
	GetAuthorizationList	Abruf aller Berechtigungen einer LEI

1606

1607 Die Operationen von PHRService erlauben das Einstellen, Suchen, Herunterladen und  
 1608 Löschen von Dokumenten sowie die Aktualisierung von Metadaten. Die zum Aufruf  
 1609 benötigte HomeCommunity als Teil des RecordIdentifiers können Primärsysteme über die  
 1610 Operation GetHomeCommunityID des Webservices PHRManagementService beziehen.  
 1611 Dieser Webservice erlaubt es außerdem einem Versicherten, in der LE-Umgebung sein  
 1612 Aktenkonto zu aktivieren und eine Leistungserbringerinstitution ad-hoc zu berechtigen  
 1613 (Operation RequestFacilityAuthorization). Eine LEI kann ihre Berechtigungen für  
 1614 Aktenkonten abrufen und aktualisieren.

1615 Die Webservices werden vom Fachmodul ePA im Dienstverzeichnis des Konnektors  
 1616 registriert und damit für Primärsysteme auffindbar gemacht (siehe Kapitel 6.8  
 1617 Verwendung des Dienstverzeichnisdienstes).



## 7.1 PHRService

In ePA 2.0 werden 2 Versionen des Webservice PHRService unterstützt.

Der Webservice PHRService V1.x unterstützt wie bisher die Operationen putDocuments, find, getDocuments, removeDocuments. Da die Funktion des Adels nicht mehr unterstützt wird, wird die Operation updateDocumentSet mit einem Fehler abgebrochen.

Der Webservice PHRService V2.x ist neu und unterstützt wie bisher die Operationen putDocuments, find, getDocuments, removeDocuments. Die Operation updateDocumentSet wird nicht unterstützt.

Wenn sich die Anforderungen für die beiden Versionen des Webservice PHRService unterscheiden, so stellt die neue Anforderung über den Suffix den Bezug zu V2.x her. Die parallel hierzu bereits existierende Anforderung gilt für Webservice PHRService 1.x. Alle anderen Anforderungen gelten für beide Versionen.

Der Webservice PHRService setzt die logische Schnittstelle I\_PHR\_Management gemäß [gemSysL\_ePA] um.

### **A 14373-03A\_14373-01 - FM ePA: PHRService**

Das Fachmodul ePA MUSS für Primärsysteme den Webservice PHRService gemäß Tabelle Tab\_FM\_ePA\_005 anbieten.

**Tabelle 19: Tab\_FM\_ePA\_005 Beschreibung des Webservices PHRService**

<b>Name</b>	PHRService	
<b>Version</b>	1.24.0	
<b><u>SOAP-Header</u></b>	<b><u>Name</u></b>	<b><u>Inhalt</u></b>
	<u>MandantID</u>	<u>MandantID gemäß [ConnectorContext.xsd]</u>
	<u>ClientSystemID</u>	<u>ClientSystemID gemäß [ConnectorContext.xsd]</u>
	<u>WorkplaceID</u>	<u>WorkplaceID gemäß [ConnectorContext.xsd]</u>
	<u>RecordIdentifier</u>	<u>RecordIdentifier gemäß [gemSpec_DM_ePA#2.2]</u>
<b><u>Namensraum</u></b>	<u>urn:ihe:iti:xds-b:2007</u>	
<b><u>Abkürzung Namensraum</u></b>	<u>ihe</u>	
<b><u>Operationen</u></b>	<b><u>Name (logisch)</u></b>	<b><u>IHE-Umsetzung der Schnittstelle</u></b>
	<u>putDocuments</u>	<u>[ITI-41] "ProvideAndRegisterDocumentSet-b" als Akteur "Document Recipient" gemäß XDR mit der Option "Transmit Home Community Id"</u>

	<a href="#">find</a>	<a href="#">[ITI-18] "Registry Stored Query" als Akteur "Initiating Gateway" gemäß XCA</a>
	<a href="#">getDocuments</a>	<a href="#">[ITI-43] "Retrieve Document Set" als Akteur "Initiating Gateway" gemäß XCA</a>
	<a href="#">removeDocuments</a>	<a href="#">[ITI-86] "Remove Documents" als Akteur "Document Repository" gemäß RMD</a>
	<a href="#">updateDocumentSet</a>	<a href="#">[ITI-92] "Restricted Update Document Set" als Akteur "RMU Update Responder" gemäß RMU mit der Option "Forward" Funktion wird nicht mehr unterstützt. Operation wird mit Code 7400 beendet.</a>
<b>WSDL</b>	<b><a href="#">PHRService.wsdl</a></b>	

[&lt;=]

**A 14373-04 - FM ePA: PHRService Version 2.x**

Das Fachmodul ePA MUSS für Primärsysteme den Webservice PHRService Version 2.x gemäß Tabelle Tab FM ePA 005 2.x anbieten.

**Tabelle 20: Tab FM ePA 005 2.x Beschreibung des Webservices PHRService**

<b>Name</b>	<a href="#">PHRService</a>	
<b>Version</b>	<a href="#">2.0.0</a>	
<b>SOAP-Header</b>	<b>Name</b>	<b>Inhalt</b>
	MandantID	MandantID gemäß [ConnectorContext.xsd]
	ClientSystemID	ClientSystemID gemäß [ConnectorContext.xsd]
	WorkplaceID	WorkplaceID gemäß [ConnectorContext.xsd]
	RecordIdentifier	RecordIdentifier gemäß [gemSpec_DM_ePA#2.2]
<b>Namensraum</b>	urn:ihe:iti:xds-b:2007	
<b>Abkürzung Namensraum</b>	ihe	
<b>Operationen</b>	<b>Name (logisch)</b>	<b>IHE-Umsetzung der Schnittstelle</b>
	putDocuments	[ITI-41] "ProvideAndRegisterDocumentSet-b" als Akteur "Document Recipient" gemäß XDR

		mit der Option "Transmit Home Community Id"
	find	[ITI-18] "Registry Stored Query" als Akteur "Initiating Gateway" gemäß XCA
	getDocuments	[ITI-43] "Retrieve Document Set" als Akteur "Initiating Gateway" gemäß XCA
	removeDocuments	[ITI-86] "Remove Documents" als Akteur "Document Repository" gemäß RMD
	<del>updateDocumentSet</del>	<del>[ITI-92] "Restricted Update Document Set" als Akteur "RMU Update Responder" gemäß RMU mit der Option "Forward"</del>
<b>WSDL</b>	<b>PHRService <u>V 2 0 0</u>.wsdl</b>	

[<=]

Der SOAP-Header ermöglicht es dem Webservice, die Zugriffsberechtigungsprüfung durchzuführen (Kapitel 6.4 Aufrufkontext) und einen SM-B für den Zugriff auf die Akte des Versicherten auszuwählen (Kapitel 6.5 Login).

#### **A\_14376 - FM ePA: PHRService - Fehlermeldungen gemäß IHE**

Falls nicht durch andere Anforderungen geregelt, MUSS der Webservice PHRService die Fehlermeldungen der Profile in Tabelle Tab\_FM\_ePA\_002 zurückgeben.

[<=]

#### **A\_14377-01 - FM ePA: PHRService - Fehlermeldungen gemäß IHE-Mapping**

Der Webservice PHRService MUSS alle Fehler aus Tab\_FM\_ePA\_011 und Tab\_FM\_ePA\_050 als IHE-Fehler nach Tab\_FM\_ePA\_012 abbilden und in der IHE-Response eingebettet an das aufrufende System zurückgeben.

**Tabelle 21: Tab\_FM\_ePA\_012 Mapping von gematik-Fehlern nach IHE-Fehlern**

Fehlerattribut nach gematik-Schema	Fehlerattribut gemäß IHE-Profilen
Code	errorCode
Fehlertext	codeContext
Severity	severity
<i>Keine Entsprechung</i>	location

[<=]

1660

1661 **A\_14874 - FM ePA: PHRService - Mapping für Fehlerkategorie "Fatal"**

1662 Der Webservice PHRService MUSS den gematik-Fehlerwert "Fatal" im Feld "Severity" für  
 1663 IHE auf den Wert "Error" in "severity" abbilden. [≤]

1664 **7.1.1 Definition/Signatur**

1665 Dieses Unterkapitel beschreibt die in [PHRService.wsdl] definierten Methoden, d.h.  
 1666 Aufruf- und Rückgabeparameter sowie alle möglichen Fehlermeldungen.

1667 **7.1.1.1 putDocuments**1668 **Tabelle 22: Tab\_FM\_ePA\_006 Beschreibung und Parameter der Operation putDocuments**

Name	putDocuments	
<b>Beschreibung</b>	Diese Operation ermöglicht Primärsystemen das Einstellen von Dokumenten in das ePA-Aktensystem.	
<b>Aufrufparameter</b>	<b>Name</b>	<b>Beschreibung</b>
	ProvideAndRegisterDocumentSetRequest	Der Parameter enthält die zu speichernden XDS-Dokumente und SubmissionSets inklusive Metadaten gemäß [PHRService.wsdl].
<b>Rückgabeparameter</b>	<b>Name</b>	<b>Beschreibung</b>
	RegistryResponse	Der Parameter enthält den Status der aufgerufenen Operation und Informationen über eventuell aufgetretene Fehler gemäß [PHRService.wsdl].

1669

1670 **Fehlermeldungen**

1671 Die Operation putDocuments kann folgende Fehlermeldungen zurückliefern:

- 1672 • 7200, 7202, 7205, 7206, 7209, 7211, 7212, 7214, 7215, 7220, 7221, 7400,  
 1673 7403, 7404, 7406 gemäß Tab\_FM\_ePA\_011
- 1674 • 4000 gemäß Tab\_FM\_ePA\_050
- 1675 • reguläre bei IHE für [ITI-41] definierte Fehlermeldungen

### 7.1.1.2 find

Die Operation *find* ermöglicht einem Primärsystem das Suchen von Inhalten (Dokumenten und SubmissionSets) im ePA-Aktensystem.

**Tabelle 23: Tab\_FM\_ePA\_013 Beschreibung und Parameter der Operation find (Semantik)**

Name	find	
<b>Beschreibung</b>	Diese Operation ermöglicht Primärsystemen das Suchen von Dokumenten und SubmissionSets im ePA-Aktensystem.	
<b>Aufrufparameter</b>	<b>Name</b>	<b>Beschreibung</b>
	AdhocQueryRequest	Der Parameter enthält die gewünschte Suchanfrage ("Stored Query") inklusive Parametern gemäß [PHRService.wsdl].
<b>Rückgabeparameter</b>	<b>Name</b>	<b>Beschreibung</b>
	AdhocQueryResponse	Der Parameter enthält die Suchergebnisse der aufgerufenen Operation und Informationen über eventuell aufgetretene Fehler gemäß [PHRService.wsdl].

### Fehlermeldungen

Die Operation *find* kann folgende Fehlermeldungen zurückliefern:

- 7200, 7202, 7205, 7206, 7209, 7214, 7215, 7220, 7221, 7400, 7403, 7404, 7406 gemäß Tab\_FM\_ePA\_011
- 4000 gemäß Tab\_FM\_ePA\_050
- reguläre bei IHE für [ITI-18] und [ITI-38] definierte Fehlermeldungen

### 7.1.1.3 getDocuments

Die Operation *getDocuments* ermöglicht Primärsystemen das Herunterladen von Dokumenten aus dem ePA-Aktensystem.

**Tabelle 24: Tab\_FM\_ePA\_027 Beschreibung und Parameter der Operation getDocuments (Semantik)**

Name	getDocuments
<b>Beschreibung</b>	Diese Operation ermöglicht Primärsystemen das Herunterladen von Dokumenten aus dem ePA-Aktensystem.

Aufrufparameter	Name	Beschreibung
	RetrieveDocumentSetRequest	Der Parameter enthält die gewünschte Download-Anfrage inklusive Parametern gemäß [PHRService.wsdl].
Rückgabeparameter	Name	Beschreibung
	RetrieveDocumentSetResponse	Der Parameter enthält die angefragten Dokumente oder Fehler, falls ein oder mehrere Dokumente nicht abgerufen werden konnten gemäß [PHRService.wsdl].

1694

1695 **Fehlermeldungen**

1696 Die Operation getDocuments kann folgende Fehlermeldungen zurückliefern:

- 1697 • 7200, 7202, 7205, 7206, 7209, 7211, 7212, 7214, 7215, 7220, 7221, 7400, 7403,  
1698 7404, 7406 gemäß Tab\_FM\_ePA\_011
- 1699 • 4000 gemäß Tab\_FM\_ePA\_050
- 1700 • reguläre bei IHE für [ITI-43] und [ITI-80] definierte Fehlermeldungen

1701 **7.1.1.4 removeDocuments**

1702 Die Operation removeDocuments ermöglicht Primärsystemen das Löschen von  
1703 Dokumenten aus dem ePA-Aktensystem.

1704

1705 **Tabelle 25: Tab\_FM\_ePA\_029 Beschreibung und Parameter der Operation**  
1706 **removeDocuments (Semantik)**

Name	removeDocuments	
Beschreibung	Diese Operation ermöglicht Primärsystemen das Löschen von Dokumenten aus dem ePA-Aktensystem.	
Aufrufparameter	Name	Beschreibung
	RemoveDocumentsRequest	Der Parameter enthält Referenzen auf die zu löschenden Dokumente gemäß [PHRService.wsdl].
Rückgabeparameter	Name	Beschreibung

	RegistryResponse	Der Parameter enthält den Status der aufgerufenen Operation und Informationen über eventuell aufgetretene Fehler gemäß [PHRService.wsdl].
--	------------------	---

1707 Die Unterstützung von [ITI-62] "Remove Metadata" ist nicht notwendig. Die  
 1708 Dokumentenverwaltung stellt sicher, dass sowohl Dokument als auch Metadaten gelöscht  
 1709 werden.

### 1710 Fehlermeldungen

1711 Die Operation removeDocuments kann folgende Fehlermeldungen zurückliefern:

- 1712 • 7200, 7202, 7205, 7206, 7209, 7214, 7215, 7220, 7221, 7400, 7403, 7404, 7406  
 1713 gemäß Tab\_FM\_ePA\_011
- 1714 • 4000 gemäß Tab\_FM\_ePA\_050
- 1715 • reguläre bei IHE für [ITI-86] definierte Fehlermeldungen

### 1716 7.1.1.5 updateDocumentSet des WebService Version 1.x (abgekündigt)

1717 Die Operation updateDocumentSet ermöglicht Primärsystemen, Metadaten bestehender  
 1718 Dokumente zu änderndes WebService Version 1.x wird mit einem Fehler abgebrochen.

1720 Tabelle 26: Tab\_FM\_ePA\_031 Beschreibung und Parameter der Operation  
 1721 updateDocumentSet (Semantik)

Name	updateDocumentSet	
Beschreibung	Diese Operation ermöglicht Primärsystemen das Ändern von Metadaten von Dokumenten.	
Aufrufparameter	Name	Beschreibung
	SubmitObjectsRequest	Der Parameter enthält Metadaten zu den zu aktualisierenden Dokumenten gemäß [PHRService.wsdl].
Rückgabeparameter	Name	Beschreibung
	RegistryResponse	Der <del>Parameter enthält die angefragten Dokumente oder Fehler, falls ein oder mehrere Dokumente nicht abgerufen werden konnten</del> 7400 wird in RegistryResponse gemäß [PHRService.wsdl].] als IHE-Fehler an das aufrufende Primärsystem zurückgegeben, da die



		<a href="#">Funktionalität nicht mehr unterstützt wird.</a>
--	--	---

## Fehlermeldungen

Die Operation updateDocumentSet kann folgende Fehlermeldungen zurückliefern:

- ~~7200, 7202, 7205, 7206, 7209, 7214, 7215, 7220, 7221, 7400, 7403, 7404, 7406 gemäß Tab\_FM\_ePA\_011~~
- ~~4000 gemäß Tab\_FM\_ePA\_050~~
- ~~reguläre bei IHE für [ITI-92] definierte Fehlermeldungen~~

## 7.1.2 Umsetzung

- [7400](#)

Die Operationen des Webservices PHRService sind IHE-basierte Anfragen. Die Verarbeitung durch das Fachmodul ePA läuft im Wesentlichen für alle Operation gleich ab:

1. Operationsaufruf vom Primärsystem entgegennehmen und Parameter prüfen
2. Login wie in Kapitel 6.5 beschrieben (optional, falls noch nicht geschehen)
3. Fachliche Transformation der Parameter (Verschlüsselung der Dokumente, Aktualisierung bestimmter Metadaten, etc.)
4. SOAP Security Header setzen
5. Weiterleitung der IHE-Transaktion an das ePA-Aktensystem
6. Antwort oder Fehlermeldung des ePA-Aktensystems entgegennehmen
7. Antwort oder Fehlermeldung erstellen und an das aufrufende Primärsystem zurückgeben

## Übergreifende Anforderungen bei der Umsetzung des Webservices PHRService

### A\_15191 - FM ePA: PHRService - Authentisierung mittels SM-B

Der Webservice PHRService MUSS sich zur Durchführung seiner Operationen mit einem über Aufrufkontext ausgewählten SM-B gegenüber dem Aktensystem authentisieren. [ $\leq$ ]

Die Authentisierung mittels SM-B und der weitere Login-Prozess sind in Kapitel 6.5 Login beschrieben. Der Aufrufkontext wird mithilfe der SOAP-Header bestimmt.

### A\_13964 - FM ePA: PHRService - SOAP Security Header

Vor der Weiterleitung an das ePA-Aktensystem MÜSSEN die Operationen des Webservices PHRService den SOAP Security Header mit der `AuthenticationAssertion` der authentifizierten LEI gemäß Kapitel 6.5 belegen. [ $\leq$ ]

Der Begriff „Dokument“ bezeichnet im Folgenden das Originaldokument, welches in unverschlüsselter Form vom Primärsystem in einer IHE-Nachricht zur Ablage im Aktensystem übertragen wird.

**A\_15626 - FM ePA: PHRService - Ver- und Entschlüsselung von Dokumenten - Fehler**

Falls die Ver- oder Entschlüsselung von Dokumenten fehlschlägt, MUSS das Fachmodul ePA die ausgeführte Operation mit dem Code 7400 gemäß Tab\_FM\_ePA\_011 abbrechen.[<=]

**A\_16209-01 - FM ePA: PHRService - Maximale Größe eines Dokuments**

Der Webservice PHRService MUSS ein Dokument mit einer Größe bis maximal 25 MB in einer Nachricht verarbeiten können. Die Größe eines Dokuments wird ohne Transportkodierung und ohne Verschlüsselung durch den Dokumentenschlüssel ermittelt.[<=]

**A\_16210 - FM ePA: PHRService - Maximale Größe eines Dokuments - Fehler**

Falls die Größe eines Dokuments die Größe von 25 MB in einer Nachricht übersteigt, dann MUSS der Webservice PHRService die Operation mit dem Code 7211 gemäß Tab\_FM\_ePA\_011 abbrechen.[<=]

**A\_16207 - FM ePA: PHRService - Maximale Größe aller Dokumente**

Der Webservice PHRService MUSS die Summe der Dokumente mit einer Größe bis maximal 250 MB in einer Nachricht verarbeiten können. Die Größe eines Dokuments wird ohne Transportkodierung ermittelt.[<=]

**A\_16208 - FM ePA: PHRService - Maximale Größe aller Dokumente - Fehler**

Falls die Summe der Dokumente die Größe von 250 MB in einer Nachricht übersteigt, dann MUSS der Webservice PHRService die Operation mit dem Code 7212 gemäß Tab\_FM\_ePA\_011 abbrechen.[<=]

**7.1.2.17.1.1.6 putDocuments**

Die Weiterleitung der Anfragen an die Komponente Dokumentenverwaltung und der Antworten der Dokumentenverwaltung zurück an das Primärsystem erreicht das Fachmodul ePA durch die Gruppierung von IHE-Akteuren. Dazu nimmt das Fachmodul ePA die Anfrage als XDR „Document Recipient“ vom Primärsystem entgegen und leitet sie anschließend an die Komponente Dokumentenverwaltung via [ITI-80] "Cross-Gateway Document Provide" in der Rolle eines XCDR Initiating Gateway an das ePA-Aktensystem weiter (vgl. hierzu[gemSpec\_DM\_ePA#Abbildung 2]). Das ePA-Aktensystem setzt dementsprechend ein XCDR Responding Gateway um. Die Antworten nehmen den umgekehrten Weg.

Die Gruppierung von XCDR- und XDR-Akteur wird durch das XCDR-Profil erzwungen.

**A\_14353 - FM ePA: putDocuments - Gruppierung von IHE-Akteuren**

Die Operation putDocuments Webservice PHRService MUSS die IHE-Akteure XDR Document Recipient [IHE-ITI-TF] und XCDR Initiating Gateway [IHE-ITI-XCDR] gruppieren.[<=]

**A\_15763 - FM ePA: PHR\_Service: Weiterleiten einer putDocuments-Anfrage**

Das Fachmodul ePA MUSS jede Operation putDocuments an das Dokumentenverwaltungssystem über die Operation I\_Document\_Management::CrossGatewayDocumentProvide gemäß [ITI-80] „Cross-Gateway Document Provide“ als IHE-XCDR-Akteur „Initiating Gateway“ weiterleiten.[<=]

**A\_15764 - FM ePA: PHR\_Service: Weiterleiten von putDocuments-Antwort**

Das Fachmodul ePA MUSS die Antwort der Dokumentenverwaltung auf eine Anfrage des Fachmoduls gemäß [ITI-80] „Cross-Gateway Document Provide“ als gruppierter IHE XCDR-Akteur „Initiating Gateway“ [IHE-ITI-XCDR] / IHE-XDR-Akteur „Document Recipient“ [IHE-ITI-TF] an das Primärsystem weiterleiten.[<=]

1806 Die Antwort der Dokumentenverwaltung auf eine Fachmodulanfrage gemäß [ITI-80]  
 1807 „Cross-Gateway Document Provide“ enthält keinerlei Metadatenfelder, die vor der  
 1808 Weiterleitung an das anfragende Primärsystem einer Transformation bedürfen.

1809

## 1810 Dokumentenverschlüsselung

### 1811 **A\_13907 - FM ePA: putDocuments - Verschlüsselung der Dokumente**

1812 Die Operation putDocuments MUSS jedes in der Nachricht übertragene Dokument vor der  
 1813 Weiterleitung an das ePA-Aktensystem durch eine Datenstruktur gemäß  
 1814 [gemSpec\_DM\_ePA#2.4] ersetzen.[<=]

1815

### 1816 **A\_18008 - FM ePA: putDocuments - Verschlüsselung der Dokumente mit** 1817 **Verschlüsselungsdienst**

1818 Bei der Verschlüsselung des Dokuments MUSS die Operation putDocuments das  
 1819 Dokument und den Dokumentenschlüssel wie folgt verschlüsseln:

Dokument mit TUC_KON_075 verschlüsseln	Eingangsdaten: <ul style="list-style-type: none"> <li>• dataToBeEncrypted = Dokument</li> </ul> Rückgabedaten: <ul style="list-style-type: none"> <li>• encryptedData (verschlüsseltes Dokument)</li> <li>• symmetricKey (Dokumentenschlüssel)</li> </ul> Der optionale Parameter AD wird nicht verwendet.
Dokumentenschlüssel mit TUC_KON_075 verschlüsseln	Eingangsdaten: <ul style="list-style-type: none"> <li>• dataToBeEncrypted = Dokumentenschlüssel</li> <li>• symmetricKey = Aktenschlüssel aus Session-Daten</li> </ul> Rückgabedaten: <ul style="list-style-type: none"> <li>• encryptedData (verschlüsselter Dokumentenschlüssel)</li> </ul> Der optionale Parameter AD wird nicht verwendet.

1820

1821 [<=]

1822

### 1823 **A\_13903 - FM ePA: putDocuments - Löschen der Dokumentenschlüssel**

1824 Die Operation putDocuments MUSS alle Dokumentenschlüssel nach ihrer Verschlüsselung  
 1825 mit dem Aktenschlüssel löschen.[<=]

## 1826 **7.1.2-27.1.1.7 find**

1827 Das Fachmodul ePA muss eine find-Anfrage, sofern sie den Anforderungen aus Kapitel  
 1828 7.1.1.2 genügt, anschließend an das ePA-Aktensystem weiterleiten. Das Fachmodul ePA

1829 agiert dabei als XCA "Initiating Gateway", während das ePA-Aktensystem ein XCA-  
 1830 „Responding Gateway“ umsetzt (siehe Operation  
 1831 I\_Document\_Management::CrossGatewayQuery gemäß  
 1832 [gemSpec\_Dokumentenverwaltung]). Die Antworten nehmen den umgekehrten Weg.

#### 1833 **A\_15765 - FM ePA: PHR\_Service: Weiterleiten einer find-Anfrage**

1834 Das Fachmodul ePA MUSS jede Operation find an das Dokumentenverwaltungssystem  
 1835 über die Schnittstelle I\_Document\_Management::CrossGatewayQuery gemäß [ITI-38]  
 1836 "Cross-Gateway Query" als IHE-XCA-Akteur „Initiating Gateway“ weiterleiten. [ $\leq$ ]

#### 1837 **A\_15766 - FM ePA: PHR\_Service: Weiterleiten von find-Antworten**

1838 Das Fachmodul ePA MUSS die Antwort der Dokumentenverwaltung auf eine  
 1839 I\_PHR\_Management::find-Anfrage des Fachmoduls gemäß [ITI-38] "Cross-Gateway  
 1840 Query" als IHE-XCA-Akteur „Initiating Gateway“ an das Primärsystem weiterleiten. [ $\leq$ ]

### 1841 **7.1.2.37.1.1.8 getDocuments**

1842 Das Fachmodul ePA muss eine eingehende Primärsystemanfrage, sofern sie den  
 1843 Anforderungen aus Kapitel 7.1.1.3 genügt, anschließend an das ePA-Aktensystem  
 1844 weiterleiten. Das Fachmodul ePA agiert dabei als XCA "Initiating Gateway", während das  
 1845 ePA-Aktensystem ein XCA-„Responding Gateway“ umsetzt (siehe Operation  
 1846 I\_Document\_Management::CrossGatewayRetrieve in  
 1847 [gemSpec\_Dokumentenverwaltung]).

#### 1848 **A\_15767 - Weiterleiten einer getDocuments-Anfrage an das ePA-Aktensystem**

1849 Das Fachmodul ePA MUSS jede Operation getDocuments an das  
 1850 Dokumentenverwaltungssystem über die Operation  
 1851 I\_Document\_Management::CrossGatewayRetrieve gemäß [ITI-39] "Cross-Gateway  
 1852 Retrieve" als IHE-XCA-Akteur „Initiating Gateway“ weiterleiten. [ $\leq$ ]

#### 1853 **A\_15768 - FM ePA: PHR\_Service: Weiterleiten von getDocuments-Antworten**

1854 Das Fachmodul ePA MUSS die Antwort der Dokumentenverwaltung auf eine Anfrage des  
 1855 Fachmoduls gemäß [ITI-39] "Cross-Gateway Retrieve" als IHE-XCA-Akteur „Initiating  
 1856 Gateway“ an das Primärsystem weiterleiten. [ $\leq$ ]

1857

### 1858 **Dokumentenentschlüsselung**

#### 1859 **A\_14700 - FM ePA:getDocuments - Entschlüsselung der Dokumente**

1860 Die Operation getDocuments MUSS jedes übertragene Dokument (Datenstruktur gemäß  
 1861 [A\\_14977](#)) vor der Weiterleitung an das Primärsystem durch das jeweilige entschlüsselte  
 1862 Dokument (Ergebnis aus [A\\_18009](#)) ersetzen.

1863

1864 [ $\leq$ ]

## A\_18009 - FM ePA: getDocuments - Entschlüsselung der Dokumente mit Signaturdienst

Bei der Entschlüsselung des Dokuments MUSS die Operation getDocuments das Dokument und den Dokumentenschlüssel wie folgt entschlüsseln:

Dokumentenschlüssel mit TUC_KON_076 entschlüsseln	<p>Eingangsdaten:</p> <ul style="list-style-type: none"> <li>encryptedData = verschlüsselter Dokumentenschlüssel aus EncryptedData\EncryptedKey\CipherData</li> <li>symmetricKey = Aktenschlüssel (RecordKey) aus Session-Daten</li> </ul> <p>Rückgabedaten:</p> <ul style="list-style-type: none"> <li>plainData (entschlüsselter Dokumentenschlüssel)</li> </ul> <p>Der optionale Parameter AD wird nicht verwendet.</p>
Dokument mit TUC_KON_076 entschlüsseln	<p>Eingangsdaten:</p> <ul style="list-style-type: none"> <li>encryptedData (verschlüsseltes Dokument aus EncryptedData\CipherData)</li> <li>symmetricKey (Dokumentenschlüssel)</li> </ul> <p>Rückgabedaten:</p> <ul style="list-style-type: none"> <li>plainData (entschlüsseltes Dokument)</li> </ul> <p>Der optionale Parameter AD wird nicht verwendet.</p>

[<=]

## A\_14959 - FM ePA: getDocuments - Löschen der Dokumentenschlüssel

Die Operation getDocuments MUSS Dokumentenschlüssel nach ihrer Verwendung zur Entschlüsselung eines Dokuments löschen.

[<=]

### 7.1.2.47.1.1.9 removeDocuments

Die Weiterleitung der removeDocument-Anfragen an die Komponente Dokumentenverwaltung und der Antworten der Dokumentenverwaltung zurück an das Primärsystem erreicht das Fachmodul ePA durch die Kombination zweier IHE-Akteure. Dazu nimmt das Fachmodul ePA die Anfrage als IHE-Akteur RMD "Document Repository" vom Primärsystem entgegen und leitet sie anschließend in der Rolle eines RMD "Document Administrator" an das ePA-Aktensystem weiter (vgl. hierzu Abbildung Abb\_FM\_ePA\_001 IHE-Akteure und Transaktionen der Fachanwendung ePA). Das ePA-Aktensystem setzt dementsprechend ein RMD Document Repository über die Schnittstelle removeDocuments um. Die Antworten nehmen den umgekehrten Weg.

Diese Kombination beider Akteure ist deshalb notwendig, da IHE bislang keine explizite "Cross-Community"-Variante für das RMD-Profil spezifiziert hat.

**A\_15769 - FM ePA: PHR\_Service: Weiterleiten einer removeDocuments-Anfrage**  
Das Fachmodul ePA MUSS jede Operation removeDocuments an das Dokumentenverwaltungssystem über die Operation I\_Document\_Management::RemoveDocuments gemäß [ITI-86] "Remove Documents" als IHE-RMD-Akteur "Document Administrator" weiterleiten. [ $\leq$ ]

**A\_15770 - FM ePA: PHR\_Service: Weiterleiten von removeDocuments-Antwort**  
Das Fachmodul ePA MUSS die Antwort der Dokumentenverwaltung auf eine I\_Document\_Management::RemoveDocuments-Anfrage des Fachmoduls gemäß [ITI-86] "Remove Documents" als kombinierter IHE RMD-Akteur „Document Administrator“ / IHE RMD-Akteur "Document Repository", beide gemäß [IHE-ITI-RMD], an das Primärsystem weiterleiten. [ $\leq$ ]

Es müssen keine Metadaten in Anfragen oder Antworten der Operation removeDocuments transformiert werden.

#### **7.1.2.57.1.1.10 updateDocumentSet (abgekündigt)**

Die Weiterleitung der Anfragen an die Komponente Dokumentenverwaltung und der Antworten der Dokumentenverwaltung zurück an das Primärsystem erreicht das Fachmodul ePA durch die Gruppierung der IHE-Akteure RMU Update Responder und RMU Update Initiator. Dazu nimmt das Fachmodul ePA die Anfrage als Update Responder vom Primärsystem entgegen und leitet sie anschließend an die Komponente Dokumentenverwaltung via [ITI-92] "Restricted Update Document Set" in der Rolle eines RMU Update Initiator an das ePA-Aktensystem weiter (vgl. hierzu Abbildung Abb\_FM\_ePA\_001 IHE-Akteure und Transaktionen der Fachanwendung ePA). Das ePA-Aktensystem setzt dementsprechend ein RMU Update Responder um. Die Antworten nehmen den umgekehrten Weg.

Die Gruppierung von RMU Update Responder und RMU Update Initiator wird auch durch die "Forward Update" Option des RMU Update Responders gemäß RMU-Profil erzwungen.

#### **A\_15073 - FM ePA: PHR\_Service - Gruppierung für updateDocumentSet**

Die Operation updateDocumentSet MUSS die IHE-Akteure RMU Update Responder und RMU Update Initiator (beide gemäß [IHE-ITI-RMU]) gruppieren. [ $\leq$ ]

#### **A\_15771 - PHR\_Service: Weiterleiten einer updateDocumentSet-Anfrage**

Das Fachmodul ePA MUSS jede Operation updateDocumentSet an das Dokumentenverwaltungssystem über die Operation I\_Document\_Management::UpdateDocumentSet gemäß [ITI-92] "Restricted Update Document Set" als IHE-RMU-Akteur „Update Initiator“ weiterleiten. [ $\leq$ ]

#### **A\_15772 - FM ePA: PHR\_Service: Weiterleiten von updateDocumentSet-Antwort**

Das Fachmodul ePA MUSS die Antwort der Dokumentenverwaltung auf eine I\_Document\_Management::UpdateDocumentSet-Anfrage des Fachmoduls gemäß [ITI-92] "Restricted Update Document Set" als gruppierter IHE-RMU-Akteur "Update Initiator" / IHE-RMU-Akteur "Update Responder", beide gemäß [IHE-ITI-RMU], an das Primärsystem weiterleiten. [ $\leq$ ]

Die Antwort der Dokumentenverwaltung auf eine Fachmodulanfrage gemäß [ITI-92] "Cross-Gateway Document Provide" enthält keinerlei Metadatenfelder, die vor der Weiterleitung an das anfragende Primärsystem einer Transformation bedürfen.

Es erfolgt keine Weiterleitung der Anfragen an die Komponente Dokumentenverwaltung. Die Operation updateDocumentSet wird mit Fehler 7400 abgebrochen.



## **A\_20090 - Operation updateDocumentSet nicht unterstützt**

Die Operation updateDocumentSet des Webservice PHRService 1.x MUSS die aufgerufene Operation mit dem Code 7400 gemäß Tab FM\_ePA\_011 abbrechen. [ $\leq$ ]

## **7.2 PHRManagementService**

In ePA 2.0 werden 2 Versionen des Webservice PHRManagementService unterstützt, die sich in der Operation RequestFacilityAuthorization unterscheiden.

Der Webservice PHRManagementService V1.x unterstützt wie bisher die Operation RequestFacilityAuthorization auf Basis der 3 Kategorien Versicherter, Arzt und Kasse.

Der Webservice PHRManagementService V2.x ist neu und unterstützt mit der Operation RequestFacilityAuthorization Version 2.x die mittelgranulare und grobgranulare Berechtigung.

Wenn sich die Anforderungen für die beiden Versionen der Operation RequestFacilityAuthorization unterscheiden, so wird die neue Anforderung als Suffix-Anforderung den Bezug zu V2.x herstellen. Die parallel hierzu bereits existierende Anforderung gilt für RequestFacilityAuthorization 1.x. Alle Anforderungen gelten für beide Versionen.

Der Webservice PHRManagementService setzt die logischen Schnittstellen I\_Account\_Administration und I\_Authorization\_Administration gemäß [gemSysL\_ePA] um.

### **A\_13818-03 - FM ePA: PHRManagementService Version 2.x**

~~A\_13818-01 - FM ePA: PHRManagementService~~ Das Fachmodul ePA MUSS für Primärsysteme den Webservice PHRManagementService Version 2.x gemäß Tabelle Tab\_FM\_ePA\_003 anbieten.

**Tabelle 27: Tab\_FM\_ePA\_003 Beschreibung des Webservices PHRManagementService**

Name	PHRManagementService	
Versio n	<u>1-2.0.0</u>	
Namen raum	<u><a href="http://ws.gematik.de/conn/WSDL/PHRManagementService/v1.2">http://ws.gematik.de/conn/WSDL/PHRManagementService/v1.2</a> – <a href="http://ws.gematik.de/conn/phrs/PHRManagementService/WSDL/v2.0">http://ws.gematik.de/conn/phrs/PHRManagementService/WSDL/v2.0</a></u>	
Abkürz ung Namen raum	phr_management	
Operati onen	Name	Beschreibung
	ActivateAccount	Aktivierung eines Aktenkontos
	RequestFacilityAuthorization	Berechtigungsvergabe für eine LEI ( <u><a href="#">Berechtigungserteilung grobgranular und mittelgranular</a></u> )



	GetHomeCommunityID	Identifizierung eines ePA-Aktensystems
	GetAuthorizationList	Abruf aller Berechtigungen einer LEI
<b>WSDL</b>	<b>PHRManagementService_V2_0_0.wsdl</b>	

Der Dienst wird vom Fachmodul ePA im Dienstverzeichnis des Konnektors registriert und damit für Primärsysteme auffindbar gemacht (siehe Kapitel 6.8 Verwendung des Dienstverzeichnisdienstes).

[<=]

#### A 13818-02 - FM ePA: PHRManagementService

Das Fachmodul ePA MUSS für Primärsysteme den Webservice PHRManagementService gemäß Tabelle Tab FM ePA 003 anbieten.

**Tabelle 28: Tab FM ePA 003 Beschreibung des Webservices PHRManagementService**

<b>Name</b>	<b>PHRManagementService</b>	
<b>Version</b>	<b>1.3.0</b>	
<b>Namensraum</b>	<b><a href="http://ws.gematik.de/conn/phrs/PHRManagementService/WSDL/v1.3">http://ws.gematik.de/conn/phrs/PHRManagementService/WSDL/v1.3</a></b>	
<b>Abkürzung Namensraum</b>	<b><a href="#">phr_management</a></b>	
<b>Operationen</b>	<b>Name</b>	<b>Beschreibung</b>
	<a href="#">ActivateAccount</a>	<a href="#">Aktivierung eines Aktenkontos</a>
	<a href="#">RequestFacilityAuthorization</a>	<a href="#">Berechtigungsvergabe für eine LEI</a>
	<a href="#">GetHomeCommunityID</a>	<a href="#">Identifizierung eines ePA-Aktensystems</a>
	<a href="#">GetAuthorizationList</a>	<a href="#">Abruf aller Berechtigungen einer LEI</a>
<b>WSDL</b>	<b><a href="#">PHRManagementService.wsdl</a></b>	

Der Dienst wird vom Fachmodul ePA im Dienstverzeichnis des Konnektors registriert und damit für Primärsysteme auffindbar gemacht (siehe Kapitel 6.8 Verwendung des Dienstverzeichnisdienstes).

[<=]

### **7.2.1 Definition/Signatur**

Dieses Unterkapitel beschreibt die in [PHRManagementService.wsdl] definierten Methoden, d.h. Aufruf- und Rückgabeparameter sowie alle möglichen Fehlermeldungen.

1977 **7.2.1.1 ActivateAccount**

1978 **Tabelle 29: Tab\_FM\_ePA\_016 Beschreibung und Parameter der Operation**  
 1979 **ActivateAccount (Semantik)**

Name	ActivateAccount	
<b>Beschreibung</b>	Mit dieser Operation startet das Primärsystem die Aktivierung des beantragten Aktenkontos des Versicherten bei seinem Anbieter ePA-Aktensystem. Mithilfe des <code>RecordIdentifier</code> und der darin enthaltenen <code>HomeCommunityID</code> des Anbieters ePA-Aktensystem wird das Aktenkonto des Versicherten lokalisiert. Als Ergebnis der Operation wird die Zugriffsberechtigung für den Versicherten im ePA-Aktensystem hinterlegt.	
<b>Aufrufparameter</b>	<b>Name</b>	<b>Beschreibung</b>
	Context	Aufrufkontext gemäß [ConnectorContext.xsd]
	EhcHandle	eGK der Versicherten gemäß [gemSpec_Kon#4.1.1.1]
	RecordIdentifier	Kennung der Akte des Versicherten gemäß [gemSpec_DM_ePA#2.2]
<b>Rückgabeparameter</b>	<b>Name</b>	<b>Beschreibung</b>
	Status	Status nach [gemSpec_Kon#3.5.2]

1980

1981 Die Operation ActivateAccount kann folgende Fehlermeldungen zurückliefern:

- 1982 • 7200, 7202, 7203, 7205, 7206, 7207, 7213, 7215, 7220, 7400, 7402, 7403,  
 1983 7404, 7405, 7406 gemäß Tab\_FM\_ePA\_011
- 1984 • Fehlermeldungen gemäß Tab\_FM\_ePA\_050
- 1985 • Fehlermeldungen gemäß Tab\_FM\_ePA\_051

1986

1987 **7.2.1.2 RequestFacilityAuthorization**

1988 **Tabelle 30: Tab\_FM\_ePA\_020 Beschreibung und Parameter der Operation**  
 1989 **RequestFacilityAuthorization (Semantik)**

Name	RequestFacilityAuthorization
<b>Beschreibung</b>	Die Operation startet den Autorisierungsprozess zur Berechtigungsvergabe für die Leistungserbringerinstitution in

	dem über <code>RecordIdentifier</code> referenzierten Aktenkonto des Versicherten. Die Berechtigung der Leistungserbringerinstitution erfolgt für eine vom Primärsystem angegebene <code>AuthorizationConfiguration</code> . Das Fachmodul ePA stellt die <code>AuthorizationConfiguration</code> am Kartenterminal dar und lässt sie vom Versicherten oder einem von ihm berechtigten Vertreter mittels PIN-Eingabe bestätigen. Als Ergebnis der Operation hat der Versicherte einer Leistungserbringerinstitution eine Zugriffsberechtigung auf seine Akte erteilt.	
Aufrufparameter	Name	Beschreibung
	Context	Aufrufkontext gemäß [ConnectorContext.xsd]
	EhcHandle	eGK des Versicherten oder des von ihm berechtigten Vertreters gemäß [gemSpec_Kon#4.1.1.1]
	AuthorizationConfiguration	Konfiguration der Zugriffsberechtigung, die eine konkrete Policy adressiert und das Gültigkeitsdatum bis wann die Zugriffsberechtigung erteilt wird
	RecordIdentifier	<code>RecordIdentifier</code> gemäß [gemSpec_DM_ePA#2.2]
	OrganizationName	Name der Leistungserbringerinstitution
	InsurantName	Name des Versicherten des durch <code>RecordIdentifier</code> referenzierten Aktenkontos
Rückgabeparameter	Name	Beschreibung
	Status	Status nach [gemSpec_Kon#3.5.2]

1990

1991 Die Operation `RequestFacilityAuthorization` kann folgende Fehlermeldungen zurückliefern:

1992 • 7200, 7202, 7203, 7205, 7206, 7207, 7213, 7214, 7215, 7217, 7220, 7400,  
1993 7403, 7404, 7406 gemäß Tab\_FM\_ePA\_011

1994 • Fehlermeldungen gemäß Tab\_FM\_ePA\_050

1995 • Fehlermeldungen gemäß Tab\_FM\_ePA\_051

1996 **7.2.1.3 GetHomeCommunityID**
 1997 **Tabelle 31: Tab\_FM\_ePA\_039 Beschreibung und Parameter der Operation**  
 1998 **GetHomeCommunityID (Semantik)**

<b>Name</b>	GetHomeCommunityID	
<b>Beschreibung</b>	Mit dieser Operation kann ein Primärsystem das ePA-Aktensystem zu einem Aktenkonto anhand der Versicherten-ID lokalisieren. Das Fachmodul ePA iteriert dafür über alle bekannten Anbieter ePA-Aktensystem und ruft dort jeweils die Operation <code>I_Authorization_Management::checkRecordExists</code> auf. Der zurückgegebene Parameter <code>HomeCommunityID</code> enthält die OID des ePA-Aktenanbieters und ist Teil des <code>RecordIdentifiers</code> , den Primärsysteme zum Aufruf weiterer Operationen des Fachmoduls ePA benötigen.	
<b>Aufrufparameter</b>	<b>Name</b>	<b>Beschreibung</b>
	Context	Aufrufkontext gemäß [ConnectorContext.xsd]
	InsurantID	Unveränderlicher Teil der Krankenversicherungsnummer nach [gemSpec_DM_ePA#2.2]
<b>Rückgabeparameter</b>	<b>Name</b>	<b>Beschreibung</b>
	HomeCommunityID	OID des ePA-Aktensystems gemäß [gemSpec_DM_ePA]
	Status	Status gemäß [gemSpec_Kon#3.5.2]

 1999  
 2000 Die Operation `GetHomeCommunityID` kann folgende Fehlermeldungen zurückliefern:

- 2001
- 7200, 7202, 7206, 7220, 7400 gemäß Tab\_FM\_ePA\_011
- 2002
- 4000 gemäß Tab\_FM\_ePA\_050
- 2003
- Fehlermeldungen gemäß Tab\_FM\_ePA\_032

2004 **Tabelle 32: Tab\_FM\_ePA\_032 Fehlermeldungen der Operation GetHomeCommunityID**

Code	ErrorType	Severity	Fehlertext
7290	Technical	ERROR	Die Patientenakte konnte nicht gefunden werden.
7291	Technical	ERROR	Die Patientenakte konnte nicht eindeutig identifiziert werden.

2005

## 2006 7.2.1.4 GetAuthorizationList

2007

2008 **Tabelle 33: Tab\_FM\_ePA\_040 Beschreibung und Parameter der Operation**  
 2009 **GetAuthorizationList (Semantik)**

Name	GetAuthorizationList	
Beschreibung	Mit der Operation GetAuthorizationList kann eine LEI alle für sie erteilten Zugriffsberechtigungen auf Akten der ePA-Aktensysteme abfragen. Das Fachmodul ePA iteriert dafür über alle bekannten Anbieter von ePA-Aktensystemen und ruft dort die Operation I_Authorization_Management::getAuthorizationList der jeweiligen Komponente Autorisierung auf. Als Parameter muss dabei eine AuthenticationAssertion übergeben werden. Die Rückgabeparameter umfassen die AuthorizationList, welche eine Liste von Tupeln (RecordIdentifier, Enddatum der Berechtigung) enthält, sowie den Status des Operationsaufrufes gemäß [gemSpec_Kon#3.5.2].	
Aufrufparameter	Name	Beschreibung
	Context	Aufrufkontext gemäß [ConnectorContext.xsd]
Rückgabeparameter	Name	Beschreibung
	AuthorizationList	Liste aller Zugriffsberechtigungen für die LEI
	Status	Status gemäß [gemSpec_Kon#3.5.2]

2010 Die Operation GetAuthorizationList kann folgende Fehlermeldungen zurückliefern:

- 2011 • 7200, 7202, 7205, 7206, 7214, 7220, 7221, 7400 gemäß Tab\_FM\_ePA\_011
- 2012 • 4000 gemäß Tab\_FM\_ePA\_050
- 2013 • Fehlermeldungen gemäß Tab\_FM\_ePA\_041

2014

2015 **Tabelle 34: Tab\_FM\_ePA\_041 Fehlermeldungen der Operation GetAuthorizationList**

Code	ErrorType	Severity	Fehlertext
7230	Technical	WARNING	Die Liste der Berechtigungen ist möglicherweise unvollständig, da nicht alle bekannten Aktensysteme abgefragt werden konnten.
7231	Technical	ERROR	Die Abfrage getAuthorizationList wurde zu häufig gestellt.

2016

## 2017 7.2.2 Umsetzung

### 2018 Authentisierung gegenüber dem Aktensystem

#### 2019 A\_15192 - FM ePA: PHRManagementService - Authentisierung mittels eGK

2020 Der Webservice PHRManagementService MUSS sich zur Durchführung der Operationen  
2021 ActivateAccount und RequestFacilityAuthorization mit der in den Aufrufparametern  
2022 referenzierten eGK gegenüber dem Aktensystem authentisieren. [ <= ]

#### 2023 A\_15193 - FM ePA: PHRManagementService - Authentisierung mittels SM-B

2024 Der Webservice PHRManagementService MUSS sich zur Durchführung der Operation  
2025 GetAuthorizationList mit einem über Aufrufkontext ausgewählten SM-B gegenüber dem  
2026 Aktensystem authentisieren.  
2027 [ <= ]

2028 Die Authentisierung mittels SM-B bzw. eGK und der weitere Login-Prozess sind in Kapitel  
2029 6.5 Login beschrieben. Der Aufrufkontext wird in den Parametern der Operationen  
2030 übergeben.

2031 Der Aufruf der Operation GetHomeCommunityID erfordert keine Authentisierung  
2032 gegenüber dem ePA-Aktensystem.

2033

### 2034 Übergreifende Regelungen für PHRManagementService

#### 2035 A\_14266 - FM ePA: PHRManagementService – Befüllung des 2036 Rückgabeparameters Status

2037 Das Fachmodul ePA MUSS bei jeder erfolgreich durchlaufenen Operation von  
2038 PHRManagementService den Parameter Status im Element Status/Result mit „OK“  
2039 befüllen (vgl. [ConnectorCommon.xsd]).  
2040 [ <= ]

#### 2041 A\_17121 - FM ePA: PHRManagementService - Berechtigung in Komponente 2042 Autorisierung - Fehler

2043 Falls die Operation I\_Authorization\_Management::putAuthorizationKey einen Fehler  
2044 zurückgibt, MUSS der Webservice PHRManagementService die aufgerufene Operation mit  
2045 dem Code 7400 gemäß Tab\_FM\_ePA\_011 abbrechen. [ <= ]

2046 Fehlerrückgaben der Operation I\_Authorization\_Management::putAuthorizationKey  
2047 werden in [gemSpec\_Autorisierung] spezifiziert.

### 2048 7.2.2.1 ActivateAccount

2049 Der Ablauf der Operation ActivateAccount ist in [gemSysL\_ePA#3.5.1] beschrieben und  
2050 gliedert sich in die folgenden Schritte:

- 2051 1. Prüfung der Parameter und des Sperrstatus der eGK
- 2052 2. Login des Versicherten mit der eGK
- 2053 3. Schlüsselmateriale erzeugen und verschlüsseln
- 2054 4. Hinterlegen des verschlüsselten Schlüsselmateriale für den Versicherten in der
- 2055 Komponente Autorisierung

### 2056 Authentisierung des Versicherten gegenüber dem Aktensystem

2057 Die Authentisierung gegenüber einem Aktensystem erfolgt gemäß A\_15192 mit der eGK.  
2058 Der vollständige Login-Prozess ist in Kapitel 6.5 Login beschrieben.  
2059

**Erzeugung des Schlüsselmaterials für den Zugriff durch die eGK**

Übergreifende Festlegungen zur Datensicherheit befinden sich in Kapitel 6.7 Datenschutz und Sicherheitsaspekte. Für die Verschlüsselung von Akten- und Kontextschlüssel gelten die Vorgaben aus [gemSpec\_SGD\_ePA#8].

Voraussetzung ist die Nutzung einer eGK G2 oder höher, wobei eine eGK G2 die Kryptographie mit RSA unterstützt. Eine eGK ab G2.1 unterstützt die Kryptographie mit RSA und ECC. Die normierenden Organisationen haben das Ende der Zulässigkeit für den RSA-2048 festgelegt. Aus diesem Grund wird bei Nutzung einer eGK G2 die Kryptographie mit RSA und bei eGK einer höheren Generation die Kryptographie mit ECC verwendet.

**A\_14742 - FM ePA: ActivateAccount - Akten- und Kontextschlüssel erzeugen**

Die Operation ActivateAccount MUSS einen Kontext- und einen Aktenschlüssel erzeugen. [ $\leq$ ]

**Schlüsselableitung und Verschlüsselung von Akten- und Kontextschlüssel**

Das Chifftrat von Akten- und Kontextschlüssel im Schlüsselkasten wird bei der Aktivierung des Aktenkontos in der Komponente Autorisierung hinterlegt. Hierzu werden Akten- und Kontextschlüssel mit zwei AES-256-Schlüsseln verschlüsselt. Die für die Verschlüsselung des Chifftrats benötigten zwei AES-256-Schlüssel ruft das Fachmodul ePA von den SGD's 1 und 2 ab (siehe Kap. 6.5.6- Schlüsselableitung).

**A\_17743 - FM ePA: ActivateAccount - Akten- und Kontextschlüssel für den Versicherten verschlüsseln**

Die Operation ActivateAccount MUSS gemäß dem in [gemSpec\_SGD\_ePA#2.4] beschriebenen Algorithmus die zur Verschlüsselung notwendigen AES-Schlüssel abrufen und Akten- und Kontextschlüssel gemäß [gemSpec\_Krypt#A\_17872] und [gemSpec\_SGD\_ePA#8] verschlüsseln.

[ $\leq$ ]

**Hinterlegen des Schlüsselmaterials für den Versicherten in der Komponente Autorisierung**

Zur Hinterlegung des Schlüsselmaterials wird eine TLS-Verbindung zur Komponente Autorisierung aufgebaut. Die normativen Festlegungen hierzu befinden sich in Kapitel 6.5.4.

**A\_14749 - FM ePA: ActivateAccount - Hinterlegen des verschlüsselten Schlüsselmaterials**

Die Operation ActivateAccount MUSS zur Hinterlegung der Berechtigung in der Komponente Autorisierung die Operation I\_Authorization\_Management::putAuthorizationKey gemäß [gemSpec\_Autorisierung] mit folgenden Parametern aufrufen:

- AuthenticationAssertion: als SOAP-Header, AuthenticationToken aus dem Login-Prozess zum ePA-Aktensystem
- RecordIdentifier: Parameter der aufrufenden Operation
- AuthorizationKey: AuthorizationKey: Berechtigung des Versicherten; doppelt verschlüsseltes Chifftrat und AssociatedData (aus den Antwortnachrichten der SGD's) als EncryptedKeyContainer gemäß [gemSpec\_SGD\_ePA#8]
- validTo: aktuelles Datum
- actorID: Versicherten-ID der eGK



- AuthorizationType: DOCUMENT\_AUTHORIZATION

[&lt;=]

### **A\_14271 - FM ePA: ActivateAccount - Terminalanzeige für PIN-Eingaben der Operation**

Die Operation ActivateAccount MUSS für notwendige PIN-Eingaben am Kartenterminal die in Tabelle Tab\_FM\_ePA\_021 definierte Terminalanzeige verwenden.

**Tabelle 35: Tab\_FM\_ePA\_021 Terminalanzeigen für PIN-Eingaben - Operation ActivateAccount**

PIN-Objekt zur Freischaltung (PIN-Referenz)	Parameter "Anw" für Terminalanzeigen nach [gemSpec_Kon# TAB_KON_090]
PIN.CH	Aktenkonto•0x0Baktivieren

[&lt;=]

### **7.2.2.2 RequestFacilityAuthorization**

In ePA 2.0 werden 2 Versionen der Operation RequestFacilityAuthorization unterstützt. Der Webservice PHRManagementService V1.x unterstützt wie bisher die Operation RequestFacilityAuthorization auf Basis der 3 Kategorien Versicherter, Arzt und Kasse. Der Webservice PHRManagementService V2.x ist neu und unterstützt mit der Operation RequestFacilityAuthorization die mittelgranulare und grobgranulare Berechtigung. Wenn sich die Anforderungen für die beiden Versionen der Operation RequestFacilityAuthorization unterscheiden, so wird die neue Anforderung als Suffix-Anforderung den Bezug zu V2.x herstellen. Die parallel hierzu bereits existierende Anforderung gilt für RequestFacilityAuthorization 1.x. Alle Anforderungen gelten für beide Versionen.

#### **Auswahl eines SM-B**

Das Fachmodul ePA sucht ein SM-B aus dem fest konfigurierten Informationsmodell des Konnektors, das dem übertragenen Context zugeordnet ist und zuvor durch PIN-Eingabe freigeschaltet wurde (siehe A\_15614). Die Berechtigungsvergabe zum Zugriff auf ein Aktenkonto erfolgt für eine LEI, identifiziert durch die Telematik-ID.

#### **Bestätigung der Berechtigung per PIN-Eingabe**

### **A\_14769 - FM ePA: RequestFacilityAuthorization - Bestätigung der Berechtigung**

Die Operation RequestFacilityAuthorization MUSS vor dem Einbringen der Berechtigungen in die Komponenten Autorisierung und Dokumentenverwaltung die PIN.CH des Versicherten, identifiziert durch den Parameter EhCHandle, abfragen.[<=]

### **A\_16216-01A\_16216 - FM ePA: RequestFacilityAuthorization - Terminalanzeige für PIN-Eingaben der Operation**

Die Operation RequestFacilityAuthorization MUSS für notwendige PIN-Eingaben der Operation RequestFacilityAuthorization am Kartenterminal die in Tab\_FM\_ePA\_019 definierte Terminalanzeige verwenden.

**Tabelle 36: Tab\_FM\_ePA\_019 Terminalanzeigen für PIN-Eingaben - Operation RequestFacilityAuthorization**

PIN-Objekt zur Freischaltung (PIN-Referenz)	Parameter "Anw" für Terminalanzeigen nach [gemSpec_Kon# TAB_KON_090]
PIN.CH	<del>Schritt 5:</del> Aktenzugriff

[<=]

**A\_16212 - FM ePA: RequestFacilityAuthorization - Anzeige am Kartenterminal - Anzeigetext**  
~~FM ePA: RequestFacilityAuthorization - Anzeige am Kartenterminal - Anzeigetext~~

Im Rahmen der Abfrage der PIN.CH zur Erteilung der Berechtigung MUSS die Operation RequestFacilityAuthorization unmittelbar vor der PIN-Abfrage die Anzeigetexte in der vorgegebenen Reihenfolge gemäß Tab\_FM\_ePA\_025 am Kartenterminal darstellen.

**Tabelle 37: Tab\_FM\_ePA\_025: Operation RequestFacilityAuthorization - Ausgabetexte am Kartenterminal**

Ausgabe am Kartenterminal	Quelle	Verfügbare Länge für Parameter
Es•folgen•4•Anzeigen. •0x0B Bitte•mit•[OK]•bestätigen!	-	-
1:Berechtigung•für•0x0B <OrganizationName>	Parameter OrganizationName*	27
2:auf•Akte•von•0x0B <Vorname>•<Nachname>	Parameter InsurantName* Wenn die Länge <Vorname> + Länge <Nachname> größer ist als 30 Zeichen, dann wird der Vorname nach 9 Zeichen abgeschnitten und mit '.' beendet.	30
3:mit•Ende•der•Berechtigung: •0x0B <ExpirationDate>	Parameter ExpirationDate als tt.mm.jjjj	10

4:  für•Dokumente•von• <b>0x0B</b> Vers.: [<• x>] •Med.: [<• x>] •Kasse: [<• x>]	<• x>: Anzeige <•>, falls keine Berechtigung (false) für den Dokumententopf erteilt wird Anzeige <x>, falls die Berechtigung (true) für den Dokumententopf erteilt wird Vers.: Der Wert entspricht dem Parameter AuthorizationConfiguration. Vers_Docs Med.: Der Wert entspricht dem Parameter AuthorizationConfiguration. LE_Docs Kasse: Der Wert entspricht dem Parameter AuthorizationConfiguration. KTR_Docs	3 mal 1
---	---	---------

## Hinweise:

1. Die Inhalte der mit '\*' markierten Parameter werden auf die maximal mögliche Anzahl der verbleibenden Zeichen für den Eingabetext gekürzt. Nicht genutzte Zeichen werden nicht zur Anzeige gebracht.
  2. Leerzeichen werden als "•" dargestellt
  3. 0x0B und 0x0F (Sollbruchstellen bzw. Trennung zwischen Nachricht und PIN-Prompt) sind Trennzeichen gemäß [SICCT#5.6.1]
  4. Die Zeilenumbrüche in der Spalte "Ausgabe am Kartenterminal" sind editorisch bedingt.
- [<=]**

An folgendem Beispiel wird die Anzeige am Kartenterminal und die Eingabe des Versicherten bei der Operation RequestFacilityAuthorization gezeigt:

Anzeige am Kartenterminal	Eingabe des Versicherten
Es folgen 4 Anzeigen. Bitte mit [OK] bestätigen!	Taste: OK
1:Berechtigung für Praxis Dr. Müller	Taste: OK
2:auf Akte von Max Mustermann	Taste: OK
3:mit Ende der Berechtigung: 01.08. <del>2019</del> 2021	Taste: OK
4:für Dokumente von Vers.: [x] Med.: [x] Kasse: [ ]	Taste: OK
PIN für Schritt 5: Aktenzugriff PIN.eGK:	PIN-Eingabe: 123456

Im Beispiel erteilt Max Mustermann der Praxis Dr. Müller bis 01.08.~~2019~~2021 die Berechtigung, auf die Dokumente des Versicherten und von Leistungserbringern gemäß [gemSpec\_Dokumentenverwaltung#5.3] zuzugreifen.

## A 16212-01 - FM ePA: RequestFacilityAuthorization Version 2.x - Anzeige am Kartenterminal - Anzeigetext

Im Rahmen der Abfrage der PIN.CH zur Erteilung der Berechtigung MUSS die Operation RequestFacilityAuthorization Version 2.x unmittelbar vor der PIN-Abfrage die Anzeigetexte in der vorgegebenen Reihenfolge gemäß Tab FM ePA 025 am Kartenterminal darstellen.

**Tabelle 38: Tab FM ePA 025: Operation RequestFacilityAuthorization Version 2 - Ausgabetexte am Kartenterminal**

<u>Ausgabe am Kartenterminal</u>	<u>Quelle</u>	<u>Verfügbare Länge für Parameter</u>
<u>Es•folgen•4•Anzeigen. •0x0B</u> <u>Bitte•mit•[OK]•bestätigen!</u>	=	=
<u>1:Berechtigung•für•0x0B</u> <u>&lt;OrganizationName&gt;</u>	<u>Parameter OrganizationName*</u>	<u>27</u>
<u>2:auf•Akte•von•0x0B</u> <u>&lt;Vorname&gt;•&lt;Nachname&gt;</u>	<u>Parameter InsurantName*</u> <u>Wenn die Länge &lt;Vorname&gt; + Länge &lt;Nachname&gt; größer ist als 30 Zeichen, dann wird der Vorname nach 9 Zeichen abgeschnitten und mit '.' beendet.</u>	<u>30</u>
<u>3:mit•Ende•der•Berechtigung: •0x0B</u> <u>&lt;ExpirationDate&gt;</u>	<u>Parameter ExpirationDate als tt.mm.jjjj</u>	<u>10</u>
<u>4:Zugriff•&lt;AuthorizationConfidentiality&gt;</u>	<u>Parameter AuthorizationConfiguration</u> <u>.AuthorizationConfidentiality</u> <u>Anzeige: erweitert, wenn Wert "extended"</u> <u>Anzeige: einfach, wenn Wert "normal"</u> <u>(Anzeige der Vertrauensstufen grobgranular)</u>	<u>nicht relevant</u>
<u>Details•zu•0x0BDokumentenkat</u> <u>orien?•0x0B (Ja=1, •Nein=2)</u>	<u>Das Kartenterminal erwartet die Eingabe folgender Zeichen:</u> <u>"1" : Dialog wird mit Details zu Dokumentenkategorien fortgesetzt.</u> <u>oder</u> <u>"2": Dialog wird ohne Details zu Dokumentenkategorien fortgesetzt.</u>	=

<u>Zugriff auf folgende 0x0BKategorien erlaubt:</u>	=	=
<u>Bitte mit [OK] bestätigen!</u>	=	=
<u>Es folgt eine Auflistung der Dokumentenkategorien aus Parameter DocumentCategoryList. Zur Anzeige wird ein Mapping der übertragenen Enumerated Werte gemäß Tab FM ePA 042 durchgeführt. Bei der Auflistung der Dokumentenkategorien muss das Display des angeschlossenen Kartenterminals für die anzeigbaren Zeichen ohne Panning und ohne Scrolling genutzt werden. Stehen z.B. 5 Zeilen zur Anzeige ohne Scrolling zur Verfügung, dann ist jede Zeile für die Anzeige zu nutzen. Ziel ist, dass der Versicherte ein Minimum an erforderlichen Bestätigungen durch Drücken der Taste "OK" durchführen muss.</u>	<u>Parameter AuthorizationConfiguration.DocumentCategoryList (Anzeige der Dokumentkategorien - mittelgranulare Berechtigung)</u>	<u>max. 48 Zeichen pro Zeile (weniger bei Panning)</u>

#### Hinweise:

1. Die Inhalte der mit '\*' markierten Parameter werden auf die maximal mögliche Anzahl der verbleibenden Zeichen für den Eingabetext gekürzt. Nicht genutzte Zeichen werden nicht zur Anzeige gebracht.
2. Leerzeichen werden als "•" dargestellt
3. 0x0B und 0x0F (Sollbruchstellen bzw. Trennung zwischen Nachricht und PIN-Prompt)

sind Trennzeichen gemäß [SICCT#5.6.1]

4. Die Zeilenumbrüche in der Spalte "Ausgabe am Kartenterminal" sind editorisch bedingt.

**Tabelle 39 : Tab FM ePA 042 - Mapping von DocumentCategoryEnum auf Anzeigetext am Kartenterminal**

<u>DocumentCategoryEnum</u>	<u>Anzeigetext am Kartenterminal</u>
<u>category_treatment_medical</u>	<u>Arzt</u>
<u>category_treatment_dental</u>	<u>Zahnarzt</u>
<u>category_treatment_psych</u>	<u>Psychotherapie</u>
<u>category_treatment_other</u>	<u>Andere Fachgebiete</u>
<u>category_emp</u>	<u>Medikationsplan</u>
<u>category_nfd</u>	<u>Notfalldaten</u>
<u>category_eab</u>	<u>Arztbrief</u>
<u>category_dentalrecord</u>	<u>Zahnbonusheft</u>
<u>category_childsrecord</u>	<u>Kinderuntersuchungsheft</u>
<u>category_mothersrecord</u>	<u>Mutterpass</u>
<u>category_vaccination</u>	<u>Impfpass</u>
<u>category_patientdoc</u>	<u>Von mir eingestellte Daten</u>
<u>category_ega</u>	<u>eGA-Daten</u>
<u>category_receipt</u>	<u>Quittungen</u>
<u>category_prescription</u>	<u>Rezept</u>

[<=]

Die folgenden Beispiele sollen veranschaulichen, wie die Anzeige am Kartenterminal und die Eingabe des Versicherten bei der Operation RequestFacilityAuthorization Version 2 erfolgt.

**Tabelle 40 : Tab FM ePA 043 - Beispiel Anzeige am Kartenterminal der Operation RequestFacilityAuthorization Version 2 ohne Dokumentkategorien**

<u>Anzeige am Kartenterminal</u>	<u>Eingabe des Versicherten</u>
----------------------------------	---------------------------------

Es folgen 4 Anzeigen. Bitte mit [OK] bestätigen!	<u>Taste: OK</u>
<u>1:Berechtigung für Praxis Dr. Müller</u>	<u>Taste: OK</u>
<u>2:auf Akte von Max Mustermann</u>	<u>Taste: OK</u>
<u>3:mit Ende der Berechtigung: 01.08.2021</u>	<u>Taste: OK</u>
<u>4:Zugriff erweitert</u>	<u>Taste: OK</u>
<u>Details zu Dokumentenkategorien? (Ja=1, Nein=2)</u>	<u>Taste: 2</u>
<u>PIN für Aktenzugriff</u> <u>PIN.eGK:</u>	<u>PIN-Eingabe: 123456</u>

Im Beispiel erteilt Max Mustermann der Praxis Dr. Müller bis 01.08.2021 die Berechtigung, auf normale und vertrauliche deklarierten Dokumente der Akte des Versicherten Max Mustermann zuzugreifen. Im Dialog am Kartenterminal entscheidet sich Max Mustermann dafür, die Dokumentenkategorien, die nach Rücksprache in der Praxis vereinbart wurden, nicht am Kartenterminal anzeigen zu lassen.

**Tabelle 41 : Tab FM ePA 043 - Beispiel Anzeige am Kartenterminal der Operation RequestFacilityAuthorization Version 2 mit Dokumentenkategorien**

<u>Anzeige am Kartenterminal</u>	<u>Eingabe des Versicherten</u>
Es folgen 4 Anzeigen. Bitte mit [OK] bestätigen!	<u>Taste: OK</u>
<u>1:Berechtigung für Praxis Dr. Müller</u>	<u>Taste: OK</u>
<u>2:auf Akte von Max Mustermann</u>	<u>Taste: OK</u>
<u>3:mit Ende der Berechtigung: 01.08.2021</u>	<u>Taste: OK</u>
<u>4:Zugriff einfach</u>	<u>Taste: OK</u>
<u>Details zu Dokumentenkategorien? (Ja=1, Nein=2)</u>	<u>Taste: 1</u>
<u>Zugriff auf folgende Kategorien erlaubt:</u>	<u>Taste: OK</u>
<u>Bitte mit [OK] bestätigen!</u>	<u>Taste: OK</u>
<u>Arzt</u>	<u>Taste: OK</u>
<u>Medikationsplan</u>	<u>Taste: OK</u>



<a href="#">Notfalldaten</a>	<a href="#">Taste: OK</a>
<a href="#">Arztbrief</a>	<a href="#">Taste: OK</a>
<a href="#">Impfpass</a>	<a href="#">Taste: OK</a>
<a href="#">PIN für Schritt 5: Aktenzugriff</a> <a href="#">PIN.eGK:</a>	<a href="#">PIN-Eingabe: 123456</a>

Im Beispiel erteilt Max Mustermann der Praxis Dr. Müller (Allgemeinmedizin) bis 01.08.2021 die Berechtigung, auf normale deklarierte Dokumente der Akte des Versicherten Max Mustermann zuzugreifen. Im Dialog am Kartenterminal entscheidet sich Max Mustermann dafür, die Dokumentenkategorien, die nach Rücksprache in der Praxis vereinbart wurden, am Kartenterminal anzeigen zu lassen. Auf Wunsch des Versicherten wurden die Dokumentenkategorien eingeschränkt. Am Kartenterminal werden nur die Dokumentenkategorien angezeigt, die in `AuthorizationConfiguration.DocumentCategoryList` vom Primärsystem übergeben wurden.

#### **A\_16351 - FM ePA: RequestFacilityAuthorization - Anzeige am Kartenterminal - Mapping von InsurantName und OrganizationName**

Die Operation `RequestFacilityAuthorization` MUSS bei der Anzeige von Vorname, Nachname (Parameter `InsurantName`) und `OrganizationName` jedes Zeichen auf ein entsprechendes Zeichen des vom verwendeten Kartenterminal adressierten Zeichensatzes abbilden.

[<=]

#### **A\_16352 - FM ePA: RequestFacilityAuthorization - Anzeige am Kartenterminal - nicht darstellbare Zeichen von InsurantName und OrganizationName**

Falls in Vorname oder Nachname oder `OrganizationName` enthaltene Zeichen nicht auf den vom Kartenterminal unterstützten Zeichensatz abbildbar sind KANN die Operation `RequestFacilityAuthorization` für jedes nicht abbildbare Zeichen ein Zeichen des vom verwendeten Kartenterminal adressierten Zeichensatzes als Platzhalter auf dem Display des Kartenterminals anzeigen.

[<=]

Im einfachsten Fall ist das vom Primärsystem übergebene Zeichen am Kartenterminal anzeigbar, z.B. das Zeichen 'a'. Für nicht abbildbare Zeichen gibt es verschiedene Möglichkeiten. Das Zeichen kann beispielsweise weggelassen werden oder durch ein festes Zeichen als Platzhalter ersetzt werden oder es gibt eine geeignete Abbildung auf ein lesbares Zeichen. Eine geeignete Abbildung für Buchstaben mit diakritischen Zeichen (z.B. 'ñ') ist die Darstellung des Buchstabens ohne das diakritische Zeichen ('n') auf dem Display des Kartenterminals.

Über TUC\_KON\_058 „Displaygröße ermitteln“ gemäß [gemSpec\_Kon] kann das Fachmodul ePA die Größe des durch das Kartenterminal verwendeten Displays abfragen und die Darstellung der Berechtigungen optimieren.

#### **A\_16219 - FM ePA: RequestFacilityAuthorization - Anzeige am Kartenterminal - Optimierung**

Falls ein Kartenterminal die Mindestanforderung von 48 Zeichen Anzeigetext übersteigt, MUSS die Operation `RequestFacilityAuthorization` die Anzeigen gemäß `Tab_FM_ePA_025` bündeln. Hierbei ist das Zusammenfassen von 2 oder mehr Zeilen von `Tab_FM_ePA_025`

2255 zu einer Ausgabeoperation gemeint. Die Nummerierung zu Beginn der Anzeige mit "1:"  
2256 bis "4:" wird dann angepasst und erfolgt fortlaufend bei "1:" beginnend. Der Ausgabertext  
2257 "Es folgen 4 Anzeigen ..." wird entsprechend angepasst. Der Parameter "Anw" für  
2258 Terminalanzeigen gemäß Tab\_FM\_ePA\_019 wird entsprechend angepasst.

2259  
2260 [**<=**]

2261 **A\_16218 - FM ePA: RequestFacilityAuthorization - Anzeige am Kartenterminal -**  
2262 **Nutzerinteraktion**

2263 Die Operation RequestFacilityAuthorization MUSS eine Ausgabe (entspricht einer Zeile in  
2264 Tab\_FM\_ePA\_025) am Kartenterminal solange anzeigen bis eine Nutzereingabe die  
2265 Anzeige bestätigt, abbricht oder ein Timeout wegen fehlender Nutzereingabe erfolgt.  
2266 [**<=**]

2267 **A\_16214 - FM ePA: RequestFacilityAuthorization - Anzeige am Kartenterminal -**  
2268 **Bestätigung**

2269 Falls eine Ausgabe (entspricht einer Zeile in Tab\_FM\_ePA\_025) am Kartenterminal  
2270 bestätigt wird, MUSS die Operation RequestFacilityAuthorization die nächste Ausgabe am  
2271 Kartenterminal gemäß Tab\_FM\_ePA\_025 anzeigen.  
2272 [**<=**]

2273 **A\_16215 - FM ePA: RequestFacilityAuthorization - Anzeige am Kartenterminal -**  
2274 **Abbruch**

2275 Falls eine Ausgabe Tab\_FM\_ePA\_025 am Kartenterminal abgebrochen wird (Abbruchtaste  
2276 wurde gedrückt oder Timeout), MUSS die Operation RequestFacilityAuthorization die  
2277 Operation mit Code 7217 abbrechen.  
2278 [**<=**]

2279 **A\_18182-01A\_18182 - FM ePA: RequestFacilityAuthorization - Anzeige am**  
2280 **Kartenterminal - wiederholte PIN-Eingabe**

2281 Falls eine erfolgte PIN-Eingabe den Fehler REJECTED zurückliefert, MUSS die Operation  
2282 RequestFacilityAuthorization unmittelbar daran anschließend eine erneute PIN-Abfrage  
2283 gemäß A\_14769 und A\_16216-01 durchführen, d.h. die Schritte 1-4 zur Anzeige am  
2284 Kartenterminal werden hierbei nicht durchgeführt. [**<=**]

2285 **Login am ePA-Aktensystem (Authentisierung und Autorisierung)**

2286 Die Authentisierung gegenüber einem Aktensystem erfolgt gemäß A\_15192 mit der eGK.  
2287 Der vollständige Login-Prozess ist in Kapitel 6.5 Login beschrieben. Dabei ist es  
2288 unerheblich, ob es sich um den Versicherten als Eigentümer der Akte handelt oder ob der  
2289 Versicherte in der Rolle des Vertreters agiert. In beiden Fällen wird für den Versicherten  
2290 die Authentisierung und Autorisierung mit seiner eGK durchgeführt.

2291 **Verbindung zur Dokumentenverwaltung**

2292 Die Verbindung zur Komponente Dokumentenverwaltung verläuft analog zum Login  
2293 durch eine LEI mit dem Aufruf von Operationen des Webservices PHRService. Die  
2294 Operation RequestFacilityAuthorization möchte mit der Komponente  
2295 Dokumentenverwaltung kommunizieren und baut hierzu eine sichere Verbindung gemäß  
2296 den Festlegungen in Kapitel 6.5.5 auf.

2297 **Kontoaktivierung falls erforderlich**

2298 Bevor die Berechtigung für die Telematik-ID in der Komponente Autorisierung hinterlegt  
2299 wird, wird für den Fall, dass das Aktenkonto noch nicht aktiviert wurde, die Operation  
2300 ActivateAccount implizit aufgerufen und vollständig abgearbeitet.

**A\_17213 - FM ePA: Bedingte Kontoaktivierung - Aufruf der Operation  
ActivateAccount**

Falls das Aktenkonto noch nicht aktiviert, wurde MUSS die Operation  
RequestFacilityAuthorization die Operation ActivateAccount implizit aufrufen.  
[<=]

Bei der Kontoaktivierung wird die Zustimmung des Versicherten durch PIN-Eingabe  
verlangt. Es werden Events definiert und zu Beginn und Ende der impliziten  
Kontoaktivierung erzeugt. Das Primärsystem erhält dadurch die Möglichkeit, den  
Versicherten auf die zusätzliche Kontoaktivierung hinzuweisen.

**A\_17214 - FM ePA: Bedingte Kontoaktivierung - Event  
FM\_EPA/ACTIVATE\_ACCOUNT/START**

Falls die Kontoaktivierung erforderlich ist, MUSS die Operation  
RequestFacilityAuthorization zu Beginn der Kontoaktivierung unter Verwendung des  
Systeminformationsdienstes des Konnektors ein Event mit folgendem Inhalt erzeugen:

Parameter	Inhalt
Topic	FM_EPA/ACTIVATE_ACCOUNT/START
Type	Operation
Severity	Info
RecordID	[RecordIdentifier der Aktensession]

[<=]

**A\_17215 - FM ePA: Bedingte Kontoaktivierung - Event  
FM\_EPA/ACTIVATE\_ACCOUNT/FINISHED**

Falls die Kontoaktivierung erforderlich ist, MUSS die Operation  
RequestFacilityAuthorization nach Abschluss der Kontoaktivierung unter Verwendung des  
Systeminformationsdienstes des Konnektors ein Event mit folgendem Inhalt erzeugen:

Parameter	Inhalt
Topic	FM_EPA/ACTIVATE_ACCOUNT/FINISHED
Type	Operation
Severity	Info
RecordID	[RecordIdentifier der Aktensession]

[<=]

**Berechtigung in Komponente Autorisierung für Telematik-ID erstellen**

Durch den Login (Authentisierung und Autorisierung) liegt in der Session zur Operation  
RequestFacilityAuthorization der Aktenschlüssel und der Kontextschlüssel im Klartext vor.

2328 Beide Schlüssel werden mit AES-Schlüsseln, die von SGD 1 und 2 abgerufen werden,  
 2329 verschlüsselt und mittels `I_Authorization_Management::putAuthorizationKey` in die  
 2330 Komponente Autorisierung eingebracht.

### 2331 **A\_17988 - FM ePA: RequestFacilityAuthorization - Schlüsselableitung in** 2332 **Abhängigkeit von der Rolle**

2333 Für die Verschlüsselung von Akten- und Kontextschlüssel MUSS das Fachmodul ePA bei  
 2334 Durchführung der Schlüsselableitung die Rolle des Berechtigenden bestimmen und die  
 2335 Operation `KeyDerivation` gemäß Anwendungsfall folgender Tabelle aufrufen:  
 2336

login	Rolle des Berechtigenden	umzusetzender Anwendungsfall aus gemSpec_SGD_ePA
eGK	Versicherter (als Akteninhaber): unveränderlicher Teil der KVNR aus Zertifikat C.AUT der eGK entspricht KVNR aus Parameter RecordIdentifier der aufrufenden Operation	<a href="#">gemSpec_SGD_ePA#2.6</a>
eGK	Vertreter: unveränderlicher Teil der KVNR aus Zertifikat C.AUT der eGK entspricht nicht KVNR aus Parameter RecordIdentifier der aufrufenden Operation	<a href="#">gemSpec_SGD_ePA#2.8</a>

2337  
 2338 [`<=`]

### 2339 **A\_17868 - FM ePA: RequestFacilityAuthorization - Akten- und Kontextschlüssel** 2340 **mit eGK verschlüsseln**

2341 Die Operation `RequestFacilityAuthorization` MUSS die beiden zur Verschlüsselung  
 2342 notwendigen AES-Schlüssel abrufen und Akten- und Kontextschlüssel gemäß  
 2343 [`gemSpec_Krypt#A_17872`] und [`gemSpec_SGD_ePA#8`] verschlüsseln.  
 2344 [`<=`]

### 2345 **A\_14829 - FM ePA: RequestFacilityAuthorization - Hinterlegen des** 2346 **verschlüsselten Schlüsselmaterials in der Komponente Autorisierung**

2347 Die Operation `RequestFacilityAuthorization` MUSS zur Hinterlegung der Berechtigung in  
 2348 der Komponente Autorisierung die Operation  
 2349 `I_Authorization_Management::putAuthorizationKey` mit folgenden Parametern aufrufen:

- 2350 • `AuthenticationAssertion`: als SOAP-Header, `AuthenticationToken` aus dem Login-  
 2351 Prozess zum ePA-Aktensystem
- 2352 • `RecordIdentifier`: Parameter der aufrufenden Operation
- 2353 • `AuthorizationKey`: `AuthorizationKey`: Berechtigung der Telematik-ID; enthält  
 2354 doppelt verschlüsseltes Chifftrat und `AssociatedData` (aus den Antwortnachrichten  
 2355 der SGDs) als `EncryptedKeyContainer` gemäß [`gemSpec_SGD_ePA#8`]
- 2356 • `validTo`: vom Primärsystem übergebenes Gültigkeitsdatum bis wann die  
 2357 Zugriffsberechtigung erteilt wird
- 2358 • `actorID`: Telematik-ID des zum Aufrufkontext ausgewählten SM-B
- 2359 • `AuthorizationType`: `DOCUMENT_AUTHORIZATION`

2360 [`<=`]

2361 Der `RecordIdentifier` wird aus den Aufrufparametern von `RequestFacilityAuthorization`  
 2362 übernommen, die `AuthenticationAssertion` wurde beim Login über die Komponente  
 2363 Zugangsgateway für Versicherte erzeugt.

#### 2364 **Berechtigung der LEI in die Dokumentenverwaltung einbringen**

2365 Das Fachmodul erstellt im Kontext der Operation `RequestFacilityAuthorization` ein Policy  
 2366 Document, sendet dieses an die Komponente Dokumentenverwaltung wodurch die  
 2367 Berechtigung für die LEI in der Dokumentenverwaltung hinterlegt wird.

2368 Die Nutzungsvorgaben für XDS-Metadaten bei Policy Documents sind  
 2369 in [gemSpec\_DM\_ePA#2.1.4.2] beschrieben.

2370 Die Nutzungsvorgaben zum Inhalt eines Policy Documents zur Berechtigung einer  
 2371 Leistungserbringerinstitution werden durch die Anforderung [A\\_15442](#) in  
 2372 [gemSpec\_Dokumentenverwaltung] geregelt.

#### 2373 **A\_15693 - FM ePA: RequestFacilityAuthorization - Erstellung von Policy** 2374 **Document**

2375 Die Operation `RequestFacilityAuthorization` MUSS ein Policy Document als eine XACML  
 2376 2.0 Policy konform zu Advanced Patient Privacy Consent gemäß [IHE-ITI-APPC] unter  
 2377 Berücksichtigung der Anforderungen an deren Inhalt in  
 2378 [gemSpec\_Dokumentenverwaltung#Tab\_Dokv\_300 in Anhang B (Base Policy)] erstellen  
 2379 und die Werte unter Berücksichtigung von `Tab_FM_ePA_023` belegen:  
 2380

2381 **Tabelle 42: Tab\_FM\_ePA\_023 Base Policy Belegung**

Element-, Attribut- oder Textknoten gemäß [XACML] von Base Policy	Wert
/PolicySet/Target/Subjects/Subject[1]/Subject Match/ AttributeValue/InstanceIdentifier/@extension	Telematik-ID des zum Aufrufkontext ausgewählten SM-B
/PolicySet/Target/Subjects/Subject[2]/Subject Match/ AttributeValue/text()	Inhalt des Aufrufparameters AuthorizationConfiguration / OrganizationName
/PolicySet/Target/Resources/Resource/ResourceMatch/ AttributeValue/InstanceIdentifier/@extension	KVNR der zum Login benutzen eGK
/PolicySet/Target/Environments/Environment/ EnvironmentMatch[2]/AttributeValue/text()	Inhalt von Aufrufparameter AuthorizationConfiguration / ExpirationDate entsprechend der Bildungsvorschrift aus <code>Tab_Dokv_300</code>
/PolicySet/ ...	Es werden je nach Berechtigung zwischen 1 und 3 Elementen <code>PolicySetIdReference</code> unter dem Element <code>PolicySet</code> eingefügt, d.h., falls ein Flag im Aufrufparameter <code>AuthorizationConfigu</code>

	ration gesetzt ist, wird ein Element mit dem Text (Policy Set ID) erstellt.	
	<b>Flag</b>	<b>Text (Policy Set ID)</b>
	Vers_Docs	urn:gematik:policy-set-id:permissions-access-group-hcp-insurant-documents
	LE_Docs	urn:gematik:policy-set-id:permissions-access-group-hcp
	KTR_Docs	urn:gematik:policy-set-id:permissions-access-group-hcp-insurance-documents

[<=]

#### **A 15693-01 - FM ePA: RequestFacilityAuthorization Version 2.x - Erstellung von Policy Document**

Die Operation RequestFacilityAuthorization Version 2.x MUSS ein Policy Document als eine XACML 2.0 Policy konform zu Advanced Patient Privacy Consent gemäß [IHE-ITI-APPC] unter Berücksichtigung der Anforderungen an deren Inhalt in [gemSpec Dokumentenverwaltung#Tab Dokv 502] erstellen und die Werte unter Berücksichtigung von Tab FM ePA 023 belegen:

**Tabelle 43: Tab FM ePA 023 Base Policy Belegung**

<b><u>Element-, Attribut- oder Textknoten gemäß [XACML] von Base Policy</u></b>	<b><u>Wert</u></b>
<u>/PolicySet/Target/Subjects/Subject[1]/Subject Match/Attribute/InstanceIdentifier/@extension</u>	<u>Telematik-ID des zum Aufrufkontext ausgewählten SM-B</u>
<u>/PolicySet/Target/Subjects/Subject[2]/Subject Match/Attribute/text()</u>	<u>Inhalt des Aufrufparameters AuthorizationConfiguration / OrganizationName</u>
<u>/PolicySet/Target/Resources/Resource/ResourceMatch/Attribute/InstanceIdentifier/@extension</u>	<u>KVNR der zum Login benutzten eGK</u>
<u>/PolicySet/Target/Environments/Environment/EnvironmentMatch[2]/Attribute/text()</u>	<u>Inhalt von Aufrufparameter AuthorizationConfiguration / ExpirationDate entsprechend der Bildungsvorschrift aus Tab Dokv 300</u>



<a href="#">/PolicySet/Policy[1]/Rule/Resources/Resource[1]/ResourceMatch/AttributeValue/CodedValue/@displayName</a>	<a href="#">grobgranulare Berechtigung: Wenn das Element AuthorizationConfidentiality der Operation RequestFacilityAuthorization den Wert "normal" oder "extended", dann setze Wert auf "normal".</a>
<a href="#">/PolicySet/Policy[1]/Rule/Resources/Resource[2]/ResourceMatch/AttributeValue/CodedValue/@displayName</a>	<a href="#">grobgranulare Berechtigung: Wenn AuthorizationConfidentiality= "extended", dann setze Wert auf "extended".</a>
<a href="#">/PolicySet/Policy[2]/...</a>	<a href="#">mittelgranulare Berechtigung: Es wird für jede in Element DocumentCategoryList der Operation RequestFacilityAuthorization übergebene Dokumentenkategorie ein Rule-Element gemäß [gemSpec_Dokumentenverwaltung#Tab_Dokv_502] angelegt und korrespondierend zur Dokumentenkategorie befüllt.</a>

[&lt;=]

### **A\_14833 - FM ePA: RequestFacilityAuthorization - Ablage der Policy-Dokumente in der Dokumentenverwaltung**

Die Operation RequestFacilityAuthorization MUSS das Policy-Dokument und seine Metadaten mit der IHE Transaktion [ITI-80] "Cross-Gateway Document Provide" gemäß [gemSpec\_Dokumentenverwaltung] für die durch RecordIdentifier adressierte Akte in der Komponente Dokumentenverwaltung hinterlegen. [<=]

### **A\_17437 - FM ePA: RequestFacilityAuthorization - SOAP-Security-Header**

Vor der Ablage des Policy-Dokuments im ePA-Aktensystem MUSS die Operation RequestFacilityAuthorization den SOAP Security Header mit der AuthenticationAssertion der zur Authentisierung verwendeten eGK belegen.

[&lt;=]

### **A\_14834 - FM ePA: RequestFacilityAuthorization - Berechtigungen in Dokumentenverwaltung einbringen - Fehler im Aktensystem**

Falls bei der Einbringung des Policy-Dokuments in die Komponente Dokumentenverwaltung ein IHE-Fehler auftritt, MUSS der Webservice PHRManagementService die aufgerufene Operation mit dem Code 7215 gemäß Tab\_FM\_ePA\_011 abbrechen.

[&lt;=]

### **A\_17120 - FM ePA: RequestFacilityAuthorization - Berechtigungen in Dokumentenverwaltung einbringen - Fehler**

Falls bei der Einbringung des Policy-Dokuments in die Komponente Dokumentenverwaltung ein Fehler außerhalb der IHE-Spezifikation auftritt, MUSS der Webservice PHRManagementService die aufgerufene Operation mit dem Code 7400 gemäß Tab\_FM\_ePA\_011 abbrechen.



2418  
2419 [ $\leq$ ]

2420 Bei erfolgreicher Durchführung der Operation RequestFacilityAuthorization wurde die  
2421 Berechtigung für die LEI im Aktensystem hinterlegt. Ein Akteur der LEI kann jetzt durch  
2422 Operationen von PHRService auf Dokumente des Versicherten im Aktensystem zugreifen  
2423 das Login mit SM-B erfolgen.

### 2424 7.2.2.3 GetHomeCommunityID

2425 Der Namensdienst der TI enthält für jedes ePA-Aktensystem die IP-Adressen der  
2426 einzelnen Komponenten und die HomeCommunityID als fachlichen Identifier.  
2427 GetHomeCommunityID iteriert über alle Einträge und liefert dann die HomeCommunityID  
2428 des ePA-Aktensystems zurück, welches die Akte zu der übergebenen Versicherten-ID  
2429 führt. Als Fehler der Operation werden die Fälle abgefangen, dass kein oder mehr als ein  
2430 passendes ePA-Aktensystem gefunden wird. Liefert der Aufruf von  
2431 I\_Authorization\_Management::checkRecordExists den Statuswert UNKNOWN zurück, geht  
2432 die Operation GetHomeCommunityID davon aus, dass das ePA-Aktensystem keine  
2433 Patientenakte zu der übertragenen Versicherten-ID führt. Der Fehlerfall, dass die  
2434 Lokalisierungsinformationen zum Zeitpunkt des Aufrufs von GetHomeCommunityID nicht  
2435 zur Verfügung stehen, wird in Kapitel 6.3 behandelt.

### 2436 Aufbau einer TLS-Verbindung zur Komponente Autorisierung eines ePA- 2437 Aktensystems

2438 Gemäß A\_14105 muss zur Kommunikation mit der Komponente Autorisierung eines ePA-  
2439 Aktensystems eine TLS-Verbindung mit serverseitiger Authentisierung aufgebaut werden.

2440

### 2441 Abfrage der ePA-Aktensysteme

#### 2442 A\_15228 - FM ePA: GetHomeCommunityID - Anfrage an alle bekannten ePA- 2443 Aktensysteme

2444 Die Operation GetHomeCommunityID MUSS die Existenz eines zur Versicherten-ID  
2445 passenden Aktenkontos bei den im Namensdienst der TI gelisteten ePA-Aktensystemen  
2446 anfragen.

2447 [ $\leq$ ]

2448 Da ein Versicherter höchstens ein Aktenkonto bei genau einem ePA-Aktensystem hat,  
2449 kann Fachmodul ePA die Operation GetHomeCommunityID erfolgreich beenden, sobald  
2450 das entsprechende ePA-Aktensystem gefunden wurde.

#### 2451 A\_14586 - FM ePA: GetHomeCommunityID - Schnittstelle zur Abfrage am ePA- 2452 Aktensystem

2453 Die Operation GetHomeCommunityID MUSS die Existenz eines Aktenkontos in einem  
2454 ePA-Aktensystem mit I\_Authorization\_Management::checkRecordExists der Komponente  
2455 Autorisierung abfragen. [ $\leq$ ]

2456

#### 2457 A\_13786 - FM ePA: GetHomeCommunityID - Eine Akte

2458 Falls ein ePA-Aktensystem bestimmt werden konnte, dass zu der Versicherten-ID eine  
2459 Akte mit einem Status aus der Menge (ACTIVATED, REGISTERED, DISMISSED,  
2460 SUSPENDED) führt, MUSS die Operation GetHomeCommunityID die HomeCommunityID  
2461 dieses ePA-Aktensystems zurückgeben.

2462  
2463 [ $\leq$ ]

2464 Falls mindestens ein ePA-Aktensystem erreichbar ist und einen Statuswert zurückliefert,  
2465 wird bei fehlgeschlagenen Aufrufen anderer ePA-Aktensysteme angenommen, dass diese  
2466 kein passendes Aktenkonto zur der Versicherten-ID führen.

#### 2467 **Fehlerbehandlung**

##### 2468 **A\_17765 - FM ePA: GetHomeCommunityID - Abfrage eines Aktenkontos nicht möglich**

2469 Falls ein Aufruf von I\_Authorization\_Management::checkRecordExists nicht durchgeführt  
2470 werden konnte oder nicht erfolgreich war, MUSS die Operation GetHomeCommunityID  
2471 die Lokalisierung des ePA-Aktenkontos weiterführen.

2472  
2473  
2474 [**<=**]

##### 2475 **A\_13784 - FM ePA: GetHomeCommunityID - Keine Akte - Fehler**

2476 Falls kein ePA-Aktensystem bestimmt werden konnte, das zu einer Versicherten-ID eine  
2477 Akte mit einem Status aus der Menge (ACTIVATED, REGISTERED, DISMISSED,  
2478 SUSPENDED) führt, MUSS die Operation GetHomeCommunityID mit dem Code 7290  
2479 gemäß Tab\_FM\_ePA\_032 abbrechen.

2480  
2481 [**<=**]

##### 2482 **A\_13785 - FM ePA: GetHomeCommunityID - Zwei oder mehr Akten - Fehler**

2483 Falls mehr als ein ePA-Aktensystem bestimmt werden konnte, das zu einer Versicherten-  
2484 ID eine Akte mit einem Status aus der Menge (ACTIVATED, REGISTERED, DISMISSED,  
2485 SUSPENDED) führt, MUSS die Operation GetHomeCommunityID mit dem Code 7291  
2486 gemäß Tab\_FM\_ePA\_032 abbrechen.

2487  
2488 [**<=**]

#### 2489 **7.2.2.4 GetAuthorizationList**

##### 2490 **Auswahl eines SM-B**

2491 Das Fachmodul ePA sucht ein SM-B aus dem fest konfigurierten Informationsmodell des  
2492 Konnektors, das dem übertragenen Context zugeordnet ist und zuvor durch PIN-Eingabe  
2493 freigeschaltet wurde (siehe [A\\_15218](#)). Die Berechtigungen werden für die Telematik-ID  
2494 des ausgewählten SM-B ermittelt.

##### 2495 **Aufbau einer TLS-Verbindung zur Komponente Autorisierung eines ePA-Aktensystems**

2496  
2497 Gemäß [A\\_14105](#) muss zur Kommunikation mit der Komponente Autorisierung eines ePA-  
2498 Aktensystems eine TLS-Verbindung mit serverseitiger Authentisierung aufgebaut werden.

##### 2499 **Abfrage der ePA-Aktensysteme**

##### 2500 **A\_17167 - FM ePA: GetAuthorizationList - Anfrage an alle bekannten ePA-Aktensysteme**

2501 Die Operation GetAuthorizationList MUSS die zum Zugriff durch eine LEI berechtigten  
2502 Aktenkonten bei allen im Namensdienst der TI gelisteten ePA-Aktensystemen anfragen.  
2503  
2504 [**<=**]

##### 2505 **Login an den ePA-Aktensystemen (nur Authentisierung)**

2506 Der Abruf der Berechtigungen erfordert die Authentisierung gegenüber den ePA-  
2507 Aktensystemen ([A\\_15193](#)). Der Ablauf verläuft jeweils analog zum Login bei Aufruf einer  
2508 Operation des Webservices PHRService. Eine Autorisierung und Verbindung zur  
2509 Komponente Dokumentenverwaltung ist nicht notwendig.

##### 2510 **Abfrage der Berechtigungen an den ePA-Aktensystemen**

Zur Ermittlung der Berechtigungen wird an allen im Namensdienst der TI gelisteten ePA-Aktensystemen die Operation `I_Authorization_Management::getAuthorizationList` der jeweiligen Komponente Autorisierung aufgerufen. Die Operation `I_Authorization_Management::getAuthorizationList` liefert eine Liste von KVNRS, für die im Schlüsselkasten ein `AuthorizationKey` hinterlegt ist, der die zur übergebenen `AuthenticationAssertion` gehörende LEI zum Zugriff berechtigt sowie das Enddatum der Zugriffsberechtigung. Die KVNRS werden in vollständige `RecordIdentifier` transformiert und als Liste, zusammen mit dem jeweiligen Enddatum der Berechtigung, an das aufrufende Clientsystem übergeben. Ein Fehler der Operation `I_Authorization_Management::getAuthorizationList` führt nicht zum Abbruch der Operation `GetAuthorizationList`, sondern lediglich zu einer Warnung. Falls alle Aufrufe von `I_Authorization_Management::getAuthorizationList` zu einem Fehler führen, wird die Operation `GetAuthorizationList` mit einem Fehler abgebrochen.

#### 2524 **A\_17174 - FM ePA: GetAuthorizationList - Abfrage berechtigter Aktenkonten**

Die Operation `GetAuthorizationList` MUSS zur Abfrage der zum Zugriff durch eine LEI berechtigten Aktenkonten an einem ePA-Aktensystem die Operation `I_Authorization_Management::getAuthorizationList` mit folgenden Parametern aufrufen:

- `AuthenticationAssertion`: als SOAP-Header, `AuthenticationToken` aus dem Login-Prozess zum ePA-Aktensystem (nur Authentisierung)

2530  
2531 [`<=`]

#### 2532 **A\_19009 - GetAuthorizationList - Häufigkeit der Abfrage berechtigter Aktenkonten - Fehler**

Falls einer der zur Durchführung der Operation benötigten Aufrufe von `I_Authorization_Management::getAuthorizationList` den Fehler `TOO_MANY_REQUESTS` zurückgibt, MUSS das Fachmodul ePA die aufgerufene Operation mit dem Code 7231 gemäß `Tab_FM_ePA_041` Fehlermeldungen der Operation `GetAuthorizationList` abbrechen. [`<=`]

#### 2539 **Fehlerbehandlung**

Die Operation `GetAuthorizationList` muss alle bekannten ePA-Aktensysteme anfragen, die jeweils mit verschiedenen Fehlern antworten können. Das Fachmodul zeigt mit dem Fehlercode 7215 eindeutig ein Problem auf Seite der Aktensysteme an, Fehlercode 7400 hingegen deutet auf ein Problem im Konnektor hin, bedarf aber einer genaueren Analyse der Log-Dateien.

2545

#### 2546 **A\_17767 - FM ePA: GetAuthorizationList - Abfrage der Berechtigung einer einzelnen Akte nicht möglich**

Falls ein Aufruf von `I_Authorization_Management::getAuthorizationList` nicht durchgeführt werden konnte oder nicht erfolgreich war, MUSS die Operation `GetAuthorizationList` die Abfrage der Berechtigungen für die anderen Aktenkonten weiterführen.

2552  
2553 [`<=`]

#### 2554 **A\_17219 - FM ePA: GetAuthorizationList - Abfrage berechtigter Aktenkonten - Warnung**

Falls mindestens ein Aufruf von `I_Authorization_Management::getAuthorizationList` erfolgreich und mindestens ein Aufruf nicht durchgeführt werden konnte oder fehlerhaft war, MUSS die Operation `GetAuthorizationList` eine Warnung mit dem Code 7230 gemäß `Tab_FM_ePA_041` zurückgeben.

2560 [`<=`]

2561 **A\_17175 - FM ePA: GetAuthorizationList - Abfrage berechtigter Aktenkonten -**  
 2562 **Fehler**  
 2563 Falls alle zur Durchführung einer Operation benötigten Aufrufe von  
 2564 I\_Authorization\_Management::getAuthorizationList einen Fehler zurückgeben, MUSS das  
 2565 Fachmodul ePA die aufgerufene Operation mit dem Code 7400 gemäß Tab\_FM\_ePA\_011  
 2566 abbrechen.  
 2567 [**<=**]

2568 Sind für eine LEI keine Berechtigungen vorhanden, gibt die Operation  
 2569 GetAuthorizationList eine leere Liste in dem Rückgabeparameter AuthorizationList zurück.

2570 **Transformation KVNR nach RecordIdentifier**

2571 **A\_17177 - FM ePA: GetAuthorizationList - Erstellung der RecordIdentifier**  
 2572 Die Operation GetAuthorizationList MUSS aus jeder über  
 2573 I\_Authorization\_Management::getAuthorizationList erhaltenen KVNR einen vollständigen  
 2574 RecordIdentifier gemäß [gemSpec\_DM\_ePA] bilden.  
 2575 [**<=**]

2577

## 8 Anhang A – Verzeichnisse

### 8.1 Abkürzungen

Kürzel	Erläuterung
APPC	Advanced Patient Privacy Consents
ATNA	Audit Trail and Node Authentication Profile
BPPC	Basic Patient Privacy Consents
CDA	Clinical Document Architecture
HL7	Health Level Seven
IHE	Integrating the Healthcare Enterprise
IHE ITI TF	IHE IT Infrastructure Technical Framework
PHR	Personal Health Record
SAML	Security Assertion Markup Language
SGD	Schlüsselgenerierungsdienst
VAU	Vertrauenswürdige Ausführungsumgebung
WS-I	Web Services Interoperability Organization
XCA	Cross-Community Access Profile
XDR	Cross-Enterprise Document Reliable Interchange Profile
XDS	Cross-Enterprise Document Sharing Profile
XCDR	Cross-Community Document Reliable Interchange Profile
XACML	eXtensible Access Control Markup Language
XUA	Cross-Enterprise User Assertion Profile

2579

2580 **8.2 Glossar**

Begriff	Erläuterung
Anbieter-ID	siehe HomeCommunityID
AuthenticationAssertion	Authentifizierungsbestätigung, die entweder LEI oder Versicherten identifiziert. Im Falle der LEI stellt das Fachmodul ePA die AuthenticationAssertion aus, im Falle des Versicherten die Komponente Zugangsgateway für Versicherte des ePA-Aktensystems.
AuthorizationAssertion	Autorisierungsbestätigung, ausgestellt durch die Komponente Autorisierung, mit der das Fachmodul ePA einen Berechtigten bei der Dokumentenverwaltung autorisieren kann.
Funktionsmerkmal	Der Begriff beschreibt eine Funktion oder auch einzelne, eine logische Einheit bildende Teilfunktionen der TI im Rahmen der funktionalen Zerlegung des Systems.
HomeCommunityID	Eindeutige Kennung für einen Anbieter eines ePA-Aktensystems, Aufbau gemäß [gemSpec_DM_ePA]
RecordIdentifier	Eindeutige Kennung für die Akte eines Versicherten; Aufbau gemäß [gemSpec_DM_ePA]

2581  
 2582  
 2583 Weitere Begriffserklärungen befinden sich in [gemGlossar].

2584 **8.3 Abbildungsverzeichnis**

2585 [Es konnten keine Einträge für ein Abbildungsverzeichnis gefunden werden.]

2586 **8.4 Tabellenverzeichnis**

2587	Tabelle 1: Tab_FM_ePA_008 Konfigurationswerte des Fachmoduls ePA .....	16
2588	Tabelle 2: Tab_FM_ePA_053 Übersicht der Fehlerfälle nach Status des Status eines	
2589	Aktenkontos .....	18
2590	Tabelle 3: Tab_FM_ePA_002 Profile, Akteure und Optionen des Webservices PHRService	
2591	.....	23
2592	Tabelle 4: Tab_FM_ePA_034 Übersicht der Funktionen, die ein SM-B benötigen, mit	
2593	Zuordnung zu den aufrufenden Operationen und ob die SM-B eine Berechtigung zum	
2594	Zugriff haben muss.....	28
2595	Tabelle 5: Tab_FM_ePA_001 Daten zur Kommunikation mit den Komponenten des ePA-	
2596	Aktensystems (abhängig vom Nutzer).....	31

2597	Tabelle 6: Tab_FM_ePA_033 Fehlermeldungen bei der Authentisierung mittels eGK.....	35
2598	Tabelle 7: Tab_FM_ePA_030 Authentifizierungsbestätigung erstellen .....	36
2599	Tabelle 8: Tab_FM_ePA_026 Aufrufparameter der Operation	
2600	I_Authorization::getAuthorizationKey .....	37
2601	Tabelle 9: Tab_FM_ePA_007 Service-Informationen der Services des Fachmoduls ePA ..	46
2602	Tabelle 10: Tab_FM_ePA_014 Parameter des Fehlerprotokolls.....	48
2603	Tabelle 11: Tab_FM_ePA_015 Parameter des Debug-Protokolls .....	49
2604	Tabelle 12: Tab_FM_ePA_022 Parameter des Sicherheitsprotokolls .....	49
2605	Tabelle 13: Tab_FM_ePA_024 Parameter des Performanceprotokolls .....	50
2606	Tabelle 14: Tab_FM_ePA_010 Übergreifende Konfigurationsparameter des Fachmoduls	
2607	ePA .....	50
2608	Tabelle 15: Tab_FM_ePA_011 Übergreifende Fehlermeldungen des Fachmoduls ePA .....	52
2609	Tabelle 16: Tab_FM_ePA_050 Wiederverwendete Fehlermeldungen aus der	
2610	Konnektorspezifikation .....	53
2611	Tabelle 17: Tab_FM_ePA_051 Wiederverwendete Fehlermeldungen aus der	
2612	Übergreifenden Spezifikation Operations und Maintenance .....	54
2613	Tabelle 18: Tab_FM_ePA_004 Schnittstellenübersicht des Fachmoduls ePA .....	55
2614	Tabelle 19: Tab_FM_ePA_005 Beschreibung des Webservices PHRService .....	57
2615	Tabelle 20: Tab_FM_ePA_012 Mapping von gematik Fehlern nach IHE Fehlern .....	59
2616	Tabelle 21: Tab_FM_ePA_006 Beschreibung und Parameter der Operation putDocuments	
2617	.....	60
2618	Tabelle 22: Tab_FM_ePA_013 Beschreibung und Parameter der Operation find	
2619	(Semantik) .....	61
2620	Tabelle 23: Tab_FM_ePA_027 Beschreibung und Parameter der Operation getDocuments	
2621	(Semantik) .....	61
2622	Tabelle 24: Tab_FM_ePA_029 Beschreibung und Parameter der Operation	
2623	removeDocuments (Semantik) .....	62
2624	Tabelle 25: Tab_FM_ePA_031 Beschreibung und Parameter der Operation	
2625	updateDocumentSet (Semantik) .....	63
2626	Tabelle 26: Tab_FM_ePA_003 Beschreibung des Webservices PHRManagementService ..	70
2627	Tabelle 27: Tab_FM_ePA_016 Beschreibung und Parameter der Operation	
2628	ActivateAccount (Semantik) .....	72
2629	Tabelle 28: Tab_FM_ePA_020 Beschreibung und Parameter der Operation	
2630	RequestFacilityAuthorization (Semantik) .....	72
2631	Tabelle 29: Tab_FM_ePA_039 Beschreibung und Parameter der Operation	
2632	GetHomeCommunityID (Semantik) .....	74
2633	Tabelle 30: Tab_FM_ePA_032 Fehlermeldungen der Operation GetHomeCommunityID ..	74
2634	Tabelle 31: Tab_FM_ePA_040 Beschreibung und Parameter der Operation	
2635	GetAuthorizationList (Semantik) .....	75
2636	Tabelle 32: Tab_FM_ePA_041 Fehlermeldungen der Operation GetAuthorizationList .....	75



2637	Tabelle 33: Tab_FM_ePA_021 Terminalanzeigen für PIN-Eingaben—Operation	
2638	ActivateAccount .....	78
2639	Tabelle 34: Tab_FM_ePA_019 Terminalanzeigen für PIN-Eingaben—	
2640	Operation RequestFacilityAuthorization .....	79
2641	Tabelle 35: Tab_FM_ePA_025: Operation RequestFacilityAuthorization—Ausgabetexte am	
2642	Kartenterminal.....	79
2643	Tabelle 36: Tab_FM_ePA_023 Base Policy Belegung.....	89
2644	Tabelle 1: Tab FM ePA 008 Konfigurationswerte des Fachmoduls ePA .....	16
2645	Tabelle 2: Tab FM ePA 053 - Übersicht der Fehlerfälle nach Status des Status eines	
2646	Aktenkontos .....	18
2647	Tabelle 3: Tab FM ePA 002 Profile, Akteure und Optionen des Webservices PHRService	
2648	.....	23
2649	Tabelle 4: Tab FM ePA 034 Übersicht der Funktionen, die ein SM-B benötigen, mit	
2650	Zuordnung zu den aufrufenden Operationen und ob die SM-B eine Berechtigung zum	
2651	Zugriff haben muss.....	28
2652	Tabelle 5: Tab FM ePA 001 Daten zur Kommunikation mit den Komponenten des ePA-	
2653	Aktensystems (abhängig vom Nutzer).....	31
2654	Tabelle 6: Tab FM ePA 033 Fehlermeldungen bei der Authentisierung mittels eGK .....	35
2655	Tabelle 7: Tab FM ePA 030 Authentifizierungsbestätigung erstellen .....	36
2656	Tabelle 8: Tab FM ePA 026 Aufrufparameter der Operation	
2657	I Authorization::getAuthorizationKey .....	37
2658	Tabelle 9: Tab FM ePA 007 Service-Informationen der Services des Fachmoduls ePA..	46
2659	Tabelle 10: Tab FM ePA 014 Parameter des Fehlerprotokolls.....	48
2660	Tabelle 11: Tab FM ePA 015 Parameter des Debug-Protokolls .....	49
2661	Tabelle 12: Tab FM ePA 022 Parameter des Sicherheitsprotokolls .....	49
2662	Tabelle 13: Tab FM ePA 024 Parameter des Performanceprotokolls.....	50
2663	Tabelle 14: Tab FM ePA 010 Übergreifende Konfigurationsparameter des Fachmoduls	
2664	ePA .....	50
2665	Tabelle 15: Tab FM ePA 011 Übergreifende Fehlermeldungen des Fachmoduls ePA .....	52
2666	Tabelle 16: Tab FM ePA 050 Wiederverwendete Fehlermeldungen aus der	
2667	Konnektorspezifikation .....	53
2668	Tabelle 17: Tab FM ePA 051 Wiederverwendete Fehlermeldungen aus der	
2669	Übergreifenden Spezifikation Operations und Maintenance .....	54
2670	Tabelle 18: Tab FM ePA 004 Schnittstellenübersicht des Fachmoduls ePA .....	55
2671	Tabelle 19: Tab FM ePA 005 Beschreibung des Webservices PHRService .....	57
2672	Tabelle 20: Tab FM ePA 005 2.x Beschreibung des Webservices PHRService .....	58
2673	Tabelle 21: Tab FM ePA 012 Mapping von gematik-Fehlern nach IHE-Fehlern .....	59
2674	Tabelle 22: Tab FM ePA 006 Beschreibung und Parameter der Operation putDocuments	
2675	.....	60
2676	Tabelle 23: Tab FM ePA 013 Beschreibung und Parameter der Operation find	
2677	(Semantik) .....	61

2678	<a href="#">Tabelle 24: Tab FM ePA 027 Beschreibung und Parameter der Operation getDocuments</a>	
2679	<a href="#">(Semantik) .....</a>	61
2680	<a href="#">Tabelle 25: Tab FM ePA 029 Beschreibung und Parameter der Operation</a>	
2681	<a href="#">removeDocuments (Semantik) .....</a>	62
2682	<a href="#">Tabelle 26: Tab FM ePA 031 Beschreibung und Parameter der Operation</a>	
2683	<a href="#">updateDocumentSet (Semantik) .....</a>	63
2684	<a href="#">Tabelle 27: Tab FM ePA 003 Beschreibung des Webservices PHRManagementService</a>	70
2685	<a href="#">Tabelle 28: Tab FM ePA 003 Beschreibung des Webservices PHRManagementService</a>	71
2686	<a href="#">Tabelle 29: Tab FM ePA 016 Beschreibung und Parameter der Operation</a>	
2687	<a href="#">ActivateAccount (Semantik) .....</a>	72
2688	<a href="#">Tabelle 30: Tab FM ePA 020 Beschreibung und Parameter der Operation</a>	
2689	<a href="#">RequestFacilityAuthorization (Semantik) .....</a>	72
2690	<a href="#">Tabelle 31: Tab FM ePA 039 Beschreibung und Parameter der Operation</a>	
2691	<a href="#">GetHomeCommunityID (Semantik) .....</a>	74
2692	<a href="#">Tabelle 32: Tab FM ePA 032 Fehlermeldungen der Operation GetHomeCommunityID..</a>	74
2693	<a href="#">Tabelle 33: Tab FM ePA 040 Beschreibung und Parameter der Operation</a>	
2694	<a href="#">GetAuthorizationList (Semantik) .....</a>	75
2695	<a href="#">Tabelle 34: Tab FM ePA 041 Fehlermeldungen der Operation GetAuthorizationList.....</a>	75
2696	<a href="#">Tabelle 35: Tab FM ePA 021 Terminalanzeigen für PIN-Eingaben - Operation</a>	
2697	<a href="#">ActivateAccount .....</a>	78
2698	<a href="#">Tabelle 36: Tab FM ePA 019 Terminalanzeigen für PIN-Eingaben -</a>	
2699	<a href="#">Operation RequestFacilityAuthorization .....</a>	79
2700	<a href="#">Tabelle 37: Tab FM ePA 025: Operation RequestFacilityAuthorization - Ausgabertexte am</a>	
2701	<a href="#">Kartenterminal .....</a>	79
2702	<a href="#">Tabelle 38: Tab FM ePA 025: Operation RequestFacilityAuthorization Version 2 -</a>	
2703	<a href="#">Ausgabertexte am Kartenterminal .....</a>	81
2704	<a href="#">Tabelle 39 : Tab FM ePA 042 - Mapping von DocumentCategoryEnum auf Anzeigetext</a>	
2705	<a href="#">am Kartenterminal .....</a>	83
2706	<a href="#">Tabelle 40 : Tab FM ePA 043 - Beispiel Anzeige am Kartenterminal der Operation</a>	
2707	<a href="#">RequestFacilityAuthorization Version 2 ohne Dokumentkategorien .....</a>	83
2708	<a href="#">Tabelle 41 : Tab FM ePA 043 - Beispiel Anzeige am Kartenterminal der Operation</a>	
2709	<a href="#">RequestFacilityAuthorization Version 2 mit Dokumentenkategorien .....</a>	84
2710	<a href="#">Tabelle 42: Tab FM ePA 023 Base Policy Belegung.....</a>	89
2711	<a href="#">Tabelle 43: Tab FM ePA 023 Base Policy Belegung.....</a>	90
2712		

## 2713 8.5 Referenzierte Dokumente

### 2714 8.5.1 Dokumente der gematik

2715 Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument  
 2716 referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der  
 2717 vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und

2718 Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert; Version und  
 2719 Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht  
 2720 aufgeführt. Deren zu diesem Dokument jeweils gültige Versionsnummern sind in der  
 2721 aktuellen, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die  
 2722 vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Einführung der Gesundheitskarte - Glossar
[gemSpec_Aktensystem]	gematik: Spezifikation ePA-Aktensystem
[gemSpec_Authentisierung_Vers]	gematik: Spezifikation Authentisierung des Versicherten ePA
[gemSpec_Autorisierung]	gematik: Spezifikation Autorisierung ePA
[gemSpec_DM_ePA]	gematik: Datenmodell ePA
[gemSpec_FM_ePA]	gematik: Spezifikation Fachmodul ePA
[gemSpec_eGK_ObjSys] [gemSpec_eGK_ObjSys_G2_1]	gematik: Spezifikation der elektronischen Gesundheitskarte eGK-Objektsystem
[gemSpec_OID]	gematik: Spezifikation Festlegung von OIDs
[gemSpec_OM]	gematik: Übergreifende Spezifikation Operations und Maintenance
[gemSysL_ePA]	gematik: Systemspezifisches Konzept ePA
[gemSpec_Krypt]	gematik: Übergreifende Spezifikation - Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_SGD_ePA]	gematik: Spezifikation Schlüsselerzeugungsdienst ePA

2723

## 2724 8.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[IHE-ITI-ACWP]	IHE International (2009): IHE IT Infrastructure White Paper Access Control Revision 1.3, <a href="http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF_WhitePaper">http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF_WhitePaper</a>

	<a href="#">AccessControl_2009-09-28.pdf</a>
[IHE-ITI-APPC]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework Supplement, Advanced Patient Privacy Consents (APPC), Revision 1.2 – Trial Implementation, <a href="http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_APPC.pdf">http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_APPC.pdf</a>
[IHE-ITI-DEN]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework Supplement, Document Encryption (DEN), Revision 1.3 – Trial Implementation, <a href="http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_DEN.pdf">http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_DEN.pdf</a>
[IHE-ITI-RMD]	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-SeR]	IHE International (2016): IHE IT Infrastructure (ITI) Technical Framework Supplement, Secure Retrieve (SeR), Trial Implementation Revision 1.3, <a href="http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_SeR.pdf">http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_SeR.pdf</a>
[IHE_SHR D_GL]	IHE International (2018): IHE Technical Frameworks, General Introduction, Appendix D: Glossary, Revision 2.0, <a href="https://www.ihe.net/uploadedFiles/Documents/Templates/IHE_TF_GenIntro_AppD_Glossary_Rev2.0_2018-03-09.pdf">https://www.ihe.net/uploadedFiles/Documents/Templates/IHE_TF_GenIntro_AppD_Glossary_Rev2.0_2018-03-09.pdf</a>
[IHE-ITI-TF]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework, Revision 15.0
[IHE-ITI-TF1]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework, Volume 1 (ITI TF-1) – Integration Profiles, Revision 15.0, <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>
[IHE-ITI-TF2a]	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]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework, Volume 2b (ITI TF-2b) – Transactions Part B, Revision 15.0, <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-2b) – 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-VS]	IHE Deutschland (2018): Value Sets für Aktenprojekte im deutschen Gesundheitswesen, Implementierungsleitfaden, Version 2.0, <a href="http://www.ihe-d.de/download/ihe-valuesets-v2-0/">http://www.ihe-d.de/download/ihe-valuesets-v2-0/</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>
<del>[IHE-ITI-RMU]</del>	<del>IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework Supplement, Restricted Metadata Update (RMU), Revision 1.1 – Trial Implementation, <a href="https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RMU.pdf">https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RMU.pdf</a></del>
[KVNR]	Vertrauensstelle Krankenversichertennummer <a href="https://www.itsg.de/gkv-interne-services/vertrauensstelle-kvnr/">https://www.itsg.de/gkv-interne-services/vertrauensstelle-kvnr/</a>
[RFC2119]	IETF (1997): Key words for use in RFCs to Indicate Requirement Levels, RFC 2119, <a href="http://tools.ietf.org/html/rfc2119">http://tools.ietf.org/html/rfc2119</a>
[SOAP1.2]	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>

[WSS-SAML]	OASIS (2006): Web Services Security: SAML Token Profile 1.1, <a href="https://www.oasis-open.org/committees/download.php/16768/wss-v1.1-spec-os-SAMLSecurityTokenProfile.pdf">https://www.oasis-open.org/committees/download.php/16768/wss-v1.1-spec-os-SAMLSecurityTokenProfile.pdf</a>
------------	--

2725

ENTWURF