gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation Fachmodul ePA

Version:	1.3.0
Revision:	166399
Stand:	02.10.2019
Status:	freigegeben
Klassifizierung:	öffentlich
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

Inhaltsverzeichnis

1 Einordnung des Dokumentes 5
1.1 Zielsetzung 5
1.2 Zielgruppe 5
1.3 Geltungsbereich 5
1.4 Abgrenzungen 6
1.5 Methodik 6
2 Systemüberblick 7
3 Systemkontext 8
4 Zerlegung des Produkttyps 9
5 Technologien und Standards 10
5.1 Webservices 10
5.2 Integrating the Healthcare Enterprise (IHE) 10
5.2.1 Relevante IHE-Integrationsprofile 10
5.2.2 Überblick über IHE-Akteure und assoziierte Transaktionen 12
6 Übergreifende Festlegungen 14
6.1 Allgemein 14
6.2 IHE 21
6.3 Lokalisierung von ePA-Aktensystemen 23
6.4 Aufrufkontext und Auswahl eines SM-B 24
6.5 Login 27
6.5.1 Aktensession 28
6.5.2 Authentisierung mittels SM-B 30
6.5.3 Authentisierung mittels eGK 32
6.5.4 Autorisierung 34
6.5.5 Verbindung zur Dokumentenverwaltung 37
6.5.6 Schlüsselableitung 39
6.6 Logout 43
6.7 Datenschutz und Sicherheitsaspekte 44
6.8 Verwendung des Dienstverzeichnisdienstes 45
6.9 Protokollierung und Logging 46
6.10 Konfiguration 49
6.11 Fehlerbehandlung und Fehlermeldungen 49

7 Funktionsmerkmale 53

7.1 PHRService 54
7.1.1 Definition/Signatur 56
7.1.1.1 putDocuments 56
7.1.1.2 find 57
7.1.1.3 getDocuments 58
7.1.1.4 removeDocuments 58
7.1.1.5 updateDocumentSet 59
7.1.2 Umsetzung 60
7.1.2.1 putDocuments 61
7.1.2.2 find 63
7.1.2.3 getDocuments 63
7.1.2.4 removeDocuments 64
7.1.2.5 updateDocumentSet 65

7.2 PHRManagementService 66
7.2.1 Definition/Signatur 67
7.2.1.1 ActivateAccount 67
7.2.1.2 RequestFacilityAuthorization 68
7.2.1.3 GetHomeCommunityID 69
7.2.1.4 GetAuthorizationList 70
7.2.2 Umsetzung 71
7.2.2.1 ActivateAccount 72
7.2.2.2 RequestFacilityAuthorization 74
7.2.2.3 GetHomeCommunityID 82
7.2.2.4 GetAuthorizationList 84

8 Anhang A – Verzeichnisse 86

8.1 Abkürzungen 86

8.2 Glossar 87

8.3 Abbildungsverzeichnis 87

8.4 Tabellenverzeichnis 87

8.5 Referenzierte Dokumente 89
8.5.1 Dokumente der gematik 89
8.5.2 Weitere Dokumente 90

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 verwalteten. 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.

1.4 Abgrenzungen

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

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

1.5 Methodik

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

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

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

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

2 Systemüberblick

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 anderseits 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.

3 Systemkontext

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

4 Zerlegung des Produkttyps

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

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

Das Herunterladen von Dokumenten wird über die folgenden Transaktionen umgesetzt:

1. Retrieve Document Set [ITI-43]: Das Primärsystem stößt als XDS-Akteur „Document Consumer" den Download eines oder mehrerer Dokumente an.
2. Cross-Gateway Retrieve [ITI-39]: das Fachmodul ePA als XCA-Akteur „Initiating Gateway" nimmt die Anfrage entgegen und leitet sie an den Anbieter ePA-Aktensystem (XCA-Akteur „Responding Gateway") weiter.
3. Die angefragten Dokumente werden vom Anbieter ePA-Aktensystem über XCA „Responding Gateway" und „Initiating Gateway" an das Primärsystem zurückgeliefert.

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

[<=]

A_15648 - FM ePA: Übergreifende Anforderung - Timeout bei TLS-Verbindungsaufbau - Fehler
Falls beim TLS-Verbindungsaufbau zu jeweils allen zur Durchführung einer Operation benötigten Komponenten und Diensten

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

der Wert von EPA_TLS_HS_TIMEOUT überschritten wird, MUSS das Fachmodul ePA den TLS-Verbindungsaufbau abbrechen und die vom Primärsystem aufgerufene Operation mit dem Code 7202 gemäß Tab_FM_ePA_011 abbrechen.
[<=]

A_15649 - FM ePA: Übergreifende Anforderung - Aktensystem antwortet nicht - Fehler
Falls beim TLS-Verbindungsaufbau zu jeweils allen zur Durchführung einer Operation benötigten Komponenten und Diensten

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

die Antworten nach der Anzahl von EPA_KEEP_ALIVE_TRY_COUNT Versuchen ausbleibt, MUSS das Fachmodul ePA die Netzwerkverbindungen beenden und die vom

Primärsystem aufgerufene Operation mit dem Code 7220 gemäß Tab_FM_ePA_011 abbrechen.
[<=]

A_17948 - FM ePA: Authentisierung mit eGK - TLS-Verbindung - Fehler
Falls beim Aufbau der TLS-Verbindung zu jeweils allen zur Durchführung einer Operation benötigten Komponenten und Diensten

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

ein Fehler auftritt, MUSS das Fachmodul ePA die Operation mit dem Code 7202 gemäß Tab_FM_ePA_011 abbrechen.
[<=]

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

Status des Aktenkontos

A_17744 - FM ePA: Übergreifende Anforderung - Status des Aktenkontos - Fehlerbehandlung
Das Fachmodul ePA MUSS in Abhängigkeit des Status des Aktenkontos und der ausgeführten Operation mit den nachfolgend zugeordneten Codes als Fehler oder Warnung abbrechen:

Tabelle 2: Tab_FM_ePA_053 - Übersicht der Fehlerfälle nach Status des Status eines AktenkontosTabelle 3: Tab_FM_ePA_053 - Übersicht der Fehlerfälle nach Status des Status eines 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 putDocuments, 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

[<=]

Hinweise:

- Eine Auflistung und Erläuterung aller Status befindet sich in [gemSpec_Aktensystem].
- Ein Aktenkonto kann nur aktiviert werden, falls es sich im Status REGISTERED befindet.
- ~~Alternative Versichertenidentitäten und~~ Berechtigungen für LEI können auch bei einem Aktenkonto hinzugefügt werden, das sich im Status DISMISSED befindet.
- Falls RequestFacilityAuthorization mit einem Aktenkonto aufgerufen wird, das sich im Status REGISTERED befindet, führt das Fachmodul vorher implizit die Operation ActivateAccount durch, um das Aktenkonto zu aktivieren.

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

Der Status und die Existenz eines Aktenkontos kann mit Hilfe der Operation I_Authorization_Management::checkRecordExists der Komponente Autorisierung eines ePA-Aktensystems ermittelt werden. Für manche Operationen müssen alle bekannten ePA-Aktensysteme angefragt werden, 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.

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 - 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 4: 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 wird benötigt, um Update-Nachricht weiterzuleiten an XCA Responding Gateway der Dokumentenverwaltung. Die Option erzwingt eine Gruppierung mit einem RMU Update Initiator.
	Update Initiator	Keine	Keine Optionen benötigt.
APPC gemäß [IHE-ITI-APPC]	Content Creator*	Keine	Keine Optionen benötigt.
XCDR gemäß [IHE-ITI-XCDR]	XCDR Initiating Gateway	Keine	Keine Option benötigt.
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 abbrechen.**[<=]**

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.

6.4 Aufrufkontext und Auswahl eines SM-B

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

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

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

A_14947 - FM ePA: Login - Ermittlung des Aufrufkontexts via Aufrufparameter
Der Webservice PHRManagementService MUSS den Aufrufkontext gemäß [ConnectorContext.xsd] anhand des im Aufruf übergebenen Parameters Context bestimmen.**[<=]**

A_15142 - FM ePA: Login - Ermittlung des Aufrufkontexts via SOAP-Header
Der Webservice PHRService MUSS den Aufrufkontext gemäß [ConnectorContext.xsd] anhand der nach Tab_FM_ePA_005 übertragenen SOAP-Header bestimmen.
[<=]

Default-Aufrufkontext

A_14084 - FM ePA: Login - Bereitstellung Default-Aufrufkontext
Das Fachmodul ePA MUSS im Informationsmodell des Konnektors einen Default-Aufrufkontext für die Nutzung des Webservices PHRService bereitstellen mit:

- MandantId = "Mandant_ePA_Default"
- ClientsystemId = "Clientsystem_ePA_Default"
- WorkplaceId = "Workplace_ePA_Default

[<=]

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 - FM ePA: Login - Zugriffsberechtigung auf vom Konnektor verwaltete Ressourcen - Fehler
Falls bei der Prüfung der Zugriffsberechtigung auf das ausgewählte SM-B 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 5: 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?)
Authentisierung am ePA-Aktensystem Zur Erstellung (Signatur) einer AuthenticationAssertion benötigt das Fachmodul ePA ein gültiges SM-B.	Alle Operationen des Webservices PHRService und die Operation GetAuthorizationList
Autorisierung am ePA-Aktensystem Zum Abruf des Chiffrats, welches Akten- und Kontextschlüssel enthält, benötigt das Fachmodul ePA eine AuthenticationAssertion für ein gültiges SM-B, dessen Telematik-ID zuvor zum Zugriff auf die Patientenakte berechtigt wurde. Zum Abruf der Schlüssel gemäß [gemSpec_SGD_ePA], mit denen das Chiffrat entschlüsselt werden kann, benötigt das Fachmodul ePA ein gültiges SM-B, dessen Telematik-ID zuvor zum Zugriff auf die Patientenakte berechtigt wurde.	Alle Operationen des Webservices PHRService
C2C mit eGK Zur Freischaltung von PrK.CH.AUT (eGK) bei der Authentisierung wird ein beliebiges SM-B benötigt.	ActivateAccount, RequestFacilityAuthorization
Berechtigungsvergabe Die Berechtigungsvergabe an eine LEI erfolgt für die Telematik-ID des ausgewählten SM-B.	RequestFacilityAuthorization

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

A_15614 - FM ePA: Übergreifende Anforderung - Ermittlung eines SM-B
Das Fachmodul ePA MUSS zu jedem Aufrufkontext ein im Informationsmodell des Konnektors konfiguriertes, freigeschaltetes SM-B des Mandanten ermitteln.
[<=]

A_17928 - FM ePA: Übergreifende Anforderung - Ermittlung eines SM-B - Prüfung OID
Das Fachmodul ePA MUSS eine SM-B ermitteln, welche im Zertifikat C.HCI.OSIG im Feld `ProfessionOID` der ZertifikatsExtension `Admission` mindestens eine der

zulässigen Autorisierungsempfänger-Rollen gemäß [gemSpec_OID#Tab_PKI_402] und [gemSpec_OID#Tab_PKI_403]

- oid_praxis_arzt
- oid_zahnarztpraxis
- oid_praxis_psychotherapeut
- oid_krankenhaus
- oid_oeffentliche_apotheke
- oid_krankenhausapotheke
- oid_bundeswehrapotheke
- oid_mobile_einrichtung_rettungsdienst

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:

Tabelle 6: Tab_FM_ePA_001 Daten zur Kommunikation mit den Komponenten des ePA-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 • SM-B: Fachmodul • eGK: Komponente Zugangsgateway für Versicherte des ePA-Aktensystems	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_17225) erzeugt bzw. ausgetauscht werden.	z.B. Ableitungsschlüssel, Authentisierungstoken
SGD-Assets	Kryptographische Geheimnisse, die beim Aufbau der sicheren Verbindung zu einem SGD (A_17777) erzeugt bzw. ausgetauscht werden.	z.B. kurzlebige ECIES-Schlüssel

A_13677 - FM ePA: Aktensession - Trennung von Operation
Das Fachmodul ePA MUSS alle Operationsaufrufe sowie die den Operationen zugehörige Aktensession voneinander trennen.**[<=]**

A_15143 - FM ePA: Aktensession - Temporäre Speicherung und Wiederverwendung (SM-B)
Das Fachmodul ePA KANN auf Basis des Tupels (Telematik-ID der zur Authentisierung verwendeten SM-B, RecordIdentifier) eine Aktensession temporär speichern und wiederverwenden.**[<=]**

A_15144 - FM ePA: Aktensession - Temporäre Speicherung und Wiederverwendung (eGK)
Das Fachmodul ePA KANN auf Basis des Tupels (Versicherten-ID einer zur Authentisierung verwendeten eGK, RecordIdentifier) eine Aktensession temporär speichern und wiederverwenden.

[<=]

A_17949 - 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 und alle dazugehörigen Daten löschen.**[<=]**

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

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 Signaturdienstes 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.**[**<=**]**

A_14945 - 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 7: 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~~	• ~~pinResult = REJECTED für falsche PIN (pinResult als Ergebnis Perform Verification)~~ • ~~4043, 4049~~ • ~~Alle weiteren Fehlercodes, die der Kartendienst zurückgibt~~
~~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.~~
[<=**]**

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 8: 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	• ~~pinResult = REJECTED für falsche PIN (pinResult als Ergebnis Perform Verification)~~ • 4043, 4049 • Alle weiteren Fehlercodes, die der Kartendienst zurückgibt
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.
[<=]

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.**[<=]**

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.**[<=]**

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.
[<=]

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 9: 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 Chiffrat mit Akten- und Kontextschlüssel sowie eine Autorisierungsbestätigung (`AuthorizationAssertion`) zur Kommunikation mit der Dokumentenverwaltung ausgehändigt. Das Chiffrat wird mit zwei gemäß [gemSpec_SGD_ePA] abgeleiteten Schlüsseln der SGDs entschlüsselt. Der Ablauf gliedert sich in die folgenden Schritte:

1. TLS-Verbindung zur Komponente Autorisierung aufbauen
2. Aufruf der Operation I_Authorization::getAuthorizationKey der Komponente Autorisierung, Übergabe der `AuthenticationAssertion` und entsprechender Signatur im SOAP-Header gemäß [WSS-SAML]
3. Verbindungsaufbau zu zwei SGDs und Abruf jeweils eines AES-Schlüssels

4. Entschlüsselung von Akten- und Kontextschlüssel zur Nutzung in der Aktensession

Verbindungsaufbau zur Komponente Autorisierung

Im Konnektor baut das Fachmodul ePA mit Hilfe von TUC_KON_110 „Kartenbasierte TLS-Verbindung aufbauen" gemäß [gemSpec_Kon#4.1.11.4.1] die TLS-Verbindung ohne Clientauthentisierung und mit Rollenprüfung auf.

A_14105 - FM ePA: Autorisierung - TLS-Verbindung zur Komponente Autorisierung aufbauen
Das Fachmodul ePA MUSS zur Kommunikation mit der Komponente Autorisierung eine TLS-Verbindung aufbauen bzw. eine bestehende TLS-Verbindung nutzen.**[<=]**

A_14223 - FM ePA: Autorisierung - Verbindung mit Zertifikats- und Rollenprüfung
Das Fachmodul ePA MUSS beim Aufbau der TLS-Verbindung zur Komponente Autorisierung eine Zertifikats- und Rollenprüfung für das Zertifikatsprofil C.FD.TLS-S gemäß [gemSpec_PKI] mit der Rolle oid_epa_authz gemäß [gemSpec_OID#GS-A_4446] durchführen.
[<=]

A_14222 - FM ePA: Autorisierung - Verwendung der lokalisierten URI
Das Fachmodul ePA MUSS beim Aufbau der TLS-Verbindung zur Komponente Autorisierung deren lokalisierte Adresse verwenden.**[<=]**

Abruf des Chiffrats für den authentisierten Nutzer (LEI oder Versicherter / Vertreter)

A_14014 - FM ePA: Autorisierung Aktensession - Request SAML
Das Fachmodul ePA MUSS zur Autorisierung der Aktensession die Operation I_Authorization::getAuthorizationKey gemäß [gemSpec_Autorisierung] mit folgenden Parametern aufrufen:

Tabelle 10: Tab_FM_ePA_026 Aufrufparameter der Operation I_Authorization::getAuthorizationKey

Parameter	Inhalt	Beschreibung
RecordIdentifier	[`RecordIdentifier` 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

[<=]

Legende:

- Inhalte in eckigen Klammern ([...]) sind ihrer Beschreibung nach zu ersetzen.
- Die Parameter sind der Spezifikation [gemSpec_Autorisierung] entnommen.

A_14243 - FM ePA: Autorisierung Aktensession - Fehler - keine Autorisierung vorhanden
Falls beim Aufruf der Operation I_Authorization::getAuthorizationKey eines Aktendienstes des Versicherten keine Berechtigung für den Nutzer im Aktenkonto hinterlegt ist (ACCESS_DENIED, KEY_ERROR), MUSS das Fachmodul ePA die Operation mit dem Code 7209 gemäß Tab_FM_ePA_011 abbrechen.**[**<=**]**

A_14024 - FM ePA: Autorisierung Aktensession - Fehler
Wurde die Operation I_Authorization::getAuthorizationKey eines Aktendienstes des Versicherten mit einem anderen Fehler als ACCESS_DENIED~~,~~ oder KEY_ERROR beendet, dann MUSS das Fachmodul ePA die Operation mit dem Code 7400 gemäß Tab_FM_ePA_011 abbrechen.**[**<=**]**

Weitere Fehlerrückgaben der Operation I_Authorization~~_Management~~::getAuthorizationKey werden in [gemSpec_Autorisierung] spezifiziert.

Schlüsselableitung und Entschlüsselung von Akten- und Kontextschlüssel

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

Benachrichtigung des Primärsystem über bestehende Berechtigungen zum Zugriff auf ein Aktenkonto

A_15134 - FM ePA: Autorisierung Aktensession - Benachrichtigung an das Primärsystem
Wurde die Operation I_Authorization::getAuthorizationKey zur Autorisierung der LEI erfolgreich aufgerufen MUSS das Fachmodul ePA unter Verwendung des 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 `DateTime` in folgendem Format angegeben: `yyyy-mm-ddThh:mm:ss+hh:mm` Es ist – gemäß ISO 8601 [ISO8601] – die lokale Zeit und die Differenz zur UTC anzugeben.]

[<=**]**

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

6.5.5 Verbindung zur Dokumentenverwaltung

Alle Operationen des Webservices PHRService sowie die Operatione RequestFacilityAuthorization benötigen einen initialisierten Aktenkontext in der Dokumentenverwaltung, d.h. eine Verbindung zum Verarbeitungskontext der Vertrauenswürdigen Ausführungsumgebung (VAU) des Versicherten wie in [gemSpec_Dokumentenverwaltung#4.4] beschrieben. Das Fachmodul ePA muss dafür eine TLS-Verbindung zur Komponente Dokumentenverwaltung des Aktensystems, in welchem das Aktenkonto des Versicherten liegt, aufbauen. Die Dokumente des Aktenkontos werden zwischen dem Fachmodul ePA und dem Verarbeitungskontext der VAU in einem sicheren Kanal auf HTTP-Anwendungsschicht gemäß [gemSpec_Krypt#6.1] übertragen.

Die Schnittstelle der Dokumentenverwaltung wird in [gemSpec_Dokumentenverwaltung#5.4] spezifiziert.

Aufbau der TLS-Verbindung

A_15531 - FM ePA: Dokumentenverwaltung - TLS-Verbindung zur Komponente Dokumentenverwaltung aufbauen
Das Fachmodul ePA MUSS zur Kommunikation mit der Komponente Dokumentenverwaltung eine TLS-Verbindung aufbauen bzw. eine bestehende TLS-Verbindung nutzen.**[**<=**]**

A_15532 - FM ePA: Dokumentenverwaltung - TLS mit Zertifikats- und Rollenprüfung
Das Fachmodul ePA MUSS beim Aufbau der TLS-Verbindung zur Komponente Dokumentenverwaltung eine Zertifikats- und Rollenprüfung für das Zertifikatsprofil C.FD.TLS-S gemäß [gemSpec_PKI] mit der Rolle oid_epa_dvw gemäß [gemSpec_OID#GS-A_4446] durchführen.**[**<=**]**

A_15533 - FM ePA: Dokumentenverwaltung - Verwendung der lokalisierten URI
Das Fachmodul ePA MUSS beim Aufbau der TLS-Verbindung zur Komponente Dokumentenverwaltung deren lokalisierte Adresse verwenden.**[**<=**]**

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

A_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 #6.1].**[**<=**]**

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 abbrechen.**[<=]**

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 - FM ePA: Dokumentenverwaltung - Initialisierung des Aktenkontexts - Fehler in der Dokumentenverwaltung
~~Falls bei der Kommunikation mit der Komponente Dokumentenverwaltung zur Initialisierung des Aktenkontexts ein Fehler TECHNICAL_ERROR auftritt, MUSS das Fachmodul ePA die Operation mit dem Code 7215 gemäß Tab_FM_ePA_011 abbrechen.~~ **[<=]**

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 ~~TECHNICAL_ERROR~~ auftritt, MUSS das Fachmodul ePA die Operation mit dem Code 7215 gemäß Tab_FM_ePA_011 abbrechen. **[<=]**

A_17119 - FM ePA: Dokumentenverwaltung - Initialisierung des Aktenkontexts - Fehler
~~Falls bei der Kommunikation mit der Komponente Dokumentenverwaltung zur Initialisierung des Aktenkontexts ein anderer Fehler als TECHNICAL_ERROR auftritt, MUSS das Fachmodul ePA die Operation mit dem Code 7400 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 SGDs 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 Chiffrat 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:

- Login (Authentisierung) mit eGK: Code 106 gemäß Tab_FM_ePA_051
- Login (Authentisierung) mit SM-B: Code 7221 gemäß Tab_FM_ePA_011.

[<=]

A_17871 - FM ePA: Schlüsselableitung - Fehler an der Schnittstelle zum Schlüsselgenerierungsdienst
Falls beim Abruf der AES-Schlüssel gemäß [gemSpec_SGD_ePA] ein anderer Fehler als "certificate not valid" oder "signature not valid" auftritt, MUSS das Fachmodul ePA die aufgerufene Operation mit dem Code 7215 gemäß Tab_FM_ePA_011 abbrechen.**[<=]**

Als Ergebnis bei einer erfolgreichen Schlüsselableitung zum Verschlüsseln erhält das Fachmodul ePA von jedem der beiden SGD eine Antwortnachricht für KeyDerivation im Format: "OK-KeyDerivation "+Key+" "+a.
Key ist der für die Verschlüsselung zu verwendende symmetrische Schlüssel und a entspricht AssociatedData für den entsprechenden SGD.

Festlegungen zur Verschlüsselung von Akten- und Kontextschlüssel

A_17992 - FM ePA: Schlüsselableitung - Ermittlung von AssociatedData
Falls bei der Erteilung einer Berechtigung (Operation ActivateAccount, Operation RequestFacilityAuthorization) der Aufruf der Operation KeyDerivation beim SGD zur Schlüsselableitung erfolgreich war MUSS das Fachmodul ePA den Wert `phrs:AuthorizationKey/phrs:EncryptedKeyContainer/phrs:AssociatedData` gemäß [gemSpec_SGD_ePA#8] mit dem Inhalt aus 'a' der Antwortnachrichten befüllen.
[<=]

Zur Erteilung einer Berechtigung unter Verwendung der Operation ActivateAccount wird der Anwendungsfall gemSpec_SGD_ePA#2.4 betrachtet.
Zur Erteilung einer Berechtigung unter Verwendung der Operation RequestFacilityAuthorization werden die Anwendungsfälle gemSpec_SGD_ePA#2.6 und gemSpec_SGD_ePA#2.8 betrachtet.

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

A_18007 - Schlüsselableitung bei Verschlüsselung - Verschlüsselung mit Verschlüsselungsdienst
Das Fachmodul ePA MUSS beim Erstellen eines AuthorizationKeys den Akten- und Kontextschlüssel mit den von der Schlüsselableitung mit SGD 1 und SGD 2 erhaltenen symmetrischen Schlüssel unter Berücksichtigung der Strukturen in [gemSpec_SGD_ePA#8] unter Berücksichtigung der Reihenfolge wie folgt verschlüsseln:

1. Verschlüsseln mit symmetrischem Schlüssel von SGD 1 durch Aufruf von TUC_KON_075	Eingangsdaten: • dataToBeEncrypted = Klartextpräsentation von Akten- und Kontextschlüssel gemäß gemSpec_SGD_ePA#Tab_Austauschformat Akten- und Kontextschlüssel • symmetricKey = aus SGD 1 abgeleiteter symmetrischer Schlüssel • associatedData = Anteil 'a' aus KeyDeriviation Response des SGD 1 Ausgangsdaten: • encryptedData Mit encryptedData und aus SGD 1 abgeleiteter symmetrischer Schlüssel wird eine Struktur [gemSpec_SGD_ePA#Tab_erste_Verschlüsselungsschicht] gebildet.
2. Verschlüsseln mit symmetrischem Schlüssel von SGD 2 durch Aufruf von TUC_KON_075	Eingangsdaten: • dataToBeEncrypted = im vorangegangenen Schritt gebildete Struktur [gemSpec_SGD_ePA#Tab_erste_Verschlüsselungsschicht] • symmetricKey = aus SGD 2 abgeleiteter symmetrischer Schlüssel • associatedData = Anteil 'a' aus KeyDeriviation Response des SGD 2 Ausgangsdaten: • encryptedData 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.

[<=]

Festlegungen zur Entschlüsselung von Akten- und Kontextschlüssel

I_Authorization::getAuthorizationKey liefert abhängig von der Telematik-ID bzw. KVNR der übertragenen AuthenticationAssertion das Chiffrat für einen berechtigten Nutzer mit Akten- und Kontextschlüssel, die Information durch wen die Berechtigung erfolgte und eine dazu passende AuthorizationAssertion. Das Fachmodul ePA kann im nächsten Schritt das Chiffrat entschlüsseln und Akten- und Kontextschlüssel liegen im Klartext vor und können verwendet werden.

A_17869 - FM ePA: Schlüsselableitung bei Entschlüsselung - Entschlüsselung mit Verschlüsselungsdienst
Falls AuthorizationKey für den authentisierten Nutzer von der Komponente Autorisierung abgerufen werden konnte, MUSS das Fachmodul ePA die AES-Schlüssel von den beiden SGDs abrufen und damit Akten- und Kontextschlüssel unter Berücksichtigung der Strukturen in [gemSpec_SGD_ePA#8] wie folgt unter Berücksichtigung der Reihenfolge entschlüsseln:

1. Entschlüsseln mit symmetrischem Schlüssel von SGD 2 durch Aufruf von TUC_KON_076	Eingangsdaten: • encryptedData = `phrs:AuthorizationKey/phrs:EncryptedKeyContainer/phrs:Ciphertext` • symmetricKey = aus SGD 2 abgeleiteter symmetrischer Schlüssel • associatedData = `phrs:AuthorizationKey/phrs:EncryptedKeyContainer/phrs:AssociatedData [1]` Ausgangsdaten: • plainData als einfach symmetrisch verschlüsselter Akten- und Kontextschlüssel (siehe gemSpec_SGD_ePA#Tab_erste_Verschlüsselungsschicht)
2. Entschlüsseln mit symmetrischem Schlüssel von SGD 1 durch Aufruf von TUC_KON_076	Eingangsdaten: • encryptedData = `phrs:EncryptedKeyContainer\phrs:Ciphertext` aus plainData (Schritt 1) • symmetricKey = aus SGD 1 abgeleiteter symmetrischer Schlüssel • associatedData = `phrs:EncryptedKeyContainer/phrs:AssociatedData` aus plainData (Schritt 1) Ausgangsdaten: • plainData als Klartextpräsentation von Akten- und Kontextschlüssel (siehe gemSpec_SGD_ePA#Tab_Austauschformat Akten- und Kontextschlüssel)

[<=]

A_17986 - FM ePA: Schlüsselableitung bei Entschlüsselung- Abhängigkeit von der Rolle
Bei der Entschlüsselung von Akten- und Kontextschlüssel MUSS das Fachmodul ePA bei Durchführung der Schlüsselableitung die Operation KeyDerivation gemäß Anwendungsfall gemSpec_SGD_ePA#2.5,2.7,2.9 aufrufen.
[<=]

A_17993 - FM ePA: Schlüsselableitung bei Entschlüsselung - Verwendung von AssociatedData
Bei der Entschlüsselung von Akten- und Kontextschlüssel MUSS das Fachmodul ePA das Element `phrs:AuthorizationKey/phrs:EncryptedKeyContainer/phrs:AssociatedData` des ermittelten AuthorizationKey für den Aufruf der Operation KeyDerivation beim SGD wie folgt verwenden:

KeyDerivation <Teilstring aus AssociatedData als Ableitungsinformationen für den entsprechenden SGD>
[<=]

Die Ermittlung der Ableitungsinformation für SGD1 und SGD2 ist in [gemSpec_SGD_ePA#8] beschrieben.

Zur Optimierung der Performance muss das Fachmodul die Schlüsselableitung für SGD 1 (Basisablauf Schritt 1) und SGD 2 (Basisablauf Schritt 3) und das Erzeugen eines ephemeren ECDH-Schlüsselpaares (Basisablauf Schritt 5) parallel ausführen. Der Request an SGD 1 und der Request an SGD 2 in Basisablauf Schritt 7 können ebenfalls parallelisiert werden (siehe [gemSpec_SGD_ePA#A_17925]) . Die bei einer Schlüsselableitung für eine Entschlüsselung im Request für KeyDerivation zu übermittelnden Informationen werden sowohl für SGD 1 als auch SGD 2 dem Element `phrs:AuthorizationKey/phrs:EncryptedKeyContainer/phrs:AssociatedData` entnommen.

A_17736 - FM ePA: Schlüsselableitung bei Entschlüsselung - Fehler bei der Entschlüsselung
Falls der Basiskonnektor bei der Entschlüsselung von Akten- und Kontextschlüssel einen Fehler zurückgibt, MUSS das Fachmodul ePA die aufgerufene Operation mit dem Code 7400 gemäß Tab_FM_ePA_011 abbrechen.
[<=]

6.6 Logout

Das Fachmodul ePA stellt einen impliziten Logout für die Aktensession bereit, welcher nach einem Timeout bei Inaktivität bzgl. der Nutzung einer Aktensession ausgeführt wird. Es veranlasst die Löschung der zur Aktensession gehörenden Verbindungsdaten in der VAU und löscht anschließend die Aktensession. Falls noch weitere Verbindungen anderer Aktensessions in die VAU bestehen, bleiben diese aktiv (vgl. I_Document_Management_Connect::CloseContext gemäß [gemSpec_Dokumentenverwaltung]).

A_14169 - FM ePA: Logout Aktensession - Löschung der Verbindung zur VAU
Falls auf eine Aktensession länger als 20 Minuten nicht zugegriffen wird, MUSS das Fachmodul ePA die Operation I_Document_Management_Connect::CloseContext gemäß [I_Document_Management_Connect_Service.wsdl] des zugehörigen ePA-Aktensystems aufrufen.**[<=]**

A_14651 - FM ePA: Logout Aktensession - Löschung der Aktensession
Falls auf eine Aktensession länger als 20 Minuten nicht zugegriffen wird, MUSS das Fachmodul ePA die Aktensession beenden und alle dazugehörigen Daten löschen.**[<=]**

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

A_17450 - FM ePA: Logout Aktensession - Unterbindung der Erneuerung der AuthenticationAssertion
~~Falls eine Aktensession beendet wird, MUSS das Fachmodul ePA die Operation AuthInsurantService::LogoutToken der Komponenten Zugangsgateway aufrufen.~~
[<=]

A_17450-01 - FM ePA: Logout Aktensession - Unterbindung der Erneuerung der AuthenticationAssertion
Falls eine Aktensession der eGK beendet wird, MUSS das Fachmodul ePA die Operation AuthInsurantService::LogoutToken der Komponenten Zugangsgateway aufrufen. **[<=]**

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

A_17451 - FM ePA: Logout Aktensession - Unterbindung der Erneuerung der AuthenticationAssertion - Fehler
Falls die Operation AuthInsurantService::LogoutToken gemäß [gemSpec_Authentisierung_Vers] einen Fehler zurückgibt, MUSS das Fachmodul ePA diesen Fehler im Sicherheitsprotokoll eintragen.

[<=]

A_17142 - FM ePA: Logout Aktensession - Löschung der Verbindung zur VAU - Fehler
Falls die Operation I_Document_Management_Connect::CloseContext einen Fehler zurückgibt, MUSS das Fachmodul ePA diesen Fehler im Sicherheitsprotokoll eintragen.
[<=]

6.7 Datenschutz und Sicherheitsaspekte

A_14173 - FM ePA: Sicherheit - Keine persistente Speicherung von personenbezogenen Daten
Das Fachmodul ePA DARF personenbezogene Daten NICHT persistent speichern.**[<=]**

A_14722 - FM ePA: Sicherheit - Keine persistente Speicherung von Dokumenten und Metadaten
Das Fachmodul ePA DARF Dokumente und Metadaten der Patientenakte NICHT persistent speichern.**[<=]**

A_14174 - FM ePA: Sicherheit - Keine Speicherung von privaten Schlüsseln
Das Fachmodul ePA DARF symmetrische und private asymmetrische Schlüssel (z.B. Dokumentenschlüssel, Aktenschlüssel) NICHT persistent speichern.**[<=]**

A_14175 - FM ePA: Sicherheit - Keine Weitergabe vertraulicher Informationsobjekte an das PS
Das Fachmodul ePA DARF Schlüsselmaterial und Daten der Aktensession NICHT an das PS weitergegeben.**[<=]**

Regelungen aus [gemSpec_Krypt]

Für die Erzeugung von Schlüsselmaterial gilt übergreifend [gemSpec_Krypt#GS-A_4368].

Regelungen für TLS-Verbindungen

Für TLS-Verbindungen gelten die Regelungen aus [gemSpec_Krypt#3.3.2].

6.8 Verwendung des Dienstverzeichnisdienstes

A_13828 - FM ePA: Service-Informationen für Dienstverzeichnisdienste
Während der Bootup-Phase des Konnektors MUSS das Fachmodul ePA die in Tab_FM_ePA_007 gemäß dem XML-Schema [ServiceInformation.xsd] definierten Services in den Dienstverzeichnisdienst des Konnektors [gemSpec_Kon#4.1.3] einbringen.

Tabelle 11: 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/Versions /Version/@TargetNamespace	aktueller Namensraumbezeichner gemäß Tab_FM_ePA_005	aktueller Namensraumbezeichner gemäß Tab_FM_ePA_003
ServiceInformation/Service/Versions /Version/@Version	aktuelle Versionsnummer gemäß Tab_FM_ePA_005	aktuelle Versionsnummer gemäß Tab_FM_ePA_003
ServiceInformation/Service/Versions /Version/Abstract	Initiale Version	Initiale Version
ServiceInformation/Service/Versions /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/Versions /Version/EndpointTLS/@Location	Absoluter URL des über HTTP Secure (HTTPS) erreichbaren Dienstes	Absoluter URL des über HTTP Secure (HTTPS) erreichbaren Dienstes
ServiceInformation/Service/Versions /Version/WSDL/@Location	<leer>	<leer>

[<=]

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 Webservers. 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 12: 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

[<=]

A_17229 - FM ePA: Fachmodulprotokoll (Debug)

~~Das Fachmodul ePA MUSS für Testzwecke im Fachmodulprotokoll Debug-Einträge mit mindestens den folgenden Parametern erfassen:~~

Tabelle 13: Tab_FM_ePA_015 Parameter des Debug-Protokolls

~~Feld~~	~~Beschreibung~~
~~eventType~~	~~„Op“~~
~~Schwere~~	~~„Debug“~~

[<=]

A_17229-01 - FM ePA: Fachmodulprotokoll (Debug)

~~Das Fachmodul ePA MUSS~~ Falls nicht im Produktivbetrieb laufend, KANN das Fachmodul ePA für Testzwecke im Fachmodulprotokoll Debug-Einträge mit mindestens den folgenden Parametern erfassen:

Tabelle 14: Tab_FM_ePA_015 Parameter des Debug-Protokolls

Feld	Beschreibung
eventType	„Op“
Schwere	„Debug“

[<=]

A_17230 - FM ePA: Sicherheitsprotokoll
Das Fachmodul ePA MUSS sicherheitsrelevante Fehler und Ereignisse über den Protokollierungsdienst des Konnektors im Sicherheitsprotokoll des Konnektors mindestens mit den folgenden Parametern erfassen:

Tabelle 15: 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

[<=]

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 16: 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

[<=]

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 17: 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

[<=]

Die Einsicht von Protokolldateien und Administration der Konfigurationsparameter erfolgen über die Managementschnittstelle des Konnektors (vgl. [gemSpec_Kon#4.3.4]).

6.11 Fehlerbehandlung und Fehlermeldungen

Fehlerkonzept

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

Die Methodik in diesem Dokument sieht in diesem Kapitel eine übergreifende Behandlung der Fehler vor, falls alle Anfragen an das ePA-Aktensystem oder seine Komponenten, die zwingend zur Durchführung einer Operation oder Funktionalität benötigt werden, fehlschlagen. Diese Anforderungen greifen also auch, falls nur die

Kommunikation mit einem einzigen ePA-Aktensystem notwendig ist. Alle weiteren Situationen werden jeweils in den Unterkapiteln der Operationen behandelt. Falls unterschiedliche Probleme innerhalb einer Operation auftreten, liefert diese Operation dann ggfs. einen allgemeinen Fehler an das aufrufende System zurück, da eine Differenzierung der Fehlersituationen schnell unübersichtlich und für den Nutzer nicht hilfreich ist. Jeder Fehlercode wird dann aber im Fachmodulprotokoll abgelegt und erlaubt so eine genaue Analyse.

Übergreifende Festlegungen zu Fehlermeldungen

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

Für das Fehlermanagement gelten neben den hier aufgeführten spezifischen Anforderungen die Anforderungen aus Kapitel 3 der übergreifenden Spezifikation [gemSpec_OM#3].

A_14405 - FM ePA: Übergreifende Anforderung - Fehlermeldungen des Webservice PHRManagementService (SOAP-Fault)
Das Fachmodul ePA MUSS Fehler, die bei Operationen des Webservice PHRManagementService auftreten, mittels gematik-SOAP-Fault an das aufrufende System melden.**[<=]**

Details zu gematik-SOAP-Faults finden sich in [gemSpec_OM#3.2.3]. Der Code 7400 wird für Fehlerfälle verwendet, die technisch bedingt sind und durch den Nutzer nicht behoben werden können. Diese Fehlerfälle erfordern eine Analyse und Behebung durch 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 18: 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
7210	Technical	ERROR	Die Berechtigung kann nicht hinterlegt werden.
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 Schlüsselmaterial 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 19: 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

Tabelle 20: 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

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

Tabelle 21: Tab_FM_ePA_004 Schnittstellenübersicht des Fachmoduls ePA

Schnittstelle	**Beschreibung und Operationen**	
PHRService	IHE-Schnittstelle zur Dokumentenverwaltung	
	Logische Operation	**Beschreibung**
	putDocuments	Dokumente einstellen
	find	Dokumente suchen
	getDocuments	Dokumente herunterladen
	removeDocuments	Dokumente löschen
	updateDocumentSet	Metadaten von Dokumenten ändern
PHRManagementService	Schnittstelle zur Aktivierung und Rechtevergabe	
	Logische Operation	**Beschreibung**
	ActivateAccount	Aktivierung eines Aktenkontos
	RequestFacilityAuthorization	Berechtigungsvergabe für eine LEI
	GetHomeCommunityID	Identifizierung eines ePA-Aktensystems
	GetAuthorizationList	Abruf aller Berechtigungen einer LEI

Die Operationen von PHRService erlauben das Einstellen, Suchen, Herunterladen und Löschen von Dokumenten sowie die Aktualisierung von Metadaten. Die zum Aufruf benötigte HomeCommunity als Teil des RecordIdentifiers können Primärsysteme über die Operation GetHomeCommunityID des Webservices PHRManagementService beziehen. Dieser Webservice erlaubt es außerdem einem Versicherten, in der LE-Umgebung sein Aktenkonto zu aktivieren und eine Leistungserbringerinstitution ad-hoc zu berechtigen

(Operation RequestFacilityAuthorization). Eine LEI kann ihre Berechtigungen für Aktenkonten abrufen und aktualisieren~~, sowie die alternativen Versichertenidentitäten der Versicherten berechtigen.~~

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

7.1 PHRService

Der Webservice PHRService setzt die logische Schnittstelle I_PHR_Management gemäß [gemSysL_ePA] um.

A_14373 - FM ePA: PHRService
Das Fachmodul ePA MUSS für Primärsysteme den Webservice PHRService gemäß Tabelle Tab_FM_ePA_005 anbieten.

Tabelle 22: Tab_FM_ePA_005 Beschreibung des Webservices PHRService

Name	**PHRService**	
Version	1.0.0	
SOAP-Header	**Name**	**Inhalt**
	MandantID	MandantID gemäß [ConnectorContext.xsd]
	ClientSystemID	ClientSystemID gemäß [ConnectorContext.xsd]
	WorkplaceID	WorkplaceID gemäß [ConnectorContext.xsd]
	RecordIdentifier	`RecordIdentifier` gemäß [gemSpec_DM_ePA#2.2]
Namensraum	urn:ihe:iti:xds-b:2007	
Abkürzung Namensraum	ihe	
Operationen	**Name (logisch)**	**IHE-Umsetzung der Schnittstelle**
	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
	updateDocumentSet	[ITI-92] "Restricted Update Document Set" als Akteur "RMU Update Responder" gemäß RMU mit der Option "Forward"
WSDL	**PHRService.wsdl**	

[<=]

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 - FM ePA: PHRService - Fehlermeldungen gemäß IHE-Mapping
~~Der Webservice PHRService MUSS alle Fehler aus Tab_FM_ePA_011 als IHE-Fehler nach Tab_FM_ePA_012 abbilden und in der IHE-Response eingebettet an das aufrufende System zurückgeben.~~

Tabelle 23: 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~~
~~*Keine Entsprechung*~~	~~location~~

[<=]

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 24: 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
Keine Entsprechung	location

[<=]

A_14874 - FM ePA: PHRService - Mapping für Fehlerkategorie "Fatal"
Der Webservice PHRService MUSS den gematik-Fehlerwert "Fatal" im Feld "Severity" für IHE auf den Wert "Error" in "severity" abbilden.**[<=]**

7.1.1 Definition/Signatur

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

7.1.1.1 putDocuments

Tabelle 25: Tab_FM_ePA_006 Beschreibung und Parameter der Operation putDocuments

Name	**putDocuments**	
Beschreibung	Diese Operation ermöglicht Primärsystemen das Einstellen von Dokumenten in das ePA-Aktensystem.	
Aufrufparameter	**Name**	**Beschreibung**
	ProvideAndRegisterDocumentSetRequest	Der Parameter enthält die zu speichernden XDS-Dokumente und SubmissionSets inklusive Metadaten gemäß [PHRService.wsdl].
Rückgabeparameter	**Name**	**Beschreibung**

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

Fehlermeldungen

Die Operation putDocuments kann folgende Fehlermeldungen zurückliefern:

- 7200, 7202, 7205, 7206, 7209, 7211, 7212, 7214, 7215, 7220, 7221, 7400, 7403, 7404, 7406 gemäß Tab_FM_ePA_011
- 4000 gemäß Tab_FM_ePA_050
- 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 26: Tab_FM_ePA_013 Beschreibung und Parameter der Operation find (Semantik)

Name	**find**	
Beschreibung	Diese Operation ermöglicht Primärsystemen das Suchen von Dokumenten und SubmissionSets im ePA-Aktensystem.	
Aufrufparameter	**Name**	**Beschreibung**
	AdhocQueryRequest	Der Parameter enthält die gewünschte Suchanfrage ("Stored Query") inklusive Parametern gemäß [PHRService.wsdl].
Rückgabeparameter	**Name**	**Beschreibung**
	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 27: Tab_FM_ePA_027 Beschreibung und Parameter der Operation getDocuments (Semantik)

Name	**getDocuments**	
Beschreibung	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].

Fehlermeldungen

Die Operation getDocuments kann folgende Fehlermeldungen zurückliefern:

- 7200, 7202,7205, 7206, , 7209, 7211, 7212, 7214, 7215, 7220, 7221, 7400, 7403, 7404, 7406 gemäß Tab_FM_ePA_011
- 4000 gemäß Tab_FM_ePA_050
- reguläre bei IHE für [ITI-43] und [ITI-80] definierte Fehlermeldungen

7.1.1.4 removeDocuments

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

Tabelle 28: Tab_FM_ePA_029 Beschreibung und Parameter der Operation 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].

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

Fehlermeldungen

Die Operation removeDocuments 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-86] definierte Fehlermeldungen

7.1.1.5 updateDocumentSet

Die Operation updateDocumentSet ermöglicht Primärsystemen, Metadaten bestehender Dokumente zu ändern.

Tabelle 29: Tab_FM_ePA_031 Beschreibung und Parameter der Operation 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 Parameter enthält die angefragten Dokumente oder Fehler, falls ein oder mehrere Dokumente nicht abgerufen werden konnten gemäß [PHRService.wsdl].

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

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.**[<=]**

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.**[<=]**

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 - 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 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.**[<=]**

7.1.2.1 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.**[<=]**

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

Dokumentenverschlüsselung

A_13907 - FM ePA: putDocuments - Verschlüsselung der Dokumente
Die Operation putDocuments MUSS jedes in der Nachricht übertragene Dokument vor der Weiterleitung an das ePA-Aktensystem durch eine Datenstruktur gemäß [gemSpec_DM_ePA#2.4] ersetzen.**[<=]**

A_18008 - FM ePA: putDocuments - Verschlüsselung der Dokumente mit Verschlüsselungsdienst
Bei der Verschlüsselung des Dokuments MUSS die Operation putDocuments das Dokument und den Dokumentenschlüssel wie folgt verschlüsseln:

Dokument mit TUC_KON_075 verschlüsseln	Eingangsdaten: • dataToBeEncrypted = Dokument Rückgabedaten: • encryptedData (verschlüsseltes Dokument) • symmetricKey (Dokumentenschlüssel) Der optionale Parameter AD wird nicht verwendet.
Dokumentenschlüssel mit TUC_KON_075 verschlüsseln	Eingangsdaten: • dataToBeEncrypted = Dokumentenschlüssel • symmetricKey = Aktenschlüssel aus Session-Daten Rückgabedaten: • encryptedData (verschlüsselter Dokumentenschlüssel) Der optionale Parameter AD wird nicht verwendet.

[<=]

A_13903 - FM ePA: putDocuments - Löschen der Dokumentenschlüssel
Die Operation putDocuments MUSS alle Dokumentenschlüssel nach ihrer Verschlüsselung mit dem Aktenschlüssel löschen.**[<=]**

7.1.2.2 find

Das Fachmodul ePA muss eine find-Anfrage, sofern sie den Anforderungen aus Kapitel 7.1.1.2 genügt, anschließend an das ePA-Aktensystem weiterleiten. Das Fachmodul ePA agiert dabei als XCA "Initiating Gateway", während das ePA-Aktensystem ein XCA-„Responding Gateway“ umsetzt (siehe Operation I_Document_Management::CrossGatewayQuery gemäß [gemSpec_Dokumentenverwaltung]). Die Antworten nehmen den umgekehrten Weg.

A_15765 - FM ePA: PHR_Service: Weiterleiten einer find-Anfrage
Das Fachmodul ePA MUSS jede Operation find an das Dokumentenverwaltungssystem über die Schnittstelle I_Document_Management::CrossGatewayQuery gemäß [ITI-38] "Cross-Gateway Query" als IHE-XCA-Akteur „Initiating Gateway“ weiterleiten.**[<=]**

A_15766 - FM ePA: PHR_Service: Weiterleiten von find-Antworten
Das Fachmodul ePA MUSS die Antwort der Dokumentenverwaltung auf eine I_PHR_Management::find-Anfrage des Fachmoduls gemäß [ITI-38] "Cross-Gateway Query" als IHE-XCA-Akteur „Initiating Gateway“ an das Primärsystem weiterleiten.**[<=]**

7.1.2.3 getDocuments

Das Fachmodul ePA muss eine eingehende Primärsystemanfrage, sofern sie den Anforderungen aus Kapitel 7.1.1.3 genügt, anschließend an das ePA-Aktensystem weiterleiten. Das Fachmodul ePA agiert dabei als XCA "Initiating Gateway", während das ePA-Aktensystem ein XCA-„Responding Gateway“ umsetzt (siehe Operation I_Document_Management::CrossGatewayRetrieve in [gemSpec_Dokumentenverwaltung]).

A_15767 - Weiterleiten einer getDocuments-Anfrage an das ePA-Aktensystem
Das Fachmodul ePA MUSS jede Operation getDocuments an das Dokumentenverwaltungssystem über die Operation I_Document_Management::CrossGatewayRetrieve gemäß [ITI-39] "Cross-Gateway Retrieve" als IHE-XCA-Akteur „Initiating Gateway“ weiterleiten.**[<=]**

A_15768 - FM ePA: PHR_Service: Weiterleiten von getDocuments-Antworten
Das Fachmodul ePA MUSS die Antwort der Dokumentenverwaltung auf eine Anfrage des Fachmoduls gemäß [ITI-39] "Cross-Gateway Retrieve" als IHE-XCA-Akteur „Initiating Gateway“ an das Primärsystem weiterleiten.**[<=]**

Dokumentenentschlüsselung

A_14700 - FM ePA:getDocuments - Entschlüsselung der Dokumente
Die Operation getDocuments MUSS jedes übertragene Dokument (Datenstruktur gemäß A_14977) vor der Weiterleitung an das Primärsystem durch das jeweilige entschlüsselte Dokument (Ergebnis aus A_18009) ersetzen.

[<=]

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	Eingangsdaten: • encryptedData = verschlüsselter Dokumentenschlüssel aus `EncryptedData\EncryptedKey\CipherData` • symmetricKey = Aktenschlüssel (RecordKey) aus Session-Daten Rückgabedaten: • plainData (entschlüsselter Dokumentenschlüssel) Der optionale Parameter AD wird nicht verwendet.
Dokument mit TUC_KON_076 entschlüsseln	Eingangsdaten: • encryptedData (verschlüsseltes Dokument aus `EncryptedData\CipherData`) • symmetricKey (Dokumentenschlüssel) Rückgabedaten: • plainData (entschlüsseltes Dokument Der optioanle Parameter AD wird nicht verwendet.

[<=]

A_14959 - FM ePA: getDocuments - Löschen der Dokumentenschlüssel
Die Operation getDocuments MUSS Dokumentenschlüssel nach ihrer Verwendung zur Entschlüsselung eines Dokuments löschen.
[<=]

7.1.2.4 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.**[**<=**]**

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.**[**<=**]**

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

7.1.2.5 updateDocumentSet

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: PHRService - Gruppierung für updateDocumentSet
Die Operation updateDocumentSet MUSS die IHE-Akteure RMU Update Responder und RMU Update Initiator (beide gemäß [IHE-ITI-RMU]) gruppieren.**[**<=**]**

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.**[**<=**]**

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.**[**<=**]**

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.

7.2 PHRManagementService

Der Webservice PHRManagementService setzt die logischen Schnittstellen I_Account_Administration und I_Authorization_Administration gemäß [gemSysL_ePA] um.

A_13818 - FM ePA: PHRManagementService
Das Fachmodul ePA MUSS für Primärsysteme den Webservice PHRManagementService gemäß Tabelle Tab_FM_ePA_003 anbieten.

Tabelle 30: Tab_FM_ePA_003 Beschreibung des Webservices PHRManagementService

Name	**PHRManagementService**	
Version	1.0.0	
Namensraum	http://ws.gematik.de/conn/WSDL/PHRManagementService/v1.0	
Abkürzung Namensraum	phr_management	
Operationen	**Name**	**Beschreibung**
	ActivateAccount	Aktivierung eines Aktenkontos
	RequestFacilityAuthorization	Berechtigungsvergabe für eine LEI
	GetHomeCommunityID	Identifizierung eines ePA-Aktensystems
	GetAuthorizationList	Abruf aller Berechtigungen einer LEI
WSDL	**PHRManagementService.wsdl**	

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_13818-01 - FM ePA: PHRManagementService
Das Fachmodul ePA MUSS für Primärsysteme den Webservice PHRManagementService gemäß Tabelle Tab_FM_ePA_003 anbieten.

Tabelle 31: Tab_FM_ePA_003 Beschreibung des Webservices PHRManagementService

Name	**PHRManagementService**	
Version	1.2.0 ~~1.0.0~~	
Namensraum	http://ws.gematik.de/conn/WSDL/PHRManagementService/v1.2 ~~http://ws.gematik.de/conn/WSDL/PHRManagementService/v1.0~~	
Abkürzung Namensraum	phr_management	
Operationen	**Name**	**Beschreibung**
	ActivateAccount	Aktivierung eines Aktenkontos
	RequestFacilityAuthorization	Berechtigungsvergabe für eine LEI
	GetHomeCommunityID	Identifizierung eines ePA-Aktensystems
	GetAuthorizationList	Abruf aller Berechtigungen einer LEI
WSDL	**PHRManagementService.wsdl**	

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.

7.2.1.1 ActivateAccount

Tabelle 32: Tab_FM_ePA_016 Beschreibung und Parameter der Operation ActivateAccount (Semantik)

Name	**ActivateAccount**
Beschreibung	Mit dieser Operation startet das Primärsystem die Aktivierung des beantragten Aktenkontos des Versicherten bei seinem Anbieter

	ePA-Aktensystem. Mithilfe des `RecordIdentifier` und der darin enthaltenen HomeCommunityID des Anbieters ePA-Aktensystem wird das Aktenkonto des Versicherten lokalisiert. Als Ergebnis der Operation wird die Zugriffsberechtigung für den Versicherten im ePA-Aktensystem hinterlegt.	
Aufrufparameter	**Name**	**Beschreibung**
	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]
Rückgabeparameter	**Name**	**Beschreibung**
	Status	Status nach [gemSpec_Kon#3.5.2]

Die Operation ActivateAccount kann folgende Fehlermeldungen zurückliefern:

- 7200, 7202, 7203, 7205, 7206, 7207, 7213, 7215, 7220, 7400, 7402, 7403, 7404, 7405, 7406 gemäß Tab_FM_ePA_011
- Fehlermeldungen gemäß Tab_FM_ePA_050
- Fehlermeldungen gemäß Tab_FM_ePA_051

7.2.1.2 RequestFacilityAuthorization

Tabelle 33: Tab_FM_ePA_020 Beschreibung und Parameter der Operation RequestFacilityAuthorization (Semantik)

Name	**RequestFacilityAuthorization**	
Beschreibung	Die Operation startet den Autorisierungsprozess zur Berechtigungsvergabe für die Leistungserbringerinstitution in dem über `RecordIdentifier` referenzierten Aktenkonto des Versicherten. Die Berechtigung der Leistungserbringerinstitution erfolgt für eine vom Primärsystem angegebene AuthorizationConfiguration. Das Fachmodul ePA stellt die AuthorizationConfiguration 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	`RecordIdentifier` gemäß [gemSpec_DM_ePA#2.2]
	OrganizationName	Name der Leistungserbringerinstitution
	InsurantName	Name des Versicherten des durch RecordIdentifier referenzierten Aktenkontos
Rückgabeparameter	**Name**	**Beschreibung**
	Status	Status nach [gemSpec_Kon#3.5.2]

Die Operation RequestFacilityAuthorization kann folgende Fehlermeldungen zurückliefern:

- 7200, 7202, 7203, 7205, 7206, 7207, 7213, 7214, 7215, 7217, 7220, 7400, 7403, 7404 gemäß Tab_FM_ePA_011
- Fehlermeldungen gemäß Tab_FM_ePA_050
- Fehlermeldungen gemäß Tab_FM_ePA_051

7.2.1.3 GetHomeCommunityID

Tabelle 34: Tab_FM_ePA_039 Beschreibung und Parameter der Operation GetHomeCommunityID (Semantik)

Name	GetHomeCommunityID	
Beschreibung	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 I_Authorization_Management::checkRecordExists auf. Der zurückgegebene Parameter HomeCommunityID enthält die OID des ePA-Aktenanbieters und ist Teil des `RecordIdentifiers` , den Primärsysteme zum Aufruf weiterer Operationen des Fachmoduls ePA benötigen.	
Aufrufparameter	**Name**	**Beschreibung**

	Context	Aufrufkontext gemäß [ConnectorContext.xsd]
	InsurantID	Unveränderlicher Teil der Krankenversichertennummer nach [gemSpec_DM_ePA#2.2]
Rückgabeparameter	**Name**	**Beschreibung**
	HomeCommunityID	OID des ePA-Aktensystems gemäß [gemSpec_DM_ePA]
	Status	Status gemäß [gemSpec_Kon#3.5.2]

Die Operation GetHomeCommunityID kann folgende Fehlermeldungen zurückliefern:

- 7200, 7202, 7206, 7220, 7400 gemäß Tab_FM_ePA_011
- 4000 gemäß Tab_FM_ePA_050
- Fehlermeldungen gemäß Tab_FM_ePA_032

Tabelle 35: 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.

7.2.1.4 GetAuthorizationList

Tabelle 36: Tab_FM_ePA_040 Beschreibung und Parameter der Operation 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]

Die Operation GetAuthorizationList kann folgende Fehlermeldungen zurückliefern:

- 7200, 7202, 7205, 7206, 7214, 7220, 7221, 7400 gemäß Tab_FM_ePA_011
- 4000 gemäß Tab_FM_ePA_050
- Fehlermeldungen gemäß Tab_FM_ePA_041

Tabelle 37: 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.

7.2.2 Umsetzung

Authentisierung gegenüber dem Aktensystem

A_15192 - FM ePA: PHRManagementService - Authentisierung mittels eGK
Der Webservice PHRManagementService MUSS sich zur Durchführung der Operationen ActivateAccount und RequestFacilityAuthorization mit der in den Aufrufparametern referenzierten eGK gegenüber dem Aktensystem authentisieren.**[<=]**

A_15193 - FM ePA: PHRManagementService - Authentisierung mittels SM-B
Der Webservice PHRManagementService MUSS sich zur Durchführung der Operation GetAuthorizationList mit einem über Aufrufkontext ausgewählten SM-B gegenüber dem Aktensystem authentisieren.
[<=]

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

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

Übergreifende Regelungen für PHRManagementService

A_14266 - FM ePA: PHRManagementService – Befüllung des Rückgabeparameters Status
Das Fachmodul ePA MUSS bei jeder erfolgreich durchlaufenen Operation von PHRManagementService den Parameter Status im Element Status/Result mit „OK“ befüllen (vgl. [ConnectorCommon.xsd]).
[<=]

A_17121 - FM ePA: PHRManagementService - Berechtigung in Komponente Autorisierung - Fehler
Falls die Operation I_Authorization_Management::putAuthorizationKey einen Fehler zurückgibt, MUSS der Webservice PHRManagementService die aufgerufene Operation mit dem Code 7400 gemäß Tab_FM_ePA_011 abbrechen.**[<=]**

Fehlerrückgaben der Operation I_Authorization_Management::putAuthorizationKey werden in [gemSpec_Autorisierung] spezifiziert.

7.2.2.1 ActivateAccount

Der Ablauf der Operation ActivateAccount ist in [gemSysL_ePA#3.5.1] beschrieben und gliedert sich in die folgenden Schritte:

1. Prüfung der Parameter und des Sperrstatus der eGK
2. Login des Versicherten mit der eGK
3. Schlüsselmaterial erzeugen und verschlüsseln
4. Hinterlegen des verschlüsselten Schlüsselmaterials für den Versicherten in der Komponente Autorisierung

Authentisierung des Versicherten gegenüber dem Aktensystem

Die Authentisierung gegenüber einem Aktensystem erfolgt gemäß A_15192 mit der eGK. Der vollständige Login-Prozess ist in Kapitel 6.5 Login beschrieben.

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.
[<=]

Schlüsselableitung und ~~Ent~~Verschlüsselung von Akten- und Kontextschlüssel

Das Chiffrat 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 Chiffrats benötigten zwei AES-256-Schlüssel ruft das Fachmodul ePA von den SGDs 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.

[<=]

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 Chiffrat und AssociatedData (aus den Antwortnachrichten der SGDs) als EncryptedKeyContainer gemäß [gemSpec_SGD_ePA#8]
  - validTo: aktuelles Datum
  - actorID: Versicherten-ID der eGK
  - AuthorizationType: DOCUMENT_AUTHORIZATION

[<=]

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 38: 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

[<=]

7.2.2.2 RequestFacilityAuthorization

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 - 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 39: 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	`Schritt 5: Aktenzugriff`

[<=]

A_16212 - 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 40: 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•`***0x0B***
`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: 01.08.2019`	`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 die Berechtigung, auf die Dokumente des Versicherten und von Leistungserbringern gemäß [gemSpec_Dokumentenverwaltung#5.3] zuzugreifen.

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 zu einer Ausgabeoperation gemeint. Die Nummerierung zu Beginn der Anzeige mit "1:" bis "4:" wird dann angepasst und erfolgt fortlaufend bei "1:" beginnend. Der Ausgabetext "Es folgen 4 Anzeigen ..." wird entsprechend angepasst.Der Parameter "Anw" für Terminalanzeigen gemäß Tab_FM_ePA_019 wird entsprechend angepasst.

[<=]

A_16218 - FM ePA: RequestFacilityAuthorization - Anzeige am Kartenterminal - Nutzerinteraktion
Die Operation RequestFacilityAuthorization MUSS eine Ausgabe (entspricht einer Zeile in Tab_FM_ePA_025) am Kartenterminal solange anzeigen bis eine Nutzereingabe die Anzeige bestätigt, abbricht oder ein Timeout wegen fehlender Nutzereingabe erfolgt.
[<=]

A_16214 - FM ePA: RequestFacilityAuthorization - Anzeige am Kartenterminal - Bestätigung
Falls eine Ausgabe (entspricht einer Zeile in Tab_FM_ePA_025) am Kartenterminal bestätigt wird, MUSS die Operation RequestFacilityAuthorization die nächste Ausgabe am Kartenterminal gemäß Tab_FM_ePA_025 anzeigen.
[<=]

A_16215 - FM ePA: RequestFacilityAuthorization - Anzeige am Kartenterminal - Abbruch
Falls eine Ausgabe Tab_FM_ePA_025 am Kartenterminal abgebrochen wird (Abbruchtaste wurde gedrückt oder Timeout), MUSS die Operation RequestFacilityAuthorization die Operation mit Code 7217 abbrechen.
[<=]

A_18182 - FM ePA: RequestFacilityAuthorization - Anzeige am Kartenterminal - wiederholte PIN-Eingabe
Falls eine erfolgte PIN-Eingabe den Fehler REJECTED zurückliefert, MUSS die Operation RequestFacilityAuthorization unmittelbar daran anschließend eine erneute PIN-Abfrage gemäß A_14769 und A_16216 durchführen, d.h. die Schritte 1-4 zur Anzeige am Kartenterminal werden hierbei nicht durchgeführt.**[<=]**

Login am ePA-Aktensystem (Authentisierung und Autorisierung)

Die Authentisierung gegenüber einem Aktensystem erfolgt gemäß A_15192 mit der eGK. Der vollständige Login-Prozess ist in Kapitel 6.5 Login beschrieben. Dabei ist es unerheblich, ob es sich um den Versicherten als Eigentümer der Akte handelt oder ob der Versicherte in der Rolle des Vertreters agiert. In beiden Fällen wird für den Versicherten die Authentisierung und Autorisierung mit seiner eGK durchgeführt.

Verbindung zur Dokumentenverwaltung

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

Kontoaktivierung falls erforderlich

Bevor die Berechtigung für die Telematik-ID in der Komponente Autorisierung hinterlegt wird, wird für den Fall, dass das Aktenkonto noch nicht aktiviert wurde, die Operation 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. Beide Schlüssel werden mit AES-Schlüsseln, die von SGD 1 und 2 abgerufen werden, verschlüsselt und mittels I_Authorization_Management::putAuthorizationKey in die Komponente Autorisierung eingebracht.

A_17988 - FM ePA: RequestFacilityAuthorization - Schlüsselableitung in Abhängigkeit von der Rolle
Für die Verschlüsselung von Akten- und Kontextschlüssel MUSS das Fachmodul ePA bei Durchführung der Schlüsselableitung die Rolle des Berechtigenden bestimmen und die Operation KeyDerivation gemäß Anwendungsfall folgender Tabelle aufrufen:

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	gemSpec_SGD_ePA#2.6
eGK	Vertreter: unveränderlicher Teil der KVNR aus Zertifikat C.AUT der eGK entspricht nicht KVNR aus Parameter RecordIdentifier der aufrufenden Operation	gemSpec_SGD_ePA#2.8

[<=]

A_17868 - FM ePA: RequestFacilityAuthorization - Akten- und Kontextschlüssel mit eGK verschlüsseln
Die Operation RequestFacilityAuthorization MUSS die beiden zur Verschlüsselung notwendigen AES-Schlüssel abrufen und Akten- und Kontextschlüssel gemäß [gemSpec_Krypt#A_17872] und [gemSpec_SGD_ePA#8] verschlüsseln.
[<=]

A_14829 - FM ePA: RequestFacilityAuthorization - Hinterlegen des verschlüsselten Schlüsselmaterials in der Komponente Autorisierung
Die Operation RequestFacilityAuthorization MUSS zur Hinterlegung der Berechtigung in der Komponente Autorisierung die Operation I_Authorization_Management::putAuthorizationKey mit folgenden Parametern aufrufen:

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

[<=]

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

Berechtigung der LEI in die Dokumentenverwaltung einbringen

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

Die Nutzungsvorgaben für XDS-Metadaten bei Policy Documents sind in [gemSpec_DM_ePA#2.1.4.2] beschrieben.

Die Nutzungsvorgaben zum Inhalt eines Policy Documents zur Berechtigung einer Leistungserbringerinstitution werden durch die Anforderung A_15442 in [gemSpec_Dokumentenverwaltung] geregelt.

A_15693 - FM ePA: RequestFacilityAuthorization - Erstellung von Policy Document
Die Operation RequestFacilityAuthorization 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_300 in Anhang B (Base Policy)] erstellen und die Werte unter Berücksichtigung von Tab_FM_ePA_023 belegen:

Tabelle 41: Tab_FM_ePA_023 Base Policy Belegung

Element-, Attribut- oder Textknoten gemäß [XACML] von Base Policy	Wert	
/PolicySet/Target/Subjects/Subject[1]/SubjectMatch/ AttributeValue/InstanceIdentifier/@extension	Telematik-ID des zum Aufrufkontext ausgewählten SM-B	
/PolicySet/Target/Subjects/Subject[2]/SubjectMatch/ 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 Tab_Dokv_300	
/PolicySet/ ...	Es werden je nach Berechtigung zwischen 1 und 3 Elementen PolicySetIdReference unter dem Element PolicySet eingefügt, d.h., falls ein Flag im Aufrufparameter AuthorizationConfiguration gesetzt ist, wird ein Element mit dem Text (Policy Set ID) erstellt.	
	Flag	**Text (Policy Set ID)**
	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_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.
[<=]

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.
[<=]

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.

[<=]

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

7.2.2.3 GetHomeCommunityID

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

Aufbau einer TLS-Verbindung zur Komponente Autorisierung eines ePA-Aktensystems

Gemäß A_14105 muss zur Kommunikation mit der Komponente Autorisierung eines ePA-Aktensystems eine TLS-Verbindung mit serverseitiger Authentisierung aufgebaut werden.

Abfrage der ePA-Aktensysteme

A_15228 - FM ePA: GetHomeCommunityID - Anfrage an alle bekannten ePA-Aktensysteme
Die Operation GetHomeCommunityID MUSS die Existenz eines zur Versicherten-ID passenden Aktenkontos bei den im Namensdienst der TI gelisteten ePA-Aktensystemen anfragen.
[<=]

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

A_14586 - FM ePA: GetHomeCommunityID - Schnittstelle zur Abfrage am ePA-Aktensystem
Die Operation GetHomeCommunityID MUSS die Existenz eines Aktenkontos in einem ePA-Aktensystem mit I_Authorization_Management::checkRecordExists der Komponente Autorisierung abfragen.**[<=]**

A_13786 - FM ePA: GetHomeCommunityID - Eine Akte
Falls ein ePA-Aktensystem bestimmt werden konnte, dass zu der Versicherten-ID eine Akte mit einem Status aus der Menge (ACTIVATED, REGISTERED, DISMISSED, SUSPENDED) führt, MUSS die Operation GetHomeCommunityID die HomeCommunityID dieses ePA-Aktensystems zurückgeben.

[<=]

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

Fehlerbehandlung

A_17765 - FM ePA: GetHomeCommunityID - Abfrage eines Aktenkontos nicht möglich
Falls ein Aufruf von I_Authorization_Management::checkRecordExists nicht durchgeführt werden konnte oder nicht erfolgreich war, MUSS die Operation GetHomeCommunityID die Lokalisierung des ePA-Aktenkontos weiterführen.

[<=]

A_13784 - FM ePA: GetHomeCommunityID - Keine Akte - Fehler
Falls kein ePA-Aktensystem bestimmt werden konnte, das zu einer Versicherten-ID eine Akte mit einem Status aus der Menge (ACTIVATED, REGISTERED, DISMISSED, SUSPENDED) führt, MUSS die Operation GetHomeCommunityID mit dem Code 7290 gemäß Tab_FM_ePA_032 abbrechen.

[<=]

A_13785 - FM ePA: GetHomeCommunityID - Zwei oder mehr Akten - Fehler
Falls mehr als ein ePA-Aktensystem bestimmt werden konnte, das zu einer Versicherten-ID eine Akte mit einem Status aus der Menge (ACTIVATED, REGISTERED, DISMISSED, SUSPENDED) führt, MUSS die Operation GetHomeCommunityID mit dem Code 7291 gemäß Tab_FM_ePA_032 abbrechen.

[<=]

7.2.2.4 GetAuthorizationList

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_15218). Die Berechtigungen werden für die Telematik-ID des ausgewählten SM-B ermittelt.

Aufbau einer TLS-Verbindung zur Komponente Autorisierung eines ePA-Aktensystems

Gemäß A_14105 muss zur Kommunikation mit der Komponente Autorisierung eines ePA-Aktensystems eine TLS-Verbindung mit serverseitiger Authentisierung aufgebaut werden.

Abfrage der ePA-Aktensysteme

A_17167 - FM ePA: GetAuthorizationList - Anfrage an alle bekannten ePA-Aktensysteme
Die Operation GetAuthorizationList MUSS die zum Zugriff durch eine LEI berechtigten Aktenkonten bei allen im Namensdienst der TI gelisteten ePA-Aktensystemen anfragen.
[<=]

Login an den ePA-Aktensystemen (nur Authentisierung)

Der Abruf der Berechtigungen erfordert die Authentisierung gegenüber den ePA-Aktensystemen (A_15193). Der Ablauf verläuft jeweils analog zum Login bei Aufruf einer Operation des Webservices PHRService. Eine Autorisierung und Verbindung zur Komponente Dokumentenverwaltung ist nicht notwendig.

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.

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)

[<=]

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 hingegeben deutet auf ein Problem im Konnektor hin, bedarf aber einer genaueren Analyse der Log-Dateien.

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.

[<=]

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.
[<=]

A_17175 - FM ePA: GetAuthorizationList - Abfrage berechtigter Aktenkonten - Fehler
Falls alle zur Durchführung einer Operation benötigten Aufrufe von I_Authorization_Management::getAuthorizationList einenFehler zurückgeben, MUSS das Fachmodul ePA die aufgerufene Operation mit dem Code 7400 gemäß Tab_FM_ePA_011 abbrechen.
[<=]

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

Transformation KVNR nach RecordIdentifier

A_17177 - FM ePA: GetAuthorizationList - Erstellung der RecordIdentifier
Die Operation GetAuthorizationList MUSS aus jeder über I_Authorization_Management::getAuthorizationList erhaltenen KVNR einen vollständigen RecordIdentifier gemäß [gemSpec_DM_ePA] bilden.

[<=]

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

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]

Weitere Begriffserklärungen befinden sich in [gemGlossar].

8.3 Abbildungsverzeichnis

Es konnten keine Einträge für ein Abbildungsverzeichnis gefunden werden.

8.4 Tabellenverzeichnis

Tabelle 1: Tab_FM_ePA_008 Konfigurationswerte des Fachmoduls ePA.....14

Tabelle 2: Tab_FM_ePA_053 - Übersicht der Fehlerfälle nach Status des Status eines AktenkontosTabelle 3: Tab_FM_ePA_053 - Übersicht der Fehlerfälle nach Status des Status eines Aktenkontos.....16

Tabelle 4: Tab_FM_ePA_002 Profile, Akteure und Optionen des Webservices PHRService 22

Tabelle 5: 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 26

Tabelle 6: Tab_FM_ePA_001 Daten zur Kommunikation mit den Komponenten des ePA-Aktensystems (abhängig vom Nutzer) 28

~~Tabelle 7: Tab_FM_ePA_033 Fehlermeldungen bei der Authentisierung mittels eGK~~ 32

Tabelle 8: Tab_FM_ePA_033 Fehlermeldungen bei der Authentisierung mittels eGK 33

Tabelle 9: Tab_FM_ePA_030 Authentifizierungsbestätigung erstellen....34

Tabelle 10: Tab_FM_ePA_026 Aufrufparameter der Operation I_Authorization::getAuthorizationKey 35

Tabelle 11: Tab_FM_ePA_007 Service-Informationen der Services des Fachmoduls ePA 45

Tabelle 12: Tab_FM_ePA_014 Parameter des Fehlerprotokolls 47

Tabelle 13: Tab_FM_ePA_015 Parameter des Debug-Protokolls 47

Tabelle 14: Tab_FM_ePA_015 Parameter des Debug-Protokolls 47

Tabelle 15: Tab_FM_ePA_022 Parameter des Sicherheitsprotokolls....48

Tabelle 16: Tab_FM_ePA_024 Parameter des Performanceprotokolls 48

Tabelle 17: Tab_FM_ePA_010 Übergreifende Konfigurationsparameter des Fachmodules ePA....49

Tabelle 18: Tab_FM_ePA_011 Übergreifende Fehlermeldungen des Fachmoduls ePA .51

Tabelle 19: Tab_FM_ePA_050 Wiederverwendete Fehlermeldungen aus der Konnektorspezifikation....52

Tabelle 20: Tab_FM_ePA_051 Wiederverwendete Fehlermeldungen aus der Übergreifenden Spezifikation Operations und Maintenance....52

Tabelle 21: Tab_FM_ePA_004 Schnittstellenübersicht des Fachmoduls ePA....53

Tabelle 22: Tab_FM_ePA_005 Beschreibung des Webservices PHRService....54

Tabelle 23: Tab_FM_ePA_012 Mapping von gematik-Fehlern nach IHE-Fehlern 55

Tabelle 24: Tab_FM_ePA_012 Mapping von gematik-Fehlern nach IHE-Fehlern 56

Tabelle 25: Tab_FM_ePA_006 Beschreibung und Parameter der Operation putDocuments 56

Tabelle 26: Tab_FM_ePA_013 Beschreibung und Parameter der Operation find (Semantik) 57

Tabelle 27: Tab_FM_ePA_027 Beschreibung und Parameter der Operation getDocuments (Semantik) 58

Tabelle 28: Tab_FM_ePA_029 Beschreibung und Parameter der Operation removeDocuments (Semantik)....59

Tabelle 29: Tab_FM_ePA_031 Beschreibung und Parameter der Operation updateDocumentSet (Semantik) 59

~~Tabelle 30: Tab_FM_ePA_003 Beschreibung des Webservices PHRManagementService~~ 66

Tabelle 31: Tab_FM_ePA_003 Beschreibung des Webservices PHRManagementService 67

Tabelle 32: Tab_FM_ePA_016 Beschreibung und Parameter der Operation ActivateAccount (Semantik) 67
Tabelle 33: Tab_FM_ePA_020 Beschreibung und Parameter der Operation RequestFacilityAuthorization (Semantik) 68
Tabelle 34: Tab_FM_ePA_039 Beschreibung und Parameter der Operation GetHomeCommunityID (Semantik) 69
Tabelle 35: Tab_FM_ePA_032 Fehlermeldungen der Operation GetHomeCommunityID 70
Tabelle 36: Tab_FM_ePA_040 Beschreibung und Parameter der Operation GetAuthorizationList (Semantik) 70
Tabelle 37: Tab_FM_ePA_041 Fehlermeldungen der Operation GetAuthorizationList 71
Tabelle 38: Tab_FM_ePA_021 Terminalanzeigen für PIN-Eingaben - Operation ActivateAccount 73
Tabelle 39: Tab_FM_ePA_019 Terminalanzeigen für PIN-Eingaben - Operation RequestFacilityAuthorization 74
Tabelle 40: Tab_FM_ePA_025: Operation RequestFacilityAuthorization - Ausgabetexte am Kartenterminal 75
Tabelle 41: Tab_FM_ePA_023 Base Policy Belegung 81

8.5 Referenzierte Dokumente

8.5.1 Dokumente der gematik

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

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, http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF_WhitePaper_AccessControl_2009-09-28.pdf
[IHE-ITI-APPC]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework Supplement, Advanced Patient Privacy Consents (APPC), Revision 1.2 – Trial Implementation, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_APPC.pdf
[IHE-ITI-DEN]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework Supplement, Document Encryption (DEN), Revision 1.3 – Trial Implementation, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_DEN.pdf
[IHE-ITI-RMD]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework Supplement, Remove Metadata and Documents (RMD), Revision 1.2 – Trial Implementation, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RMD.pdf
[IHE-ITI-SeR]	IHE International (2016): IHE IT Infrastructure (ITI) Technical Framework Supplement, Secure Retrieve (SeR), Trial Implementation Revision 1.3, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_SeR.pdf

[IHE_SHRD_GL]	IHE International (2018): IHE Technical Frameworks, General Introduction, Appendix D: Glossary, Revision 2.0, https://www.ihe.net/uploadedFiles/Documents/Templates/IHE_TF_GenIntro_AppD_Glossary_Rev2.0_2018-03-09.pdf
[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, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol1.pdf
[IHE-ITI-TF2a]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework, Volume 2a (ITI TF-2a) – Transactions Part A, Revision 15.0, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2a.pdf
[IHE-ITI-TF2b]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework, Volume 2b (ITI TF-2b) – Transactions Part B, Revision 15.0, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2b.pdf
[IHE-ITI-TF2x]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework, Volume 2x (ITI TF-2b) – Volume 2 Appendices, Revision 15.1, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2x.pdf
[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, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol3.pdf
[IHE-ITI-VS]	IHE Deutschland (2018): Value Sets für Aktenprojekte im deutschen Gesundheitswesen, Implementierungsleitfaden, Version 2.0, http://www.ihe-d.de/download/ihe-valuesets-v2-0/
[IHE-ITI-XCDR]	IHE International (2017): IHE IT Infrastructure (ITI) Technical Framework Supplement, Cross-Community Document Reliable Interchange (XCDR), Revision 1.4 – Trial Implementation, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_XCDR.pdf
[IHE-ITI-RMU]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework Supplement, Restricted Metadata Update (RMU), Revision 1.1 – Trial Implementation, https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_RMU.pdf
[KVNR]	Vertrauensstelle Krankenversichertennummer https://www.itsg.de/gkv-interne-services/vertrauensstelle-kvnr/
[RFC2119]	IETF (1997): Key words for use in RFCs to Indicate Requirement Levels, RFC 2119, http://tools.ietf.org/html/rfc2119
[SOAP1.2]	W3C (2007): SOAP Version 1.2 Part 1: Messaging Framework (Second Edition), https://www.w3.org/TR/soap12-part1/

[WSS-SAML]	OASIS (2006): Web Services Security: SAML Token Profile 1.1, https://www.oasis-open.org/committees/download.php/16768/wss-v1.1-spec-os-SAMLTokenProfile.pdf