

Elektronische Gesundheitskarte und Telematikinfrastuktur

Spezifikation ePA-Frontend des Versicherten

Version: 1.1.0
Revision: 108427
Stand: 15.05.2019
Status: freigegeben
Klassifizierung: öffentlich
Referenzierung: gemSpec_Frontend_Vers

Dokumentinformationen

Änderungen zur Vorversion

Einarbeitung P18.1.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
			Einarbeitung P18.1	
1.1.0 CC	01.03.19		zur Abstimmung freigegeben	gematik
			Einarbeitung Kommentierung	
1.1.0	15.05.19		freigegeben	gematik

Inhaltsverzeichnis

1	Einordnung des Dokumentes	6
1.1	Zielsetzung	6
1.2	Zielgruppe	6
1.3	Geltungsbereich	6
1.4	Abgrenzungen	6
1.5	Methodik.....	7
2	Systemüberblick	8
3	Systemkontext	9
3.1	Akteure und Rollen.....	9
3.2	Nachbarsysteme	9
3.2.1	Identität des Nutzers.....	11
4	Zerlegung des Produkttyps	12
5	Übergreifende Festlegungen	13
5.1	Datenschutz und Sicherheit.....	13
5.2	Verwendete Standards	17
5.3	Integrating the Healthcare Enterprise IHE	17
5.3.1	Policy Documents	18
5.3.2	Versichertendokumente	21
5.4	Benutzeroberfläche	21
5.4.1	Visuelle Darstellung	21
5.4.2	Benutzerführung	21
5.4.3	Dokumente	23
5.4.4	Eingabe Metadaten für einzustellende Dokumente	24
5.4.5	Konfiguration des FdV	28
6	Funktionsmerkmale	32
6.1	Allgemein	32
6.1.1	Aktensession-Verwaltung	32
6.1.2	Kommunikation mit dem ePA-Aktensystem	33
6.1.3	Sicherer Kanal zur Dokumentenverwaltung	35
6.1.4	Geräteautorisierung	36
6.1.5	Zertifikatsprüfung	36
6.1.5.1	Vertrauensanker des TI-Vertrauensraum.....	37
6.1.5.2	TSL-Behandlung.....	37
6.1.5.3	Zertifikatsprüfung von Zertifikaten der TI.....	39
6.1.5.4	Zertifikatsprüfung von Internet-Zertifikaten.....	40

6.2	Implementation ePA-Anwendungsfälle im FdV	40
6.2.1	Übergreifende Festlegungen	40
6.2.2	Fehlerbehandlung.....	42
6.2.3	Aktivitäten.....	44
6.2.3.1	<i>Authentisieren des Nutzers.....</i>	<i>44</i>
6.2.3.2	<i>Authentisierungstoken erneuern</i>	<i>45</i>
6.2.3.3	<i>Dokumentenset in Dokumentenverwaltung hochladen</i>	<i>46</i>
6.2.3.4	<i>Dokumentenset aus Dokumentenverwaltung herunterladen</i>	<i>47</i>
6.2.3.5	<i>Dokumentenset in Dokumentenverwaltung löschen</i>	<i>48</i>
6.2.3.6	<i>Suche nach Dokumenten in Dokumentenverwaltung.....</i>	<i>49</i>
6.2.3.7	<i>Vergebene Berechtigungen bestimmen.....</i>	<i>50</i>
6.2.3.8	<i>AuthorizationKey</i>	<i>51</i>
6.2.3.8.1	Struktur AuthorizationKeyType	51
6.2.3.8.2	Schlüsselableitung für Ver- und Entschlüsselung	52
6.2.3.8.3	AuthorizationKey erstellen	53
6.2.3.8.4	AuthorizationKey entschlüsseln.....	54
6.2.3.9	<i>Schlüsselmateriale aus ePA-Aktensystem laden</i>	<i>55</i>
6.2.3.10	<i>Schlüsselmateriale aller Berechtigten aus ePA-Aktensystem laden.....</i>	<i>57</i>
6.2.3.11	<i>Schlüsselmateriale im ePA-Aktensystem speichern</i>	<i>57</i>
6.2.3.12	<i>Schlüsselmateriale im ePA-Aktensystem ersetzen</i>	<i>58</i>
6.2.3.13	<i>Schlüsselmateriale im ePA-Aktensystem löschen.....</i>	<i>59</i>
6.2.3.14	<i>Leistungserbringerinstitution im Verzeichnisdienst der TI finden.....</i>	<i>59</i>
6.2.3.15	<i>Suchanfrage Verzeichnisdienst der TI</i>	<i>61</i>
6.2.3.16	<i>PIN-Eingabe für eGK durch Nutzer.....</i>	<i>62</i>
6.2.4	Nutzerzugang ePA	63
6.2.4.1	Login Aktensession	63
6.2.4.2	Logout Aktensession	69
6.2.5	Aktenkontoverwaltung	72
6.2.5.1	Aktenkonto aktivieren	72
6.2.5.2	Anbieter wechseln	74
6.2.6	Berechtigungsverwaltung und Berechtigungserhalt	81
6.2.6.1	Berechtigung für LEI vergeben	81
6.2.6.2	Vertretung einrichten	84
6.2.6.3	Berechtigung für Kostenträger vergeben	88
6.2.6.4	Vergebene Berechtigungen anzeigen.....	91
6.2.6.5	Eingerichtete Vertretungen anzeigen.....	93
6.2.6.6	Bestehende Berechtigungen verwalten	93
6.2.6.6.1	Berechtigung für LEI ändern.....	93
6.2.6.6.2	Berechtigung für LEI löschen.....	96
6.2.6.6.3	Berechtigung für Vertreter löschen	98
6.2.6.6.4	Berechtigung für Kostenträger löschen.....	99
6.2.7	Dokumentenverwaltung	101
6.2.7.1	<i>Dokumente einstellen</i>	<i>101</i>
6.2.7.2	<i>Dokumente suchen.....</i>	<i>105</i>
6.2.7.3	<i>Dokument herunterladen</i>	<i>108</i>
6.2.7.4	<i>Dokumente im Aktenkonto löschen.....</i>	<i>109</i>
6.2.8	Protokollverwaltung	111
6.2.8.1	<i>Zugriffsprotokoll einsehen.....</i>	<i>111</i>
6.2.9	Verwaltung eGK	117

6.2.9.1	<i>PIN der eGK ändern</i>	117
6.2.9.2	<i>PIN der eGK entsperren</i>	120
6.2.10	Geräteverwaltung	122
6.2.10.1	<i>Benachrichtigungsadresse für Geräteautorisierung aktualisieren</i>	122
6.3	Realisierung der Leistungen der TI-Plattform	123
6.3.1	Transportschnittstelle für Kartenkommandos	124
6.3.1.1	<i>Kartenterminals der Sicherheitsklasse 1</i>	125
6.3.1.2	<i>Kartenterminals der Sicherheitsklasse 2</i>	125
6.3.1.3	<i>Kartenterminals der Sicherheitsklasse 3</i>	126
6.3.2	Schnittstelle für PIN-Operationen und Anbindung der eGK	127
7	Informationsmodell	128
8	Verteilungssicht	131
9	Anhang A – Verzeichnisse	132
9.1	Abkürzungen	132
9.2	Glossar	133
9.3	Abbildungsverzeichnis	133
9.4	Tabellenverzeichnis	134
9.5	Referenzierte Dokumente	136
9.5.1	Dokumente der gematik	136
9.5.2	Weitere Dokumente	137

1 Einordnung des Dokumentes

1.1 Zielsetzung

Die vorliegende Spezifikation definiert die Anforderungen zu Herstellung, Test und Betrieb des Produkttyps ePA-Frontend des Versicherten.

1.2 Zielgruppe

Das Dokument richtet sich an Hersteller des Produktes vom Produkttypen ePA-Frontend des Versicherten sowie an Hersteller und Anbieter der weiteren Produkttypen der Fachanwendung ePA.

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

Im Dokument wird spezifiziert, wie Schnittstellen benutzt werden, um fachliche Anwendungsfälle umzusetzen. Die Schnittstellen selbst werden in der Spezifikation desjenigen Produkttypen beschrieben, der die Schnittstelle bereitstellt. Auf die entsprechenden Dokumente wird referenziert (siehe auch Anhang 9.5).

Die vollständige Anforderungslage für den Produkttyp ergibt sich aus weiteren Konzept- und Spezifikationsdokumenten. Diese sind in dem Produkttypsteckbrief des Produkttyps ePA-Frontend des Versicherten verzeichnet.

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.

Sie werden im Dokument wie folgt dargestellt:

<AFO-ID> - <Titel der Afo>

Text / Beschreibung

[<=]

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

Die Spezifikation der durch den Produkttyp genutzten Interfaces erfolgt in der Spezifikation des Produkttypen, welcher das Interface anbietet. Eine Übersicht befindet sich in Kapitel "3.2- Nachbarsysteme".

2 Systemüberblick

Das ePA-Frontend des Versicherten (FdV) ermöglicht es dem Versicherten, ein ePA-Aktensystem zu nutzen. Es wird in der persönlichen Umgebung des Versicherten genutzt und führt die dezentrale Fachlogik der Fachanwendung ePA aus.

3 Systemkontext

3.1 Akteure und Rollen

Im Systemkontext des FdV interagieren verschiedene Akteure (aktive Komponenten) in unterschiedlichen Rollen mit dem FdV.

Tabelle 1: TAB_FdV_101 – Akteure und Rollen

Akteur	Rolle	Beschreibung
Nutzer	Versicherter (als Aktenkontoinhaber) oder Vertreter eines Versicherten	Primärer Anwender, Ausführen von fachlichen Anwendungsfällen mit Zugriff auf ein ePA-Aktensystem
Ausführungsumgebung	Gerät des Versicherten	Betriebs-/Ablaufumgebung des FdV
Kartenleser	Gerät des Versicherten	Ermöglicht dem FdV den Zugriff auf die eGK des Nutzers. Es kann die kontaktbehaftete oder die kontaktlose Schnittstelle der eGK genutzt werden.
Anbieter ePA-Aktensystem	Organisatorisch, kein Akteur in der Ausführung von Anwendungsfällen	Der Anbieter stellt Informationen bereit, um sich via FdV am ePA-Aktensystem anzumelden.
Hersteller ePA-Frontend des Versicherten	Organisatorisch, kein Akteur in der Ausführung von Anwendungsfällen	Der Hersteller stellt im Handbuch Informationen bereit bezüglich <ul style="list-style-type: none"> Anforderungen an die Ausführungsumgebung Möglichkeiten zur Anbindung der eGK

3.2 Nachbarsysteme

Die vom FdV direkt erreichbaren Produkttypen der TI sind

- ePA-Aktensystem,
- Signaturdienst und
- eGK (G2 und höher).

Der Signaturdienst bietet die Schnittstelle `I_Remote_Sign_Operations` für Signatur mittels der alternativen Versichertenidentität an. Siehe [gemSpec_Signaturdienst].

In TAB_FdV_102 sind die Schnittstellen des ePA-Aktensystems gelistet, welche durch das FdV genutzt werden.

Tabelle 2 : TAB_FdV_102 – Schnittstellen des ePA-Aktensystems

Schnittstelle	Operationen	Bemerkung
I_Authentication_Insurant	getAuditEvents LoginCreateChallenge LoginCreateToken LogoutToken RenewToken	Definition in [gemSpec_Authentisierung_Vers]
I_Authorization_Insurant	getAuthorizationKey	Definition in [gemSpec_Autorisierung]
I_Authorization_Management_Insurant	deleteAuthorizationKey getAuditEvents getAuthorizationList putAuthorizationKey putNotificationInfo replaceAuthorizationKey	Definition in [gemSpec_Autorisierung]
I_Account_Management_Insurant	GetAuditEvents SuspendAccount ResumeAccount	Definition in [gemSpec_Dokumentenverwaltung]
I_Proxy_Directory_Query	Search	Definition in [gemSpec_Zugangsgateway_Vers]
I_Document_Management_Connect	CloseContext OpenContext	Definition in [gemSpec_Dokumentenverwaltung]
I_Document_Management_Insurant	ProvideAndRegisterDocumentSet-b RegistryStoredQuery RemoveDocuments RetrieveDocumentSet	Definition in [gemSpec_Dokumentenverwaltung]
Status-Proxy		Definition in [gemSpec_Zugangsgateway_Vers]
TSL-Proxy		Definition in [gemSpec_Zugangsgateway_Vers]
Schlüsselgenerierungsdienst Typ 1 und Typ 2		Definition in [gemSpec_SGD_ePA]

Ausführungsumgebung des FdV ist ein Gerät des Versicherten (GdV), bspw. ein stationäres Gerät oder ein mobiles Endgerät. Es steht unter alleiniger Kontrolle des

Versicherten. Es obliegt dem Versicherten, durch geeignete Maßnahmen die Sicherheit der Daten zu stärken.

Für die Authentisierung mittels eGK und kryptographischer Operationen greift das FdV über ein Kartenlesegerät oder über die kontaktlose Schnittstelle auf die eGK zu.

3.2.1 Identität des Nutzers

Ein Versicherter kann als Nutzer des FdV das auf der eGK verfügbare Schlüsselmaterial und Zertifikate für die Authentisierung gegenüber dem ePA-Aktensystem und dem Schlüsselgenerierungsdienst verwenden.

Voraussetzung ist die Nutzung einer eGK G2 oder höher, wobei eine eGK G2 nur den RSA-2048-Algorithmenkatalog unterstützt. Eine eGK G2.1 unterstützt den RSA-2048 und ECC-256-Algorithmenkatalog. Die normierenden Organisationen haben das Ende der Zulässigkeit für den RSA-2048 festgelegt. Aus diesem Grund wird bei Nutzung einer eGK G2 der RSA-Algorithmenkatalog und bei eGK einer höheren Generation (d.h. ab eGK G2.1) der ECC-Algorithmenkatalog verwendet.

Zusätzlich zur eGK sieht das FdV die Möglichkeit der Nutzung einer alternativen Authentisierung vor. Sie muss bei der Krankenkasse des Nutzers beantragt werden. Die Authentisierung beim ePA-Aktensystem erfolgt unter Einbeziehung eines Signaturdienstes.

Für die Zertifikate der alternativen Authentisierung wird der ECC-Algorithmenkatalog verwendet.

4 Zerlegung des Produkttyps

Im Folgenden wird die Zerlegung des Produkttyps FdV dargestellt, welche für die Übersicht der funktionalen Leistungsmerkmale in der vorliegenden Spezifikation nötig ist.

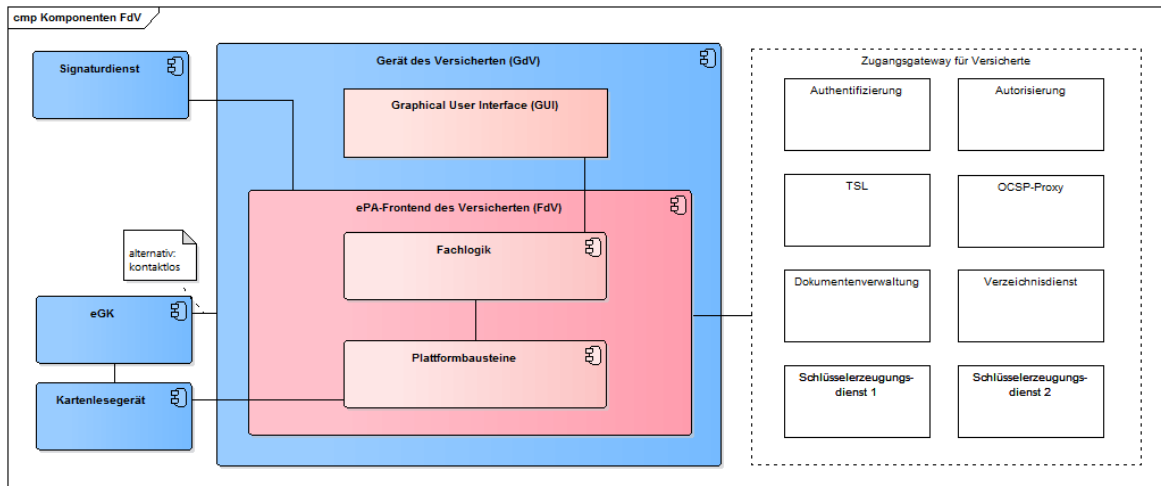


Abbildung 1: Komponenten des FdV

Tabelle 3 :TAB_FdV_167 – Komponenten des FdV

Komponente	Verantwortung und Funktionalität	Spezifiziert in
Fachlogik	Die Komponente steuert die Anwendungsfälle entsprechend den fachanwendungsspezifischen Festlegungen.	Kap. 6.2
Plattformbausteine	Diese Komponente enthält Plattformbausteine, welche Funktionalitäten der TI-Plattform zur Verfügung stellen: <ul style="list-style-type: none"> • Zugriff auf die eGK für kryptografische Operationen, PIN-Management, ... • Kryptografische Operationen Die Plattformbausteine werden durch die Fachlogik angesteuert.	Kap. 6.3

5 Übergreifende Festlegungen

5.1 Datenschutz und Sicherheit

In diesem Kapitel werden übergreifende Anforderungen beschrieben, die sich aus den Themenfeldern Datenschutz und Sicherheit ergeben.

A_16973 - ePA-Frontend des Versicherten: lokale Ausführung

Das ePA-Frontend des Versicherten MUSS sicherstellen, dass alle ePA-fachanwendungsspezifischen Anteile des ePA-Frontend des Versicherten lokal auf dem Gerät des Versicherten ausgeführt werden.

[<=]

A_15251 - ePA-Frontend des Versicherten: Anforderungen an Ausführungsumgebung

Der Hersteller des ePA-Frontends des Versicherten MUSS den Nutzer über die Annahmen und Anforderungen an die Ausführungsumgebung seines Produktes informieren.[<=]

Die Annahmen und Anforderungen sollen insbesondere Hinweise enthalten, mit welchen Maßnahmen der Nutzer seine Ausführungsumgebung sicher gestalten kann.

Die medizinischen Dokumente im ePA-Aktensystem sind Ende-zu-Ende verschlüsselt. Dadurch können die Dokumente nicht an zentraler Stelle auf mögliche Schadsoftware geprüft werden. Eine Absicherung gegen mögliche Schadsoftware muss auf dem GdV erfolgen.

A_17723 - ePA-Frontend des Versicherten: Über mögliche Schadsoftware informieren

Der Hersteller des ePA-Frontends des Versicherten MUSS den Nutzer darüber informieren, dass Dokumente Schadsoftware enthalten können und welche Maßnahmen der Nutzer zum Selbstschutz vornehmen kann.

[<=]

A_15252 - ePA-Frontend des Versicherten: Schlüsselmateriale nicht persistent speichern

Das ePA-Frontend des Versicherten DARF alle verwendeten symmetrischen und privaten asymmetrischen Schlüssel NICHT persistent speichern.[<=]

A_15253 - ePA-Frontend des Versicherten: Schutz Session-Daten

Das ePA-Frontend des Versicherten DARF Session-Daten NICHT an Dritte, außer im Rahmen der in den Anwendungsfällen spezifizierten Kommunikation, weitergeben. [<=]

Der Umfang der Session-Daten ist im Kapitel "7.-Informationsmodell" beschrieben. Die für den Versicherten im Aktenkonto bereitgestellten Dokumente gehören nicht zu den Session-Daten.

A_15254 - ePA-Frontend des Versicherten: Session-Daten nicht persistent speichern

Das ePA-Frontend des Versicherten DARF Session-Daten NICHT persistent speichern.[<=]

A_17625 - ePA-Frontend des Versicherten: Keine Speicherung von Authentisierungsmerkmalen

Das ePA-Frontend des Versicherten DARF Authentisierungsmerkmale (z.B. PIN, Passwörter usw.) NICHT speichern.

[<=]

A_17078 - ePA-Frontend des Versicherten: Risiko Session-Hijacking reduzieren

Das ePA-Frontend des Versicherten MUSS geeignete Maßnahmen ergreifen, um die Wahrscheinlichkeit erfolgreicher Session-Hijacking-Angriffe zu reduzieren.[<=]

A_15255 - ePA-Frontend des Versicherten: Schutzmaßnahmen gegen die OWASP-Mobile-Top-10-Risiken

Das ePA-Frontend des Versicherten MUSS Maßnahmen zum Schutz vor den in der aktuellen Version genannten OWASP-Top-10-Mobile-Risiken [OWASPMobileTop10] umsetzen.

[<=]

Dies betrifft bspw. die folgenden Aspekte:

- Schutz von Reverse Engineering
- Verwendung von Plattform Sicherheit Best Practice
- Secure Data Storage
- Schutz gegen code tampering
- Extraneous functionality

Für mobile Anwendungen sind OWASP Top Ten Mobile Controls [OWASP TTMC] zu beachten.

Diese Anforderung ist sowohl für Lösungen auf mobilen als auch Desktop-Plattformen umzusetzen.

Die im Aktenkonto eingestellten Dokumente werden verschlüsselt an das Aktensystem übermittelt und verarbeitet. Sie liegen im Aktensystem nie im Klartext vor. Daher kann das ePA-Aktensystem den Inhalt der Dokumente nicht auf Schadsoftware überprüfen.

A_17660 - ePA-Frontend des Versicherten: Schutzmaßnahmen gegen Schadsoftware aus Dokumenten

Das ePA-Frontend des Versicherten MUSS, wenn es Dokumentinhalte direkt anzeigt, Maßnahmen zum Schutz vor Schadsoftware in den Dokumenten umsetzen.

[<=]

Folgende Maßnahmen sind sinnvoll:

- Prüfen, ob Dokumenten-Format und Inhalt mit dem angegebenen Dokumententyp in den Metadaten übereinstimmt
- Prüfen, ob Dokumenten-Format und Inhalt zu den erlaubten ePA-Dokumentenformaten passt
- Vor der Anzeige eines Dokumentes sind Sonder- und Meta-Zeichen im Dokument für die jeweilige Anzeigesoftware mit der richtigen Escape-Syntax zu entschärfen.
- Die Anzeigesoftware ist in einer Art Sandbox zu betreiben.

A_15256 - ePA-Frontend des Versicherten: Verbot von Werbe- und Usability-Tracking

Das ePA-Frontend des Versicherten DARF ein Werbe- und Usability-Tracking NICHT verwenden.[<=]

A_15257 - ePA-Frontend des Versicherten: Qualität verwendeter Schlüssel

Das ePA-Frontend des Versicherten MUSS sicherstellen, dass die von ihm erzeugten Schlüssel die Qualität nach [gemSpec_Krypt#GS-A_4368] besitzen.

[<=]

Wenn die eGK zur Verfügung steht, dann kann diese für das Erzeugen von Schlüsseln in der geforderten Qualität (Kartenkommando GET RANDOM) genutzt werden. Ist das optionale Kartenkommando GET RANDOM für die eGK nicht verfügbar (Fehlermeldung der Karte), dann kann das Kartenkommando GET CHALLENGE (PL_TUC_GET_CHALLENGE) der eGK genutzt werden. GET RANDOM und GET CHALLENGE liefern einen ausreichend guten Zufall, der die Forderungen aus [gemSpec_Krypt#GS-A_4368] erfüllt.

Wenn die eGK nicht zur Verfügung steht, dann können Informationen von zusätzliche Quellen (Internet, Sensoren des GdV) zusammengeführt werden, um die geforderte Entropie zu erreichen.

A_15258 - ePA-Frontend des Versicherten: Dynamische Inhalte von Drittanbieter

Das ePA-Frontend des Versicherten DARF dynamische Inhalte von Drittanbietern NICHT herunterladen oder verwenden.[<=]

A_15259 - ePA-Frontend des Versicherten: Privacy bei default

Das ePA-Frontend des Versicherten MUSS bei Konfigurationsmöglichkeiten die sichere, datenschutzfreundlichere Option vorauswählen.[<=]

Bspw. ist ein Opt-In anstelle eines Opt-Out-Verfahrens anzuwenden.

A_15260 - ePA-Frontend des Versicherten: Anforderung an Berechtigungen von Systemressourcen

Das ePA-Frontend des Versicherten MUSS die Anforderungen an Berechtigungen für den Zugriff auf Ressourcen des Systems, welches das ePA-Frontend des Versicherten ausführt, auf das notwendige Maß beschränken.[<=]

Hierbei muss insbesondere bei FdV-Anwendungen auf mobilen Geräten auf den Zugriff auf Systemressourcen (bspw. Kamera) verzichtet werden, wenn diese für die ePA-Anwendungsfälle oder Zusatzfunktionalitäten des FdV nicht notwendig sind.

A_15261 - ePA-Frontend des Versicherten: Kapseln von Bibliotheken von Drittanbietern

Das ePA-Frontend des Versicherten MUSS Bibliotheken gemäß [OWASP Proactive Control#C2 Punkt 4] kapseln.

[<=]

Anforderungen zum Herstellungsprozess

A_15262 - ePA-Frontend des Versicherten: Implementierungsspezifische Sicherheitsanforderungen

Der Hersteller des ePA-Frontends des Versicherten MUSS während der Entwicklung des Produktes implementierungsspezifische Sicherheitsanforderungen dokumentieren und umsetzen. [<=]

A_15263 - ePA-Frontend des Versicherten: Verwendung eines sicheren Entwicklungsprozesses

Der Hersteller des ePA-Frontends des Versicherten MUSS während der Entwicklung des Produktes einen sicheren Entwicklungsprozess (Security Development Lifecycle) verwenden.

[<=]

Ein Beispiel für einem sicheren Entwicklungsprozess ist der Microsoft Security Development Lifecycle. Für weitere Informationen siehe [OWASP SAMM Project].

A_15443 - ePA-Frontend des Versicherten: Sicherheitsrelevante Softwarearchitektur-Review

Der Hersteller des ePA-Frontends des Versicherten MUSS einen sicherheitsrelevanten Softwarearchitektur-Review durchführen und identifizierte Architekturschwachstellen beheben. [≤]

A_15264 - ePA-Frontend des Versicherten: Durchführung einer Bedrohungsanalyse

Der Hersteller des ePA-Frontends des Versicherten MUSS eine Bedrohungsanalyse durchführen und Maßnahmen gegen die identifizierten Bedrohungen implementieren. [≤]

A_15265 - ePA-Frontend des Versicherten: Durchführung regelmäßige sicherheitsrelevante Quellcode Review

Der Hersteller des ePA-Frontends des Versicherten MUSS während der Entwicklung des Produktes regelmäßige sicherheitsrelevante Quellcode-Reviews oder automatisierte sicherheitsrelevante Quellcode-Scans durchführen und alle medium oder hoch kritische Schwachstellen beheben. [≤]

A_15266 - ePA-Frontend des Versicherten: Durchführung regelmäßiger Sicherheitstests

Der Hersteller des ePA-Frontends des Versicherten MUSS während der Entwicklung des Produktes regelmäßige automatisierte Sicherheitstests durchführen und alle medium oder hoch kritischen Schwachstellen beheben. [≤]

A_15267 - ePA-Frontend des Versicherten: Sicherheitsschulung für Entwickler

Der Hersteller des ePA-Frontends des Versicherten MUSS alle Entwickler des Produktes in sicherer Entwicklung und Secure Coding Techniken schulen. [≤]

Das ePA-Frontend des Versicherten kann Funktionalitäten enthalten, welche sich nicht aus den Anwendungsfällen der Fachanwendung ePA ergeben. Folgende Anforderungen gelten für die Abgrenzung der zusätzlichen Funktionalitäten zu denen der Fachanwendung ePA.

A_17077 - ePA-Frontend des Versicherten: Kein Sicherheitsverlust durch zusätzliche Funktionalitäten

Falls das ePA-Frontend des Versicherten zusätzliche Funktionalitäten enthält, DÜRFEN diese zusätzlichen Funktionalitäten NICHT die Sicherheit oder den Datenschutz der personenbezogenen und medizinischen Daten des Versicherten in der ePA negativ beeinträchtigen.

[≤]

A_16438 - ePA-Frontend des Versicherten: Unterscheidbarkeit zusätzlicher Funktionalitäten

Das ePA-Frontend des Versicherten MUSS sicherstellen, falls es zusätzliche Funktionalitäten enthält, dass der Nutzer diese zusätzlichen Funktionalitäten von den Funktionalitäten für die ePA unterscheiden kann. [≤]

Die Information, welche Funktionalitäten zusätzlich zu den Funktionen für die ePA enthalten und damit nicht Gegenstand der Zulassung durch die gematik sind, kann im Handbuch oder den Informationen zur Zustimmung gemäß A_16439 beschrieben werden.

A_16439 - ePA-Frontend des Versicherten: Weiterleiten von Daten - Zustimmung

Das ePA-Frontend des Versicherten MUSS sicherstellen, dass Daten, die aus der ePA ins FdV geladen werden, nur mit Zustimmung des Versicherten unter Nutzung von

expliziten Opt-in-Lösungen weitergeleitet werden können, wobei sich das Opt-In nur genau auf die Weiterleitung beziehen und nicht mit anderen Zustimmungen kombiniert werden darf.[<=]

Die in A_16439 geforderte Zustimmung kann einmalig durch den Versicherten erteilt werden und bis auf Widerruf des Versicherten für alle Datenweiterleitungen, die von dem Versicherten veranlasst werden, gelten. Das FdV kann dabei die Möglichkeit einer expliziten Opt-in-Lösung mit Widerrufsrecht oder ein anlassbezogenes Zustimmungsverfahren oder eine Wahlmöglichkeit beider Verfahren vorsehen.

A_16440 - ePA-Frontend des Versicherten: Weiterleiten von Daten - Information

Das ePA-Frontend des Versicherten MUSS sicherstellen, dass der Versicherte vor der Zustimmung zur Nutzung von aus der ePA ins FdV geladenen Daten durch Anwendungen oder Apps im oder außerhalb des Frontends in verständlicher Weise darüber informiert wird, welche Daten, wann und an wen weitergeleitet werden und zu welchem Zwecke die Anwendungen die Daten verarbeiten.[<=]

A_16441 - ePA-Frontend des Versicherten: Weiterleiten von Daten - Nachvollziehbarkeit

Das ePA-Frontend des Versicherten MUSS sicherstellen, dass der Versicherte eine Weiterleitung der Daten im Nachhinein nachvollziehen kann (z.B. durch Protokollierung). [<=]

5.2 Verwendete Standards

Für die Nutzung der Schnittstellen werden u.a. die folgenden Standards verwendet.

A_15268 - ePA-Frontend des Versicherten: Konformität zu WS-I Basic Profil 2.0

Das ePA-Frontend des Versicherten MUSS SOAP-Nachrichten gemäß den Vorgaben aus WS-I Basic Profile V2.0 [WSIBP] unterstützen. [<=]

A_15269 - ePA-Frontend des Versicherten: Verwendung von WS-Trust 1.4

Das ePA-Frontend des Versicherten MUSS für die Authentisierung den Standard [WS-Trust1.4] unterstützen.[<=]

A_15270 - ePA-Frontend des Versicherten: Verwendung von DMSLv2

Das ePA-Frontend des Versicherten MUSS für die Abfrage des Verzeichnisdienstes die Standard Directory Services Markup Language v2.0 (DSMLv2) unterstützen.[<=]

Informationen zu DMSLv2 sind unter <https://www.oasis-open.org/standards#dsmlv2> verfügbar.

5.3 Integrating the Healthcare Enterprise IHE

Die dokumentenbezogenen Schnittstellen des ePA-Aktensystems und die Verarbeitungslogik des FdV basieren auf Transaktionen des IHE ITI Technical Frameworks (IHE ITI TF). Die IHE ITI-Implementierungsstrategie ist in [gemSpec_DM_ePA] beschrieben.

Das FdV nutzt die folgenden Integrationsprofile des IHE ITI TF:

- Cross-Enterprise Document Sharing (XDS.b) Profile
- Remove Metadata and Documents (RMD) Profile

- Cross-Enterprise User Assertion (XUA) Profile
- Advanced Patient Privacy Consents (APPC) Profile

Die folgende Tabelle bietet einen Überblick über die durch das FdV umzusetzenden IHE ITI-Akteure und assoziierte Transaktionen. Siehe auch [gemSpec_DM_ePA#Abbildung Überblick über IHE ITI-Akteure und assoziierte Transaktionen].

Tabelle 4: TAB_FdV_103 – IHE Akteure und Transaktionen

Aktion	Profile	IHE-Akteur	Transaktion	Referenz
Suchanfrage auf Metadaten	XDS.b	Document Consumer	Registry Stored Query [ITI-18]	[IHE-ITI-TF2a]#3.18
Herunterladen von Dokumenten	XDS.b	Document Consumer	Retrieve Document Set [ITI-43]	[IHE-ITI-TF2b]#3.43
Einstellen von Dokumenten	XDS.b	Document Source	Provide & Register Document Set-b [ITI-41]	[IHE-ITI-TF2b]#3.41
Löschen von Dokumenten	RMD	Document Administrator	Remove Documents [ITI-86]	[IHE-ITI-TF2c]#3.86
AuthenticationAssertion übertragen	XUA	X-Service User	Provide X-User Assertion [ITI-40]	[IHE-ITI-TF2b]#3.40
Policy Document erstellen	APPC	APPC Content Creator	-	[IHE-ITI-APPC]
Interpretieren von Policy Documents	APPC	APPC Content Consumer	-	[IHE-ITI-APPC]

Die übergreifenden Einschränkungen von IHE ITI-Transaktionen sowie Festlegungen spezieller Umsetzungsvorgaben bzgl. einzelner Transaktionen sind in [gemSpec_DM_ePA] und [gemSpec_Dokumentenverwaltung] beschrieben.

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

Im FdV werden fachliche Dokumente (Versichertendokumente) und technische Dokumente (Policy Documents) unterschieden.

5.3.1 Policy Documents

Die Fachanwendung ePA verwendet das APPC-Profil für die Durchsetzung von Zugriffsregeln (Autorisierung). Die Zugriffsregeln werden gemäß APPC in Policy Documents beschrieben und als technische Dokumente im Aktenkonto des Versicherten hinterlegt.

Für jeden Vertreter, jede berechnigte Leistungserbringerinstitution (LEI), den berechtigten Kostenträger (KTR) und den Aktenkontoinhaber wird je ein Policy Document im Aktenkonto verwaltet.

Bei der Neuvergabe einer Berechtigung für Vertreter, LEI oder KTR erstellt das FdV ein neues Policy Document (Base Policy) und lädt es in das Aktenkonto hoch. Bei der Änderung einer Berechtigung (bspw. Verlängerung der Berechtigungsdauer) lädt das FdV das Policy Document aus dem Aktenkonto herunter (IHE-Akteur Content Consumer), bearbeitet es und lädt die veränderte Fassung als neu zu registrierende Policy in das Aktenkonto hoch (IHE APPC-Akteur Content Creator). Beim Hochladen einer veränderten Version eines Policy Documents wird die vorherige Version infolge des Hochladens des neuen Policy Documents automatisch durch das ePA-Aktensystem gelöscht. Beim Entzug einer Berechtigung löscht das FdV das entsprechende Policy Document aus dem Aktenkonto.

Das ePA-Aktensystem wertet die in den Policy Documents hinterlegten Zugriffsregeln aus. Es entscheidet unter Berücksichtigung der Dokumentenmetadaten, ob der anfragende Nutzer den Dokumentenzugriff (bspw. Einstellen von Dokumenten) durchführen darf oder ob der Dokumentenzugriff ablehnt wird.

Das FdV verarbeitet Policy Documents intern.

A_15271 - ePA-Frontend des Versicherten: Keine Anzeige von Policy Documents

Das ePA-Frontend des Versicherten DARF dem Nutzer Policy Documents NICHT als Dokumente anzeigen oder zur Auswahl anbieten. [≤=]

Für die XDS-Metadaten eines Policy Documents gelten die Nutzungsvorgaben aus [\[gemSpec_DM_ePA#A_14961 - Nutzungsvorgaben für die Verwendung von XDS-Metadaten bei Policy Documents\]](#)

A_15673 - ePA-Frontend des Versicherten: Policy Document (Base Policy) für LEI erstellen

Das ePA-Frontend des Versicherten MUSS für zu berechtigende LEIs eine XACML 2.0 Policy als Policy Document (Advanced Patient Privacy Consent) gemäß [IHE-ITI-APPC] unter Berücksichtigung der Anforderungen an deren Inhalt in [gemSpec_Dokumentenverwaltung#Tab_Dokv_300] erstellen (Base Policy). [≤=]

Die Inhalte der Base Policy für LEI sind in [\[gemSpec_Dokumentenverwaltung#8.3.1 Base Policy für eine Leistungserbringerinstitution\]](#) beschrieben.

Das Attribut der Base Policy mit der Attribut-ID

"urn:oasis:names:tc:xspa:1.0:subject:organization" beinhaltet den Namen der LEI, welcher für die Anzeige der Berechtigung genutzt wird.

Das Attribut der Base Policy mit der Attribut-ID

"urn:gematik:subject:organization-id" beinhaltet die TelematikID der LEI.

Beim Erstellen einer Base Policy wird der Name und die TelematikID einer LEI aus dem Verzeichnisdienst der TI bestimmt (siehe "6.2.3.15- Suchanfrage Verzeichnisdienst der TI").

Das Attribut der Base Policy mit der Attribut-ID "urn:ihe:iti:ser:2016:patient-id" beinhaltet die Versicherten-ID des Aktenkontoinhabers

Das Attribut EnvironmentMatch/MatchId

"urn:oasis:names:tc:xacml:1.0:function:dateTime-less-than-or-equal" beinhaltet den "gültig bis" Zeitpunkt der Berechtigung. Der Zeitpunkt ist bei der Neuerstellung eines Policy Documents ausgehend vom aktuellen Datum anhand der gewählten Option zu berechnen.

Das Attribut EnvironmentMatch/MatchID

"urn:oasis:names:tc:xacml:1.0:function:date-greater-than" beinhaltet

das Erstellungsdatum der Berechtigung. Das Erstellungsdatum entspricht bei der Neuerstellung eines Policy Documents dem aktuellen Datum.

Die `PolicySetIDReference` steuert, ob die zu berechtigende LEI dem Zugriff auf die durch LEI eingestellten sowie leistungserbringeräquivalenten Dokumente, den Zugriff auf durch Versicherte und Vertreter eingestellte Dokumente oder durch KTR eingestellte Dokumente erhält.

A_15674 - ePA-Frontend des Versicherten: Policy Document (Base Policy) für Vertreter erstellen

Das ePA-Frontend des Versicherten MUSS für zu berechtigende Vertreter eine XACML 2.0 Policy als Policy Document (Advanced Patient Privacy Consent) gemäß [IHE-ITI-APPC] unter Berücksichtigung der Anforderungen an deren Inhalt in [gemSpec_Dokumentenverwaltung#Tab_Dokv_200] erstellen (Base Policy). [`<=`]

Die Inhalte der Base Policy für Vertreter sind in [\[gemSpec_Dokumentenverwaltung#8.2.1 Base Policy für einen Vertreter\]](#) beschrieben.

Das Attribut der Base Policy mit der Attribut-ID

"urn:oasis:names:tc:xacml:1.0:subject:subject" beinhaltet den Namen des Vertreters, welcher für die Anzeige der Berechtigung genutzt wird.

Das Attribut der Base Policy mit der Attribut-ID "urn:gematik:subject:subject-id" beinhaltet die Versicherten-ID des Vertreters.

Das Attribut der Base Policy mit der Attribut-ID "urn:ihe:iti:ser:2016:patient-id" beinhaltet die Versicherten-ID des Aktenkontoinhabers.

A_17232 - ePA-Frontend des Versicherten: Policy Document (Base Policy) für Kostenträger erstellen

Das ePA-Frontend des Versicherten MUSS für einen zu berechtigenden Kostenträger eine XACML 2.0 Policy als Policy Document (Advanced Patient Privacy Consent) gemäß [IHE-ITI-APPC] unter Berücksichtigung der Anforderungen an deren Inhalt in [gemSpec_Dokumentenverwaltung#Tab_Dokv_400] erstellen (Base Policy). [`<=`]

Die Inhalte der Base Policy für KTR sind in [\[gemSpec_Dokumentenverwaltung#8.4.1 Base Policy für einen Kostenträger\]](#) beschrieben.

Das Attribut der Base Policy mit der Attribut-ID

"urn:oasis:names:tc:xspa:1.0:subject:organization" beinhaltet den Namen des KTR, welcher für die Anzeige der Berechtigung genutzt wird.

Das Attribut der Base Policy mit der Attribut-ID "urn:gematik:subject:organization-id" beinhaltet die TelematikID des KTR.

Beim Erstellen einer Base Policy wird der Name und die TelematikID eines KTR aus dem Verzeichnisdienst der TI bestimmt (siehe "6.2.3.15- Suchanfrage Verzeichnisdienst der TI").

Das Attribut der Base Policy mit der Attribut-ID "urn:ihe:iti:ser:2016:patient-id" beinhaltet die Versicherten-ID des Aktenkontoinhabers.

Die Unterscheidung bei der Verarbeitung im FdV, ob es sich bei einer Base Policy um ein Policy Document für eine LEI, einen Vertreter oder einen Kostenträger handelt, erfolgt anhand von `root` in `InstanceIdentifier`.

5.3.2 Versichertendokumente

Zu jedem Dokument verwaltet das ePA-Aktensystem Metadaten, welche für die Suche nach Dokumenten verwendet werden. Für Dokumente, welche der Nutzer in die Dokumentenverwaltung einstellt, müssen Metadaten erstellt werden.

Für die XDS-Metadaten von Dokumenten des Versicherten gelten die Nutzungsvorgaben aus [\[gemSpec_DM_ePA#A_14760 - Nutzungsvorgaben für die Verwendung von XDS-Metadaten\]](#).

5.4 Benutzeroberfläche

Das FdV ist eine für die eigenständige Nutzung der ePA durch Versicherte in einer persönlichen Umgebung konzipierte Benutzeroberfläche. Die persönliche Umgebung ist eine private, nicht öffentliche, Umgebung des Versicherten, über die dieser die alleinige Kontrolle hat.

Die folgenden Ausführungen zu Anforderungen an die visuelle Darstellung und Benutzerführung sind informativ und nicht normativ.

5.4.1 Visuelle Darstellung

Für die visuelle Darstellung der Inhalte ist eine grafische Benutzeroberfläche erforderlich, welche die Daten des Versicherten strukturiert und übersichtlich darstellt.

Das FdV soll eine einheitlich gestaltete Oberfläche zur Benutzerführung besitzen, um die Übersichtlichkeit in allen Anwendungsfällen für den Nutzer zu gewährleisten. Es soll Menüfunktionen, Texte und andere Anzeigen eindeutig, verständlich und widerspruchsfrei benennen bzw. darstellen.

Das ePA-Frontend des Versicherten soll es dem Nutzer ermöglichen, zu jeder Zeit zu erkennen, in welchem ePA-Anwendungsfall sich die Applikation gerade befindet.

5.4.2 Benutzerführung

Die Bedienung des FdV soll für den Nutzer intuitiv gestaltet werden. Das FdV soll dem Nutzer alle anzeigbaren Texte mindestens in der Sprache Deutsch bereitstellen. Zusätzliche Sprachen können unterstützt werden.

DIN Normen und Verordnungen zur Beachtung:

Zusätzlich zu den in diesem Kapitel aufgeführten Anforderungen an das FdV zur Benutzerführung sollen auch die in der ISO 9241 aufgeführten Qualitätsrichtlinien zur Sicherstellung der Ergonomie interaktiver Systeme und Anforderungen aus der Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (Barrierefreie-Informationstechnik-Verordnung – BITV 2.0) beachtet werden.

Insbesondere sollen die nachfolgend aufgeführten Teile der ISO 9241 berücksichtigt werden:

DIN EN ISO 9241 – Teile mit Bezug zur Software-Ergonomie

- Teil 8: Anforderungen an Farbdarstellungen

- Teil 9: Anforderungen an Eingabegeräte – außer Tastaturen
- Teil 110: Grundsätze der Dialoggestaltung (ersetzt den bisherigen Teil 10)
- Teil 11: Anforderungen an die Gebrauchstauglichkeit – Leitsätze
- Teil 12: Informationsdarstellung
- Teil 13: Benutzerführung
- Teil 14: Dialogführung mittels Menüs
- Teil 15: Dialogführung mittels Kommandosprachen
- Teil 16: Dialogführung mittels direkter Manipulation
- Teil 17: Dialogführung mittels Bildschirmformularen
- Teil 171: Leitlinien für die Zugänglichkeit von Software BITV 2.0

BITV 2.0 - Barrierefreie Informationstechnik-Verordnung

Die Umsetzung der Verordnung dient zur behindertengerechten Umsetzung von Webseiten und anderen grafischen Oberflächen.

Insbesondere sollen deshalb neben der Übernahme der international anerkannten Standards für barrierefreie Webinhalte (Web Content Accessibility Guidelines (WCAG) 2.1) auch die Belange gehörloser, hör-, lern- und geistig behinderter Menschen berücksichtigt werden.

Die BITV 2.0 regelt unter anderem den sachlichen Geltungsbereich, die einzubeziehenden Gruppen behinderter Menschen und die anzuwendenden Standards.

Weitere Richtlinien und Empfehlungen zur digitalen Barrierefreiheit sind die EU Richtlinie 2016/2102 für öffentliche Stellen und die europäische Norm EN 301 549 V1.2.1 mit dem Titel "Accessibility requirements for ICT products and services".

Das FdV soll die Schnittstellen für die Unterstützung der barrierefreien Bedienungsmöglichkeit, welche vom Betriebssystem zur Verfügung gestellt werden, nutzen.

Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, die Aktensession jederzeit zu beenden.

Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, Anwendungsfälle auch vor der Beendigung jederzeit abubrechen.

Nach dem Start des FdV und einem ggf. durchgeführten Login wird dem Versicherten eine Startoberfläche angezeigt, auf der klar erkennbar ist, welche Arten von Dokumentenzugriffen und Verwaltungsfunktionen ausgeführt werden können.

Die Bezeichnung der Inhalte und Anwendungsfälle muss für den Nutzer eindeutig und verständlich sein. Bezeichnungen sollen nach Möglichkeit vollständig ausgeschrieben sein, Abkürzungen sind zu vermeiden.

Hinweise am FdV

Um dem Nutzer die Bedienung zu vereinfachen, sollen ihm Hinweise angezeigt werden, die den Zweck sowie den inhaltlichen Ablauf eines Anwendungsfalls betreffen.

Im Hinweistext können die einzelnen Schritte des Anwendungsfalls sowie die Auswirkungen auf die Nutzung der Anwendung im Rahmen der Versorgung beschrieben sein.

Ist ein Anwendungsfall durchgeführt worden, muss das FdV das Ergebnis für den Versicherten klar verständlich anzeigen, z. B. "Die Vertretung wurde erfolgreich eingerichtet."

Ist ein Anwendungsfall durch den Versicherten abgebrochen worden oder technisch nicht durchführbar, muss der Versicherte ebenfalls einen für ihn verständlichen Hinweis erhalten. In jedem Fall muss das Ergebnis für den Versicherten klar erkennbar sein.

Für die Anzeige in Fehlerfällen siehe Kapitel "6.2.2- Fehlerbehandlung".

Zur Sicherstellung, dass keine Daten versehentlich gelöscht werden, soll der Nutzer nach der Auswahl der Löschen-Funktion darauf hingewiesen werden, dass es sich hierbei um eine unwiderrufliche Aktion handelt.

5.4.3 Dokumente

Der Nutzer kann nach Dokumenten in der ePA suchen und diese herunterladen oder sich anzeigen lassen.

A_15283 - ePA-Frontend des Versicherten: Dokumentgrößen von 25 MB

Das ePA-Frontend des Versicherten MUSS für alle Außenschnittstellen, in denen ein Dokument verarbeitet wird, Dokumente mit einer Größe von mindestens 25 MB unterstützen.[<=]

Für die Anzeige der Dokumente werden die auf dem Gerät des Versicherten (GdV) verfügbaren Standardprogramme verwendet. Unter einem Standardprogramm wird das im GdV mit einem Dokumenttypen verknüpfte Programm verstanden (z.B. Dateityp PDF mittels eines auf dem GdV verfügbaren PDF Reader). Das FdV braucht keine Funktionalität zur Anzeige von Dokumenten in beliebigem Format bereitstellen.

A_17226 - ePA-Frontend des Versicherten: Anzeige Metadaten von Dokumenten

Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, alle zu einem Dokument zugehörigen Metadaten mit fachlichen Informationen einzusehen.[<=]

Technische Metadaten zu einem Dokument müssen nicht angezeigt werden.

A_15284 - ePA-Frontend des Versicherten: Anzeige von Dokumenten

Das ePA-Frontend des Versicherten SOLL Standardprogramme zur Anzeige von aus der ePA heruntergeladenen Dokumenten verwenden. [<=]

Ist kein Programm zur Anzeige des Dokumentenformates auf dem GdV verfügbar, dann kann der Nutzer das Dokument nur lokal speichern.

A_15285 - ePA-Frontend des Versicherten: Anzeige strukturierter Dokumente

Das ePA-Frontend des Versicherten MUSS für strukturierte Dokumente eine für den Nutzer lesbare Darstellung mit dem vollständigen Inhalt des Dokumentes generieren und dem Nutzer anzeigen können. [<=]

Für Informationen zu strukturierten Dokumenten siehe [gemSpec_DM_ePA#Tab_DM_100]. Wenn ein Arztbrief Dokument mit xml und pdf Anteil vorliegt, muss nur das PDF angezeigt werden.

Der Nutzer kann Dokumente in die ePA einstellen. Dafür müssen diese im FdV ausgewählt werden.

A_15286 - ePA-Frontend des Versicherten: Auswahl von Dokumenten

Das ePA-Frontend des Versicherten MUSS dem Nutzer ermöglichen, mehrere Dokumente aus lokal eingebundenem Speicher auszuwählen, um sie in die ePA einzustellen.[<=]

5.4.4 Eingabe Metadaten für einzustellende Dokumente

Für Dokumente, welche durch den Nutzer in die ePA eingestellt werden, sind Metadaten anzugeben, auf deren Basis Dokumente gesucht und heruntergeladen werden können.

Die XDS-Metadaten und ihre Nutzungsvorgaben sind in [\[gemSpec_DM_ePA#A_14760\]](#) beschrieben.

Tabelle 5 : TAB_FdV_125 – Metadatenattribute

Metadatenattribut XDS.b	Dokument einstellen: Anzeige	Dokument einstellen: Defaultwert	Dokument einstellen: Änderbar	Bemerkung
Metadatenelement Document Entry				
author				Das Document Entry-Element muss als einen Eintrag den Submission Set author beinhalten. Dieser Eintrag wird dem Nutzer nicht angezeigt, da er defaultmäßig mit dem einstellenden Nutzer belegt ist. Der Nutzer kann weitere Autoren angeben.
authorPerson	ja	leer	ja	
authorInstitution	ja	leer	ja	
authorRole	ja	leer	ja	value set authorRole
authorSpecialty	ja	leer	ja	
authorTelecommunication	ja	leer	ja	
availabilityStatus	nein			nicht genutzt

classCode	ja	"DOK" (Dokumente ohne besondere Form (Notizen))	ja	value set classCode
comments	nein			nicht genutzt
confidentialityCode	ja	"PAT"	ja	value set confidentialityCode Der Wert "PAT" muss gesetzt werden. Weitere Werte außer "LEI", "KTR" und "LEÄ" sind möglich.
creationTime	ja	Systemzeit	ja	
entryUUID	nein	vom FdV vergeben	nein	
eventCodeList	ja	"H1" (vom Patienten mitgebracht)	ja	value set eventCodeList
formatCode	ja	"urn:ihe:iti:xds:2017:mimeType Sufficient"	nein	aus Dokument zu bestimmen value set formatCode
hash	nein	durch FdV berechnet	nein	
healthcareFacilityTypeCode	ja	'PAT' (Patient außerhalb der Betreuung)	ja	value set healthcareFacilityTypeCode
homeCommunityId	nein	aus Session-Daten	nein	
languageCode	ja	"de-DE"	ja	
legalAuthenticator	nein			nicht genutzt
limitedMetadata	nein	X	nein	
mimeType	ja	aus Eigenschaft der Datei (bspw. Dateiendung oder Zuordnung einer XML-Datei zu	nein	

		einem XML-Schema)		
objectType	nein	"urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1"	nein	
patientId	nein	aus Session-Daten	nein	
practiceSettingCode	ja	"PAT" (Patient außerhalb der Betreuung)	ja	value set practiceSettingCode
referenceIdList	nein			
repositoryUniqueId	nein	entspricht homeCommunityId	nein	
serviceStartTime	ja		ja	
serviceStopTime	ja		ja	
size	ja	vom FdV berechnet	nein	Es ist die Größe des verschlüsselten Dokumentes anzuzeigen.
sourcePatientId	nein			nicht verwendet
sourcePatientInfo	nein			nicht verwendet
title	ja	leer	ja	
typeCode	ja	"PATD" (Patienteneigene Dokumente)	ja	value set typeCode
uniqueId	nein	vom FdV vergeben	nein	
URI	ja	Dateiname	nein	
Metadatenelement Submission Set				
author				

authorPerson	nein	Vorname, Nachname und Titel aus Authentisierungszertifikat des Nutzers	nein	
authorInstitution	nein	leer	nein	
authorRole	nein	"11" (Dokumentierender)	nein	value set authorRole
authorSpecialty	nein	leer	nein	
authorTelecommunication	nein	leer	nein	
availabilityStatus	nein			nicht verwendet
comments	nein			nicht verwendet
contentTypeCode	nein	8 (Veranlassung durch Patient)	nein	value set contentTypeCode
entryUUID	nein	vom FdV vergeben	nein	
homeCommunityId	nein	aus Session-Daten	nein	
intendedRecipient	nein			nicht verwendet
limitedMetadata	nein	X	nein	
patientId	nein	aus Session-Daten	nein	
sourceId	nein	leer	nein	
submissionTime	nein	Systemzeit	nein	
title	nein			nicht verwendet

uniqueId	nein	vom FdV vergeben	nein	

Für value sets siehe [gemSpec_DM_ePA].

A_15287 - ePA-Frontend des Versicherten: Eingabe Metadaten für Dokument einstellen

Das ePA-Frontend des Versicherten MUSS dem Nutzer beim Einstellen von Dokumenten die Metadatenattribute gemäß Tab_FdV_125 anzeigen und gemäß Tab_FdV_125 zum Editieren anbieten.[<=]

Das FdV soll für die Eingabe von Metadaten required-Attribute als Pflichtfelder kennzeichnen.

A_15563 - ePA-Frontend des Versicherten: Eingabe Metadaten - Defaultwerte

Das ePA-Frontend des Versicherten MUSS Felder für die Eingabe von Metadaten gemäß Tab_FdV_125 vorbelegen. [<=]

Defaultmäßig wird der Nutzer als Submission Set author (Einstellender) gesetzt. Die Werte für den author werden mit den Informationen givenname, surname und title aus den subject des C.CH.AUT bzw. C.CH.AUT_ALT Zertifikates vorbelegt. Das Zertifikat wird im Anwendungsfall "Login Aktensession" in die Session-Daten übernommen.

Gemäß den Festlegungen in [\[gemSpec_DM_ePA#A_14760\]](#) muss ein Document Entry author (Ersteller) dem Eintrag bei Submission Set author (Einstellender) entsprechen. Dieser Document Entry author muss nicht angezeigt werden. Der Nutzer kann zusätzliche Document Entry author (Ersteller) erfassen.

Entsprechend den Nutzungsvorgaben für die Verwendung von XDS-Metadaten sind für einzelne Attribute Value Sets zu verwenden. Für eine bessere Bedienbarkeit bei der Eingabe der Metadaten werden die in der GUI auswählbaren Werte defaultmäßig auf einen Teil des Value Sets gemäß [\[gemSpec_DM_ePA#Vorschläge zur verkürzten Ansicht der Auswahl von Werten aus Value Sets\]](#) eingeschränkt. Über die Konfiguration der Applikation hat der Nutzer die Möglichkeit, die anzuzeigenden Werte zu ändern, d.h. nicht angezeigte Werte aus dem Value Set hinzuzunehmen oder angezeigte Werte zu verbergen.

Das FdV soll dem Nutzer in der GUI für Attribute von Metadaten, welche entsprechend einem Value Set belegt werden, eine konfigurierbare Auswahl anbieten. Wenn das Attribut optional ist, dann muss die Auswahl einen leeren Eintrag beinhalten.

A_15291 - ePA-Frontend des Versicherten: Schlüsselwerte aus Value Sets decodieren

Das ePA-Frontend des Versicherten MUSS Schlüsselwerte aus Value Sets decodieren und in einem für den Nutzer verständlichen Text anzeigen.[<=]

5.4.5 Konfiguration des FdV

Im Folgenden sind Konfigurationsparameter beschrieben, deren Werte für die Nutzung der Schnittstellen benötigt werden. Darüber hinaus kann der Hersteller des FdV zusätzliche Konfigurationsparameter definieren.

A_15292 - ePA-Frontend des Versicherten: Parameter speichern und laden

Das ePA-Frontend des Versicherten MUSS die Parameter aus TAB_FdV_104 persistent speichern und zum Start der Applikation laden.

Tabelle 6: TAB_FdV_104 – Parameter FdV

Parameter	Beschreibung	Wertebereich (Default Wert)
Aktenkontoinhaber: Akten-ID	Akten-ID (RecordIdentifier) des Aktenkontos für den Versicherten	siehe Bildungsvorschrift gemäß [gemSpec_DM_ePA#RecordIdentifier]
Aktenkontoinhaber: FQDN Anbieter ePA-Aktensystem	FQDN für den Zugriff auf das ePA-Aktensystem des zugehörigen Anbieters für den Versicherten	
Aktenkontoinhaber: Anbieter-ID	"HomeCommunityId" des ePA-Aktensystems Der Parameter wird mittels Abfrage des Namensdienstes im Internet bestimmt. Er wird durch das FdV automatisch gesetzt und ist nicht durch den Nutzer konfigurierbar.	siehe [gemSpec_DM_ePA]
Aktenkontoinhaber: Geräteidentifikator	Von der Autorisierung einmalig übermittelte Zufallszahl. Wird durch das FdV übernommen und ist nicht durch den Nutzer konfigurierbar. Der Parameter wird nicht angezeigt.	base64Binary, 120 Zeichen
Aktenkontoinhaber: Letzte Anmeldung zum Aktenkonto	Zeitpunkt des letzten erfolgreichen Login des Nutzers in das Aktenkonto von dem Gerät. Dient der Auswahl der Benachrichtigungen; Der Parameter wird durch das FdV automatisch gesetzt und ist nicht durch den Nutzer konfigurierbar.	Timestamp
für jede Vertretung: Name des Versicherten	Name des zu vertretenden Versicherten Der Datensatz Vertretung (Versicherten Name, Akten-ID, ...) muss für mehrere Vertretungen konfigurierbar sein.	
für jede Vertretung: Akten-ID	Akten-ID (RecordIdentifier) des Aktenkontos für den zu vertretenden Versicherten	siehe Bildungsvorschrift gemäß [gemSpec_DM_ePA#RecordIdentifier]

für jede Vertretung: FQDN Anbieter ePA-Aktensystem	FQDN für den Zugriff auf das ePA-Aktensystem des zugehörigen Anbieters für den zu vertretenden Versicherten	
für jede Vertretung: Anbieter-ID	"HomeCommunityId" des ePA-Aktensystems Der Parameter wird mittels Abfrage des Namensdienstes im Internet bestimmt. Er wird durch das FdV automatisch gesetzt und ist nicht durch den Nutzer konfigurierbar.	siehe [gemSpec_DM_ePA]
für jede Vertretung: Versicherten-ID des zu Vertretenden	unveränderlicher Teil der KVNR des zu Vertretenden	alphanummerisch, 10-stellig
für jede Vertretung: Geräteidentifikator	Von der Autorisierung einmalig übermittelte Zufallszahl. Wird durch das FdV übernommen und ist nicht durch den Nutzer konfigurierbar. Der Parameter wird nicht angezeigt.	base64Binary, 120 Zeichen
für jede Vertretung: letzte Anmeldung zum Aktenkonto	Zeitpunkt des letzten erfolgreichen Login des Nutzers in das Aktenkonto von dem Gerät. Dient der Auswahl der Benachrichtigungen. Der Parameter wird durch das FdV automatisch gesetzt und ist nicht durch den Nutzer konfigurierbar.	Timestamp
Benachrichtigungen aktivieren	Benachrichtigung über neue, geänderte oder gelöschte ePA-Dokumente	ja/nein Default: ja
Benachrichtigungszeitraum		Optionen: <ul style="list-style-type: none"> • seit der letzten Anmeldung • durch den Versicherten einstellbarer, flexibel zurückliegender Zeitraum • zurückliegender Zeitraum (x Wochen, x Monate) beginnend mit einem konkreten Datum Default: seit der letzten Anmeldung
Dokumente einstellen:	gibt an, ob im Anwendungsfall	ja/nein

Berechtigte anzeigen	Dokumente einstellen die Liste der für den Zugriff Berechtigten vor dem Hochladen angezeigt wird.	Default: ja
Gerätenamen	Bezeichnung des GdV durch den Nutzer, um es im Freischaltprozess und während der Geräteverwaltung leichter wiedererkennen zu können. Bildet zusammen mit dem Geräteidentifikator die Geräteerkennung (DeviceID). Die Geräteerkennung wird für die Geräteautorisierung genutzt.	alphanummerisch, 64 Zeichen

[<=]

Entsprechend dem für die Akten-ID spezifizierten Format, besitzt die Akten-ID einen variablen und einen konstanten Anteil. Der variable Anteil entspricht der Versicherten-ID, welche bspw. auf der eGK des Versicherten aufgedruckt ist. Das Erfassen der Akten-ID kann auf die Versicherten-ID beschränkt werden und automatisch um die konstanten Anteile ergänzt werden.

A_15634 - ePA-Frontend des Versicherten: Anbieter-ID aus Namensdienst ermitteln

Das ePA-Frontend des Versicherten SOLL die Parameter "Aktenkontoinhaber: Anbieter-ID" und "Vertreter: Anbieter-ID" mittels DNS des Anbieters des ePA-Aktensystems im Internet auf Basis des FQDN des ePA-Aktensystems ermitteln.

Resource Record: ePA_FQDN, TXT Record: hcid[<=]

A_15293 - ePA-Frontend des Versicherten: Konfigurationsparameter verwalten

Das ePA-Frontend des Versicherten MUSS dem Nutzer ermöglichen, die nicht automatisch bestimmbar Parameter aus TAB_FdV_104 zu verwalten (anzeigen, ändern, löschen).[<=]

A_17088 - ePA-Frontend des Versicherten: Kopplung an spezifisches ePA-Aktensystem

Der Hersteller des ePA-Frontends des Versicherten KANN die Parameter für die Identifikation des zu nutzenden ePA-Aktensystems fest vorgeben und eine Konfiguration durch den Nutzer unterbinden.[<=]

Das entspricht den folgenden Parametern aus TAB_FdV_104 für Aktenkontoinhaber und für jede Vertretung:

- FQDN Anbieter ePA-Aktensystem,
- Anbieter-ID.

6 Funktionsmerkmale

6.1 Allgemein

6.1.1 Aktensession-Verwaltung

Eine Aktensession in einem FdV bezeichnet die Sitzung eines Nutzers, in der dieser fachliche Anwendungsfälle im Aktenkonto eines Versicherten ausführt. Hierbei kann es sich um das Aktenkonto des Nutzers selber (Nutzer ist Aktenkontoinhaber) oder um das Aktenkonto eines zu vertretenden Versicherten handeln, wenn dieser eine entsprechende Vertretung für den Nutzer eingerichtet hat.

Ein Aktenkonto wird eindeutig durch eine Akten-ID (RecordIdentifier, siehe [IgemSpec_DM_ePA#RecordIdentifier](#)) referenziert. Der RecordIdentifier für sein eigenes Aktenkonto wird dem Versicherten als Ergebnis der Eröffnung des Aktenkontos mitgeteilt. Wenn der Nutzer die Vertretung eines anderen Versicherten wahrnimmt, dann erhält der Nutzer den RecordIdentifier von dem zu Vertretenden.

Eine Aktensession im FdV beginnt mit dem Login und endet mit dem Logout des Nutzers aus dem Aktenkonto. Das Logout erfolgt auf Wunsch des Nutzers, mittels eines Time-outs oder nach einem Fehler beim Login.

A_15294 - ePA-Frontend des Versicherten: Login nach Notwendigkeit

Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "Login Aktensession" vor der Ausführung einer fachlichen Operation, welche eine Kommunikation mit dem ePA-Aktensystem beinhaltet, starten, wenn im Rahmen der internen Session-Verwaltung keine gültigen Session-Daten vorhanden sind.[<=]

Das Login kann explizit nach Auswahl eines Aktenkontos im FdV durch den Nutzer ausgeführt werden.

A_17505 - ePA-Frontend des Versicherten: Auswahl Versichertenidentität

Das ePA-Frontend des Versicherten MUSS dem Nutzer die Möglichkeit geben, für eine Aktensession anstelle der eGK eine alternative Identität des Versicherten zu verwenden, falls der Nutzer diese alternative Versichertenidentität zuvor im FdV bekannt gemacht hat. [<=]

Falls eine Auswahl zwischen eGK und alternativer Versichertenidentität durch den Nutzer getroffen wurde, kann diese in der Konfiguration gespeichert werden.

A_15295 - ePA-Frontend des Versicherten: Beenden der Session

Das ePA-Frontend des Versicherten MUSS zum Beenden der Aktensession den Anwendungsfall "Logout Aktensession" ausführen.[<=]

A_15296 - ePA-Frontend des Versicherten: Abmeldung des Nutzers nach Inaktivität

Das ePA-Frontend des Versicherten MUSS den Nutzer nach spätestens 20 Minuten Inaktivität (Zeitspanne nach der letzten Nutzer-Aktivität) automatisch abmelden und die Aktensession beenden.[<=]

Das FdV kann dem Nutzer vor der Abmeldung wegen Inaktivität einen Hinweis einblenden, der es dem Nutzer ermöglicht, die Aktensession fortzuführen.

Für die Dauer der Aktensession benötigt das FdV einen gültigen Authentisierungstoken. Dieser wird in der Aktivität "Authentisieren des Nutzers" im Anwendungsfall "Login

Aktensession" erstmalig ausgestellt. Der Authentisierungstoken hat eine Gültigkeitsdauer von 5 min und kann über einen Zeitraum von 120 min erneuert werden. Nach diesem Zeitraum muss sich der Nutzer neu einloggen.

A_17543 - ePA-Frontend des Versicherten: periodisch Authentisierungstoken erneuern

Das ePA-Frontend des Versicherten MUSS vor Ablauf der Gültigkeit des Authentisierungstoken versuchen, mit der Aktivität "Authentisierungstoken erneuern" einen neuen Authentisierungstoken zu erhalten.[<=]

Der Zeitpunkt zum Erneuern soll so gewählt werden, dass bei einem Fehlschlagen der Operation je nach Fehlermeldung die Aktivität noch einmal ausgeführt werden kann, bzw. eine erneute Authentisierung gestartet werden kann.

Zu einer Aktensession im FdV gehören Session-Daten, welche vom FdV für die Dauer der Aktensession vorzuhalten sind. Die Session-Daten beinhalten u.a. die in TAB_FdV_105 gelisteten Informationen. Eine vollständige Auflistung ist in "7. Informationsmodell 7. Informationsmodell" beschrieben.

Tabelle 7: TAB_FdV_105 – Session-Daten

Authentisierungstoken	Authentifizierungsbestätigung
Autorisierungstoken	Autorisierungsbestätigung
Aktenschlüssel	Symmetrischer Schlüssel, der alle Dokumente eines Versicherten schützt, indem der Aktenschlüssel die zu den Dokumenten gehörigen Dokumentenschlüssel verschlüsselt.
Kontextschlüssel	Symmetrischer Schlüssel mit dem Metadaten der Dokumente, Policy Documents für die Zugriffssteuerung und das Zugriffsprotokoll für die persistente Speicherung im ePA-Aktensystem verschlüsselt werden.

Die Informationen zu diesen Session-Daten ergeben sich aus dem Anwendungsfall "Login Aktensession".

Nach dem Ende der Aktensession (Anwendungsfall "Logout") werden die Session-Daten verworfen.

6.1.2 Kommunikation mit dem ePA-Aktensystem

Das FdV nutzt TLS-Verbindungen für die Kommunikation zum ePA-Aktensystem. Es verbindet sich mit der Komponente Zugangsgateway des Versicherten. Das FdV führt eine Authentisierung des Servers durch, wobei sich das Zugangsgateway mittels eines öffentlich prüfbaren Zertifikats authentisiert. Für die TLS-Verbindung gelten die Vorgaben aus [gemSpec_Krypt].

Der Anbieter des ePA-Aktensystems, welchen der Versicherte gewählt hat, teilt dem Versicherten einen FQDN für den Zugriff auf das ePA-Aktensystem mit. Im Falle einer Vertretung, muss der zu Vertretende dem Vertretenden den FQDN für den Zugriff auf das ePA-Aktensystem mitteilen.

A_15302 - ePA-Frontend des Versicherten: Lokalisierung Zugangsgateway für Versicherte

Das ePA-Frontend des Versicherten MUSS den Endpunkt für die Kommunikation mit dem Zugangsgateway für Versicherte mittels öffentlicher DNS-Dienste auf Basis des FQDN des ePA-Aktensystems ermitteln.[<=]

Falls für den FQDN mehrere IP-Adressen hinterlegt sind, wählt das FdV zufällig eine der IP-Adressen als Endpunkt für den Verbindungsaufbau aus. Die Komponente Zugangsgateway des Versicherten weist bei Vollausslastung der Systemressourcen im ePA-Aktensystem die Verbindungsanfrage ab. In diesem Fall kann das FdV zufällig eine der weiteren IP-Adressen für einen neuen Verbindungsaufbau auswählen.

Jeder Anbieter eines ePA-Aktensystem verwaltet in den Nameservern Internet Resource Records zur Ermittlung der Aufruf-Schnittstellen seiner Module (siehe [IgemSpec_Aktensystem#A_14128 - Anbieter ePA-Aktensystem - Resource Records FQDN ePA](#)). Die einzelnen Module werden mit Key/Value Paaren der TXT-Records mit den Kürzeln in TAB_FdV_106 identifiziert.

Tabelle 8: TAB_FdV_106 – DNS RR ePA-Aktensystem Komponenten

ePA-Aktensystem / TI-Komponente	Resource Record	TXT-Record	<path> für Schnittstelle
Authentisierung	ePA_FQDN	authn	I_Authentication_Insurant
Autorisierung	ePA_FQDN	authz	I_Authorization_Insurant I_Authorization_Management_Insurant
Dokumentenverwaltung	ePA_FQDN	docv	I_Account_Management_Insurant I_Document_Management_Connect I_Document_Management_Insurant
Status Proxy (OCSP Responder)	ePA_FQDN	ocspf	I_OCSP_Status_Information
Verzeichnisdienst Proxy	ePA_FQDN	avzd	I_Proxy_Directory_Query
Schlüsselgenerierungsdienst Typ 1	ePA_FQDN	sgd1	
Schlüsselgenerierungsdienst Typ 2	ePA_FQDN	sgd2	

Die URL wird entsprechend den Vorgaben in [IgemSpec_Aktensystem#A-17969 - Anbieter ePA-Aktensystem - Schnittstellenadressierung](#) gebildet.

A_15297 - ePA-Frontend des Versicherten: Kommunikation über TLS-Verbindung

Das ePA-Frontend des Versicherten MUSS mit dem Zugangsgateway des Versicherten ausschließlich über TLS kommunizieren. [<=]

A_15298 - ePA-Frontend des Versicherten: Unzulässige TLS-Verbindungen ablehnen

Das ePA-Frontend des Versicherten MUSS bei jedem Verbindungsaufbau das Zugangsgateway des Versicherten anhand seines TLS-Zertifikats authentifizieren und MUSS die Verbindungen ablehnen, falls die Authentifizierung fehlschlägt.[<=]

Das Zugangsgateway für Versicherte authentisiert sich mit einem extended-validation-X.509-Zertifikat. Für Kriterien zur Prüfung des Zertifikates siehe "6.1.5- Zertifikatsprüfung".

Es gelten die Bedingungen für das TLS-Handshake gemäß [gemSpec_PKI#GS-A_4662].

A_15299 - ePA-Frontend des Versicherten: eine TLS-Verbindung pro Session

Das ePA-Frontend des Versicherten MUSS für jede Aktensession genau eine TLS-Verbindung nutzen.[<=]

Für jede Aktensession wird eine separate TLS-Verbindung genutzt.

A_15300 - ePA-Frontend des Versicherten: TLS-Verbindungsaufbau nach Notwendigkeit

Das ePA-Frontend des Versicherten MUSS eine TLS-Verbindung zum Zugangsgateway des Versicherten aufbauen, wenn die ausgeführte Operation eine Kommunikation zum ePA-Aktensystem oder den zentralen Diensten der TI beinhaltet und keine TLS-Verbindung zum Zugangsgateway des Versicherten für die Aktensession besteht.[<=]

A_15301 - ePA-Frontend des Versicherten: TLS-Verbindung beenden

Das ePA-Frontend des Versicherten MUSS die für eine Aktensession aufgebaute TLS-Verbindung zum Zugangsgateway des Versicherten schließen, wenn die Aktensession beendet wird.[<=]

A_15303 - ePA-Frontend des Versicherten: SOAP-Responses valide

Das ePA-Frontend des Versicherten MUSS bei allen SOAP-Responses eine Schemaprüfung durchführen und mit einer qualifizierten Fehlermeldung abbrechen, wenn die Nachricht nicht valide ist.[<=]

6.1.3 Sicherer Kanal zur Dokumentenverwaltung

Die Kommunikation zur Dokumentenverwaltung wird zusätzlich zu TLS über einen sicheren Kanal zwischen FdV und der Vertrauenswürdigen Ausführungsumgebung (VAU) in der Dokumentenverwaltung gesichert. Die Dokumentenverwaltung bietet dem FdV die folgenden Operationen ausschließlich über einen sicheren Kanal an:

- I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b
- I_Document_Management_Insurant::RegistryStoredQuery
- I_Document_Management_Insurant::RemoveDocuments
- I_Document_Management_Insurant::RetrieveDocumentSet
- I_Account_Management_Insurant::GetAuditEvents
- I_Account_Management_Insurant::SuspendAccount
- I_Account_Management_Insurant::ResumeAccount
- I_Document_Management_Connect::OpenContext
- I_Document_Management_Connect::CloseContext

A_15304 - ePA-Frontend des Versicherten: Umsetzung sicherer Kanal zur Dokumentenverwaltung

Das ePA-Frontend des Versicherten MUSS den im Rahmen des sicheren Verbindungsaufbaus mit der Dokumentenverwaltung ausgehandelten Sitzungsschlüssel verwenden, um den HTTP Body aller über den sicheren Kanal zu sendenden Requests an die Dokumentenverwaltung zu verschlüsseln und alle über den sicheren Kanal gesendeten Responses von der Dokumentenverwaltung zu entschlüsseln.[<=]

Für Informationen zum Kommunikationsprotokoll zwischen FdV und einer VAU siehe [\[gemSpec_Krypt#3.15 ePA-spezifische Vorgaben\]](#) und [\[gemSpec_Krypt#6 Kommunikationsprotokoll zwischen VAU und ePA-Clients\]](#).

6.1.4 Geräteautorisierung

Um einen möglichen Missbrauch und Identitätsdiebstahl erkennen zu können, wird eine Berechtigungsprüfung auf Geräteebeane auf Seiten der Versicherten umgesetzt. Der Zugriff auf ein Aktenkonto ist zulässig, wenn das Gerät, auf dem das FdV genutzt wird, durch den Nutzer über einen separaten Benachrichtigungskanal (E-Mail mit Freischalt-Link) zur Benutzung eines Aktenkontos autorisiert wurde. Siehe auch [\[gemSpec_Autorisierung#Freischaltprozess neuer Geräte\]](#).

Das Gerät wird durch die Geräteerkennung (DeviceID) identifiziert. Die Geräteerkennung beinhaltet die Geräteidentität und den Gerätenamen. Die Geräteidentität ist eine Zufallszahl, welche dem FdV von der Autorisierung übermittelt wird. Der Geräteiname ist ein bis zur 64 Zeichen langer String, welcher durch den Nutzer in der Konfiguration des FdV hinterlegt wird (siehe "[A_15292 - ePA-Frontend des Versicherten: Konfigurationsparameter verwalten](#)").

Beim erstmaligen Login des FdVs von einem GdV wird die Geräteerkennung mit leerem Geräteidentifikator (`phr:DeviceID::Device`) im Aufruf gesandt. Da noch kein bekannter Geräteidentifikator für dieses GdV in der Autorisierung registriert ist, antwortet die Autorisierung mit dem Fehler DEVICE_UNKNOWN und einer Zufallszahl im Fehlertext. Das FdV speichert die Zufallszahl als Geräteidentifikator lokal und verwendet sie in allen Aufrufen gegenüber der Komponente Autorisierung.

A_15305 - ePA-Frontend des Versicherten: Geräteidentifikator abspeichern

Das ePA-Frontend des Versicherten MUSS einen von der Autorisierung übermittelte Geräteidentifikator nutzer- und aktenkontospezifisch abspeichern. [\leq]

A_15306 - ePA-Frontend des Versicherten: DeviceID bilden

Das ePA-Frontend des Versicherten MUSS beim Start der Applikation nutzer- und aktenkontospezifisch die DeviceID aus der Geräteidentität und dem Gerätenamen aus der Konfiguration bilden und für Aufrufe an der Schnittstelle zur Komponente Autorisierung verwenden.

[\leq]

Für die Struktur von DeviceID siehe [PHR_Common.xsd].

6.1.5 Zertifikatsprüfung

Das FdV verwendet bei den in TAB_FdV_110 dargestellten Aktivitäten Zertifikate.

Tabelle 9 : TAB_FdV_110 – Zertifikatsnutzung

Aktivität	Zertifikat der TI	Zertifikatstyp	Rollen-OID	Nutzung
Einlesen der eGK	ja	C.CH.AUT	oid_egk_aut	passiv
TLS-Verbindungsaufbau zum Zugangsgateway des Versicherten	nein	TLS Internet Zertifikat	n/a	aktiv

Authentisierung	ja	C.CH.AUT C.CH.AUT_ALT	oid_egk_aut oid_egk_aut_alt	passiv
Aufbau sicherer Kanal zur VAU	ja	C.FD.AUT	oid_epa_vau	aktiv

Es gelten folgende übergreifende Festlegungen für die Prüfung aktiv durch das FdV genutzter Zertifikate.

A_15872 - ePA-Frontend des Versicherten: verpflichtende Zertifikatsprüfung

Das ePA-Frontend des Versicherten MUSS alle Zertifikate, die es aktiv verwendet (TLS-Verbindungsaufbau) auf Integrität und Authentizität prüfen. Falls die Prüfung kein positives Ergebnis ("gültig") liefert, so MUSS es die von dem Zertifikat und den darin enthaltenen Attributen (bspw. öffentliche Schlüssel) abhängenden Arbeitsabläufe ablehnen. Das ePA-Frontend des Versicherten MUSS alle öffentlichen Schlüssel, die es verwenden will, auf eine positiv verlaufene Zertifikatsprüfung zurückführen können. [≤=]

Ein Zertifikat aktiv verwenden bedeutet im Sinne von A_15872, dass ein FdV einen dort aufgeführten öffentlichen Schlüssel innerhalb einer kryptografischen Operation (Signaturprüfung, Verschlüsselung, Signaturprüfung von öffentlichen (EC)DH-Schlüsseln etc.) nutzt. Erhält ein FdV bspw. einen Access-Token, in dem Signaturen und Zertifikate enthalten sind und behandelt es diesen Token als opakes Datenobjekt, ohne die Zertifikate darin gesondert zu betrachten, dann verwendet das FdV diese Zertifikate im Sinne von A_15872 passiv.

6.1.5.1 Vertrauensanker des TI-Vertrauensraum

Der Vertrauensraum der TI ist in gemSpec_PKI#8.1 beschrieben. Für das FdV gelten abweichende Vorgaben, da das FdV nicht innerhalb der TI betrieben wird. Diese Abweichungen werden im Folgenden beschrieben.

Die Initialisierung des TI-Vertrauensraums und der Wechsel des TI-Vertrauensankers wird beim FdV durch die Bereitstellung der FdV Applikation durchgeführt.

A_17667 - ePA-Frontend des Versicherten: Behandlung des Vertrauensankers

Das ePA-Frontend des Versicherten MUSS den aktuellen TI-Vertrauensanker (TSL-Signer-CA-Zertifikat) im Auslieferungszustand der Applikation integer und authentisch mit sich führen.

Dabei MUSS der TI-Vertrauensanker fest mit dem Code der Applikation verbunden sein, d.h. eine Manipulation des TI-Vertrauensankers MUSS durch die Applikation erkannt werden.

Das ePA-Frontend des Versicherten MUSS bei einem angekündigten Wechsel des TI-Vertrauensankers den neuen TI-Vertrauensanker zusätzlich zum aktuell gültigen Vertrauensanker mit sich führen.

Das ePA-Frontend des Versicherten MUSS eindeutig identifizierte und während der Erstellung der Applikation mittels Fingerprint validierte TSL-Signer-CA-Zertifikate mit sich führen und ausschließlich diese als Vertrauensanker verwenden.

[≤=]

6.1.5.2 TSL-Behandlung

Folgende Vorgaben gelten für den Bezug und die Verarbeitung der TSL.

A_15874 - ePA-Frontend des Versicherten: Periodische Aktualisierung TI-Vertrauensraum

Das ePA-Frontend des Versicherten

MUSS zur periodischen Aktualisierung des TI-Vertrauensraums den TUC_PKI_001 mit folgenden Anpassungen umsetzen:

- Der Offline-Modus ist nicht zu berücksichtigen
- Auslöser: keine TSL lokal gespeichert oder die gespeicherte TSL ist zu alt (die in der TSL selbst kodierte Gültigkeitsdauer NextUpdate ist abgelaufen).
- Wenn innerhalb der letzten 24 Stunden keine Prüfung erfolgte, dann muss das ePA-Frontend des Versicherten prüfen, ob eine neuere TSL zur Verfügung steht. Falls eine neuere TSL am Downloadpunkt bereit steht, so muss das ePA-Frontend des Versicherten die neuere TSL herunterladen.

Das ePA-Frontend des Versicherten MUSS zum Prüfen der Aktualität und dem Herunterladen der TSL(ECC-RSA) die vom Zugangsgateway des Versicherten angebotene Schnittstelle verwenden.

[<=]

Für die Spezifikation der Schnittstelle siehe [\[gemSpec_Zugangsgateway_Vers#A_15868 - Zugangsgateway des Versicherten, Bereitstellung TSL\]](#).

Der Aufbau und der Inhalt der TSL sind durch [ETSI_TS_102_231_V3.1.2] gegeben und in [\[gemSpec_TSL#7\]](#) beschrieben.

A_16489 - ePA-Frontend des Versicherten: TSL - Prüfung Integrität und Authentizität

Das ePA-Frontend des Versicherten MUSS die Integrität und Authentizität der heruntergeladenen TSL prüfen. Falls die Prüfung kein positives Ergebnis liefert, so MUSS die gerade heruntergeladene TSL verworfen werden.

[<=]

Die Bedingungen an den Vertrauensstatus der TSL sind in gemSpec_TSL#8.2.2 beschrieben. Für das ePA-Frontend des Versicherten gilt eine "TSL-Graceperiod" von 0 Tagen, d.h., die TSL-Informationen sind nicht mehr vertrauenswürdig, wenn das aktuelle Datum nach dem Datum nextUpdate der TSL liegt.

A_17732 - ePA-Frontend des Versicherten: TSL - Truststore für Zertifikatsprüfung

Das ePA-Frontend des Versicherten MUSS die TSL auswerten, um aus den Inhalten einen Truststore für die durchzuführenden Zertifikatsprüfungen zu bilden. [<=]

Für das FdV sind ausschließlich die TSP-Dienste mit dem ServiceType SvcType/CA/PKC gem. gemSpec_TSL#TIP1-A_4099 relevant.

Hinweis: Eine Möglichkeit zur Umsetzung ist, im Rahmen der Aktualisierung der TSL (vgl. A_15874) nach positiver Prüfung der TSL-Signatur die CA-Zertifikate aus der TSL in zwei verschiedene zugriffsgeschützte Verzeichnisse zu legen: einmal für HBA/SMC-B/eGK-CAs und einmal für CAs der Komponenten-PKI der TI. Die beiden Verzeichnisse dienen dann als Truststore für die Zertifikatsprüfung, womit sich die Umsetzungskomplexität der Vorgabe aus A_15873 Punkt 2 reduziert.

A_16490 - ePA-Frontend des Versicherten: TSL nicht verfügbar

Das ePA-Frontend des Versicherten MUSS, falls keine nach A_16489 erfolgreich geprüfte TSL zur Verfügung steht oder das aktuelle Datum nach dem Datum nextUpdate der TSL liegt, den Vertrauensraum als ungültig betrachten und sicherstellen, dass alle Zertifikatsprüfungen für TI-Zertifikate mit "ungültig" bewertet werden. [<=]

Hinweis: Es ist in Bezug auf die CC-Evaluierung hilfreich, wenn die TSL-Signaturprüfung mit einer speziell dafür geschriebenen (und gehärteten) Programmkomponente

durchgeführt wird. Bei einer anschließenden XML-Auswertung der TSL mit einer Standard-XML-Bibliothek können die verarbeiteten XML-Daten dann als vertrauenswürdig angesehen werden.

6.1.5.3 Zertifikatsprüfung von Zertifikaten der TI

In der folgenden Anforderung sind die Schritte zum Prüfen eines Zertifikates der TI beschrieben. In den Schritten werden TUC_PKI_* referenziert. Sie dienen als Rahmen für den Ablauf der Prüfschritte. Die TUC_PKI_* sind in dieser Afo nicht normativ umzusetzen.

A_15873 - ePA-Frontend des Versicherten: Prüfung TI-Zertifikate

Das ePA-Frontend des Versicherten MUSS bei der Prüfung von X.509-Zertifikaten der TI folgende Prüfschritte durchlaufen.

1. Prüfung der zeitlichen Gültigkeit des Zertifikats auf Basis der aktuellen Systemzeit (orientiert an gemSpec_PKI#TUC_PKI_002)
2. Ist das Zertifikat kryptographisch (Signaturprüfung) rückführbar auf ein CA-Zertifikat aus einer authentischen und integeren und zeitlich gültigen TSL (vgl. A_15874)? (orientiert an [gemSpec_PKI#TUC_PKI_003 und TUC_PKI_004])
3. Prüfung auf den für den Anwendungsfall korrekten Zertifikatstyp gemäß TAB_FdV_110. Die OID des Zertifikatstyps gemäß [gemSpec_OID] muss in der Extension CertificatePolicies enthalten sein.
4. Falls das Zertifikat für den Aufbau des sicheren Kanals zur VAU verwendet wird (VAU-Zertifikat innerhalb des VAU-Protokolls, vgl. [gemSpec_Krypt#Kommunikationsprotokoll zwischen VAU und ePA-Clients]), so MUSS die Rolle "oid_epa_vau" gemäß [\[gemSpec_OID#GS-A_4446\]](#) im EE-Zertifikat aufgeführt sein (analog gemSpec_PKI#TUC_PKI_009). Falls nein, MUSS das Zertifikat für den Aufbau des sicheren Kanals zur VAU abgelehnt werden.
5. Falls das Zertifikat ein EE-Zertifikat ist: Ermittlung der OCSP-Statusinformation. Ist das Zertifikat nicht gesperrt (Status "good" [RFC-6960#2.2 Response]) (vgl. A_15869)? Eine OCSP-Antwort KANN lokal maximal 4 Stunden gecacht und als Prüfgrundlage verwendet werden.
Die Prüfung ist analog gemSpec_PKI#TUC_PKI_006 mit den Parametern Referenzzeitpunkt=Systemzeit, OCSP-Graceperiod=4 Stunden.
6. Prüfung der Extensions KeyUsage und ExtendedKeyUsage auf die richtige Belegung gemäß dem Anwendungsfall (orientiert an gemSpec_PKI#TUC_PKI_018 Schritt 2).

Führt einer der Prüfschritte nicht zu einem positiven Prüfergebnis, so MUSS das Zertifikat abgelehnt werden und die weitere Verarbeitung des Zertifikats oder der Attribute darin abgelehnt werden.

Das ePA-Frontend des Versicherten muss die referenzierten gemSpec_PKI#TUC_PKI_* im Rahmen dieser Anforderung nicht normativ umsetzen.[<=]

Für die Prüfung des Online-Status von Zertifikaten der TI wird die Schnittstelle I_OCSP_Status_Information genutzt. Siehe [gemSpec_PKI#Kap9]. Die Schnittstelle wird durch den Status-Proxy der Komponente Zugangsgateway des Versicherten angeboten. siehe auch [\[gemSpec_Zugangsgateway_Vers#A_15869 - Zugangsgateway des Versicherten, Bereitstellung OCSP-Forwarder\]](#).

6.1.5.4 Zertifikatsprüfung von Internet-Zertifikaten

Folgende Vorgaben gelten für die Prüfung von Internet-Zertifikaten.

A_15887 - ePA-Frontend des Versicherten: Prüfung Internet-Zertifikate

Das ePA-Frontend des Versicherten MUSS für die Prüfung des internetseitigen Zertifikats des Zugangsgateways des Versicherten das Zertifikat auf ein CA-Zertifikat einer CA, die die "CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" (<https://cabforum.org/baseline-requirements-documents/>) erfüllt, kryptographisch (Signaturprüfung) zurückführen können. Ansonsten MUSS es das Zertifikat als "ungültig" bewerten.

Es MUSS die zeitliche Gültigkeit des Zertifikats prüfen. Falls diese Prüfung negativ ausfällt, muss es das Zertifikat als "ungültig" bewerten. [\leq]

Hinweis: Der erste Teil von A_15887 ist gleichbedeutend damit, dass das CA-Zertifikat im Zertifikats-Truststore eines aktuellen Webbrowsers ist.

6.2 Implementation ePA-Anwendungsfälle im FdV

In diesem Kapitel wird die Umsetzung der im systemspezifischen Konzept [gemSysL_ePA] spezifizierten Anwendungsfälle im FdV beschrieben.

Das ePA-Frontend des Versicherten kann zusätzliche Funktionalitäten enthalten, sofern diese nicht den Schutz der personenbezogenen und medizinischen Daten des Versicherten in ePA gefährden. Die zusätzlichen Funktionalitäten müssen sich von den Anwendungsfällen der ePA abgrenzen. Insbesondere muss dem Nutzer ersichtlich sein, wenn Daten den Kontext der ePA verlassen.

6.2.1 Übergreifende Festlegungen

Voraussetzung für die Nutzung des FdV ist das Vorhandensein eines Aktenkontos:

- Der Versicherte verfügt über ein aktiviertes Aktenkonto (Anderenfalls ist ausschließlich der Anwendungsfall für die Aktivierung des Aktenkontos ausführbar.).
- Die Akten-ID (der RecordIdentifier) des Aktenkontos, welche sich mittels der Versicherten-ID des Aktenkontoinhabers bestimmen lässt, ist im FdV bekannt.
- Der FQDN für den Zugriff auf das ePA-Aktensystem ist im FdV bekannt.

A_15567 - ePA-Frontend des Versicherten: Zulässigkeit der Anwendungsfälle

Das ePA-Frontend des Versicherten MUSS die Zulässigkeit des Anwendungsfalls in Abhängigkeit von folgenden Kriterien sicherstellen:

VerificationResult

- K1: Rolle des Nutzers (Aktenkontoinhaber, Vertreter)
- K3: falls eGK zur Authentisierung genutzt wird: Status PIN (MRPIN.home) der eGK:
[OK (PasswordEnabledVerified) / BLOCKED
(PasswordBlocked) / VERIFYABLE (PasswordEnabledNotVerified.X)]

Tabelle 10: TAB_FdV_161 – Zulässigkeit von Anwendungsfällen

Anwendungsfall	K1	K3
----------------	----	----

Login Aktensession	Aktenkontoinhaber Vertreter	OK VERIFYABLE
Logout Aktensession	Aktenkontoinhaber Vertreter	immer
Aktenkonto aktivieren	Aktenkontoinhaber	OK VERIFYABLE
Anbieter wechseln	Aktenkontoinhaber	OK VERIFYABLE
Berechtigung für LEI vergeben	Aktenkontoinhaber Vertreter	OK VERIFYABLE
Vertretung einrichten	Aktenkontoinhaber	OK VERIFYABLE
Berechtigung für Kostenträger vergeben	Aktenkontoinhaber Vertreter	OK VERIFYABLE
Vergebene Berechtigungen anzeigen	Aktenkontoinhaber Vertreter	OK VERIFYABLE
Eingerichtete Vertretungen auflisten	Aktenkontoinhaber Vertreter	immer
Berechtigung für LEI ändern	Aktenkontoinhaber Vertreter	OK VERIFYABLE
Berechtigung für LEI löschen	Aktenkontoinhaber Vertreter	OK VERIFYABLE
Berechtigung für Vertreter löschen	Aktenkontoinhaber	OK VERIFYABLE
Berechtigung für Kostenträger löschen	Aktenkontoinhaber Vertreter	OK VERIFYABLE
Dokumente einstellen	Aktenkontoinhaber Vertreter	OK VERIFYABLE
Dokumente suchen	Aktenkontoinhaber Vertreter	OK VERIFYABLE
Dokumente löschen	Aktenkontoinhaber Vertreter	OK VERIFYABLE
Dokumente herunterladen	Aktenkontoinhaber Vertreter	OK VERIFYABLE

Protokolldaten einsehen	Aktenkontoinhaber Vertreter	OK VERIFYABLE
PIN der eGK ändern	Aktenkontoinhaber Vertreter	OK VERIFYABLE
PIN der eGK mit PUK entsperren	Aktenkontoinhaber Vertreter	BLOCKED OK VERIFYABLE
Benachrichtigungsadresse für Geräteautorisierung aktualisieren	Aktenkontoinhaber Vertreter	OK VERIFYABLE

[<=]

Die Rolle des Nutzers kann durch den Vergleich der Versicherten-ID aus dem Authentisierungszertifikat der eGK (C.CH.AUT) bzw. der alternativen Versichertenidentität (C.CH.AUT_ALT) des Nutzers mit der Versicherten-ID aus der Akten-ID bestimmt werden.

6.2.2 Fehlerbehandlung

Tritt ein Fehler bei der Verarbeitung von Operationsaufrufen des ePA-Aktensystems auf, dann antworten die Komponenten des ePA-Aktensystems mit einer Fehlermeldung. Das Format und die verwendeten Fehlercodes sind in den Spezifikationen der Interfaces beschrieben. Weiterhin können Fehler in der lokalen Verarbeitung auftreten.

A_15307 - ePA-Frontend des Versicherten: Abbruch bei Fehler im Anwendungsfall

Das ePA-Frontend des Versicherten MUSS, wenn bei der Abarbeitung der Aktivitäten eines Anwendungsfalls ein Fehler auftritt und keine Fehlerbehandlung beschrieben ist, den Anwendungsfall abbrechen und dem Nutzer eine verständliche Fehlermeldung anzeigen.[<=]

Wenn die Möglichkeit besteht, dass der Nutzer das fehlerverursachende Problem selbst beheben kann, kann das FdV den Nutzer auf die Lösung hinweisen. Bspw. kann dem Nutzer bei einer gesperrten PIN der Anwendungsfall "PIN der eGK entsperren" angeboten werden.

A_15308 - ePA-Frontend des Versicherten: Anzeige von Handlungsmöglichkeiten im Fehlerfall

Das ePA-Frontend des Versicherten SOLL dem Nutzer im Fehlerfall einen Hinweis geben, wenn es für den Nutzer Handlungsmöglichkeiten dazu gibt.[<=]

A_15309 - ePA-Frontend des Versicherten: Anzeige im Fehlerfall

Das ePA-Frontend des Versicherten MUSS bei Auftreten der Fehlercodes aus TAB_FdV_107 und TAB_FdV_108 dem Nutzer den entsprechenden Fehlertext anzeigen und die spezifische Aktion durchführen.

Tabelle 11: TAB_FdV_107 – Behandlung von Fehlercodes von Plattformbausteinen

Fehlercode	Fehlertext	Spezifische Aktionen durch FdV
CardTerminated	Ihre Gesundheitskarte ist	

	gesperrt, bitte wenden Sie sich an Ihre Krankenkasse.	
MemoryFailure	Ihre Gesundheitskarte ist beschädigt, bitte wenden Sie sich an Ihre Krankenkasse.	
PasswordBlocked	Die PIN/PUK wurde – nach zu häufiger falscher PIN/PUK Eingabe – blockiert.	Eine Fehlermeldung anzeigen und dem Versicherten empfehlen, entweder die PIN mit Hilfe der PUK zu entsperren bzw. bei einer gesperrten PUK sich an seine Krankenkasse zu wenden.
WrongSecretWarning	Falsche PIN, verbleibende Eingabeversuche <x>	Eine Fehlermeldung mit der verbleibenden Anzahl der Eingabeversuche bis zur Sperrung der PIN anzeigen und erneute PIN-Eingabe ermöglichen.

Tabelle 12: TAB_FdV_108 – Behandlung von Fehlern des ePA-Aktensystems

Fehlercode	Fehlertext	Spezifische Aktion durch FdV
ASSERTION_INVALID		Das FdV kann versuchen die Authentisierung mittels der übergreifenden Aktivität "Authentisieren des Nutzers" zu aktualisieren und den Operationsaufruf wiederholen.
DEVICE_UNKNOWN	Das Gerät ist nicht für die Nutzung des Aktensystems registriert. Bitte führen Sie eine Geräteautorisierung durch, indem Sie den Link zur Freischaltung aufrufen, welcher Ihnen über eine E-Mail zugesendet wird.	Der Anwendungsfall wird abgebrochen.
wst:InvalidSecurityToken	Ihre Gesundheitskarte ist ungültig, bitte wenden Sie sich an Ihre Krankenkasse.	

[<=]

A_15310 - ePA-Frontend des Versicherten: Fehlerbehandlung ungültiger Token

Das ePA-Frontend des Versicherten MUSS, wenn eine Operation mit einer Fehlermeldung antwortet, welche auf einen ungültigen Authentisierungstoken oder ungültigen Autorisierungstoken verweist, den referenzierten Token aus den Session-Daten löschen.[<=]

A_15311 - ePA-Frontend des Versicherten: Aufrufparameter ungültig

Das ePA-Frontend des Versicherten MUSS bei allen Operationen mit einer qualifizierten Fehlermeldung abbrechen, wenn notwendige Aufrufparameter unvollständig, ungültig oder inkonsistent sind.[<=]

6.2.3 Aktivitäten

Dieser Abschnitt beschreibt Aktivitäten, welche durch verschiedene Anwendungsfälle genutzt werden.

6.2.3.1 Authentisieren des Nutzers

Mit dieser Operation authentisiert sich der Nutzer am ePA-Aktensystem. Das FdV erhält bei erfolgreicher Authentisierung einen Authentisierungstoken.

A_15312 - ePA-Frontend des Versicherten: Authentisieren des Nutzers

Das ePA-Frontend des Versicherten MUSS die Aktivität "Authentisieren des Nutzers" gemäß TAB_FdV_109 umsetzen.

Tabelle 13: TAB_FdV_109 – Authentisieren des Nutzers

I_Authentication_Insurant:: LoginCreateChallenge Request erstellen	RequestSecurityToken (RST) erstellen
I_Authentication_Insurant:: LoginCreateChallenge Response verarbeiten	RequestSecurityTokenResponse (RSTR) verarbeiten Rückgabedaten: <ul style="list-style-type: none"> • st:Challenge = Challenge
I_Authentication_Insurant:: LoginCreateToken Request erstellen	RequestSecurityTokenResponse (RSTR) erstellen Eingangsdaten: <ul style="list-style-type: none"> • wst:Challenge = Challenge aus RSTR Der Request wird signiert und die Signatur im SOAP Header eingefügt. <ul style="list-style-type: none"> • wsse:BinarySecurityToken = C.CH.AUT des Nutzers • ds:SignatureValue = signierter Hashwert
wenn Authentisierung mittels eGK: Plattformbaustein PL_TUC_SIGN_HASH_nonQES zum Signieren nutzen	Eingangsdaten: <ul style="list-style-type: none"> • Identifikator = für eGK G2: PrK.CH.AUT.R2048 für eGK höhere Generation: PrK.CH.AUT.E256 • Signaturverfahren = signPSS • Hashwert = soap:Body Die Challenge wird mittels PSOComputeDigitalSignatur von der eGK signiert. Für den Aufruf der Operation wird der Nutzer zur PIN-Eingabe (MRPIN.home) für seine eGK aufgefordert, falls der notwendige Sicherheitszustand der eGK noch nicht erreicht ist. Rückgabedaten: <ul style="list-style-type: none"> 7. OK + Hashsignatur oder

	8. Fehler
wenn Authentisierung mittels alternativer Versichertenidentität:	Aufruf der signaturdienstspezifischen Schnittstelle <code>I_Remote_Sign_Operations::sign_Data</code> Eine Beschreibung der konkreten Ausgestaltung der Schnittstelle befindet sich in [vesta]. Der Response liefert u.a. das C.CH.AUT_ALT. Dieses wird in die Session-Daten übernommen.
<code>I_Authentication_Insurant::LoginCreateToken</code> Response verarbeiten	<code>RequestSecurityTokenResponse</code> Collection (RSTRC) verarbeiten Rückgabedaten: <ul style="list-style-type: none"> <code>saml2:Assertion = AuthenticationAssertion</code> <code>AuthenticationAssertion</code> (Authentisierungstoken) in Session-Daten übernehmen
Fehlerbehandlung	Wenn der Response von <code>LoginCreateToken</code> den WS-Trust Fehler <code>wst:InvalidSecurityToken</code> liefert, dann ist die eGK des Nutzers ungültig. Der Nutzer muss aufgefordert werden, seine aktuell gültige eGK zu stecken oder sich an seine Krankenkasse zu wenden. Der Anwendungsfall wird abgebrochen.

[<=]

Die Dauer der Gültigkeit des Authentisierungstoken ist in [gemSpec_Authentisierung_Vers] beschrieben.

6.2.3.2 Authentisierungstoken erneuern

Mit dieser Operation kann das FdV den Authentisierungstoken am ePA-Aktensystem verlängern.

A_17541 - ePA-Frontend des Versicherten: Authentisierungstoken erneuern

Das ePA-Frontend des Versicherten MUSS die Aktivität "Authentisierungstoken erneuern" gemäß TAB_FdV_173 umsetzen.

Tabelle 14: TAB_FdV_173 – Logout - Authentisierungstoken abmelden

Vorbedingung	<code>AuthenticationAssertion</code> in Session-Daten
<code>I_Authentication_Insurant::RenewToken</code> Request erstellen	Eingangsdaten: <ul style="list-style-type: none"> <code>RenewTarget:</code> <code>AuthenticationAssertion</code> aus Session-Daten
<code>I_Authentication_Insurant::RenewToken</code> Response verarbeiten	<code>RequestSecurityTokenResponse</code> (RSTR) verarbeiten Rückgabedaten:

	<ul style="list-style-type: none"> RequestedSecurityToken = AuthenticationAssertion AuthenticationAssertion (Authentisierungstoken) in Session-Daten ersetzen.
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

[<=]

Der vorher genutzte Authentisierungstoken wird gelöscht.

Im Fehlerfall kann die Operation wiederholt oder eine neue Authentisierung des Nutzers gestartet werden.

6.2.3.3 Dokumentenset in Dokumentenverwaltung hochladen

Mit dieser Operation werden ein oder mehrere Dokumente in die Dokumentenverwaltung hochgeladen. Hierbei kann es sich entweder um durch den Nutzer ausgewählte (fachliche) Versichertendokumente oder um technische Dokumente (z.B. ein Policy Document) handeln. Eine Mischung beider Arten von Dokumenten innerhalb eines Dokumentensets ist nicht erlaubt.

A_15314 - ePA-Frontend des Versicherten: Dokumentenset in Dokumentenverwaltung hochladen

Das ePA-Frontend des Versicherten MUSS die Aktivität "Dokumentenset in Dokumentenverwaltung hochladen" gemäß TAB_FdV_111 umsetzen.

Tabelle 15: TAB_FdV_111 – Dokumentenset in Dokumentenverwaltung hochladen

I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b Request erstellen	Eingangsparameter: <ul style="list-style-type: none"> Provide And Register Document Set-b Message gemäß IHE XDS-Transaktion [ITI-41] AuthenticationAssertion aus Session-Daten
I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b Response verarbeiten	Rückgabedaten: <ul style="list-style-type: none"> Provide And Register Document Set-b Response Message gemäß IHE XDS-Transaktion [ITI-41]

[<=]

A_15315 - ePA-Frontend des Versicherten: IHE XDS-Transaktion [ITI-41]

Das ePA-Frontend des Versicherten MUSS für die Nutzung der Operation I_Document_Management_Insurant::ProvideAndRegisterDocumentSet-b gemäß der in [IHE-ITI-TF] definierten IHE XDS-Transaktion [ITI-41] "Provide & Register Document Set-b" als Akteur "Document Source" umsetzen.[<=]

Für die XDS-Metadaten von Dokumenten des Versicherten gelten die Nutzungsvorgaben aus [\[gemSpec_DM_ePA#A_14760 - Nutzungsvorgaben für die Verwendung von XDS-Metadaten\]](#). Für die XDS-Metadaten eines Policy Documents gelten die Nutzungsvorgaben aus [\[gemSpec_DM_ePA#A_14961 - Nutzungsvorgaben für die Verwendung von XDS-Metadaten bei Policy Documents\]](#).

A_15316 - ePA-Frontend des Versicherten: Upload verschlüsselter Versicherten-Dokumente

Das ePA-Frontend des Versicherten MUSS sicherstellen, dass Dokumente des Versicherten, welche in das ePA-Aktensystem eingestellt werden, verschlüsselt sind. [≤]

Technische Dokumente (Policy Documents) werden nach der Übertragung in das Aktenkonto durch die Dokumentenverwaltung ausgewertet.

A_17772 - ePA-Frontend des Versicherten: Upload unverschlüsselter technischer Dokumente

Das ePA-Frontend des Versicherten MUSS sicherstellen, dass technische Dokumente (Policy Documents) unverschlüsselt, d.h. nicht mit dem Aktenschlüssel verschlüsselt, in das ePA-Aktensystem eingestellt werden. [≤]

A_15972 - ePA-Frontend des Versicherten: Trennung fachlicher und technischer Dokumente beim Upload

Das ePA-Frontend des Versicherten MUSS sicherstellen, dass eine Provide And Register Document Set-b Message entweder ein oder mehrere Versichertendokumente oder genau ein technisches Dokument enthält. [≤]

A_16221 - ePA-Frontend des Versicherten: IHE XDS-Transaktion [ITI-41] - Unterstützung MTOM/XOP

Das ePA-Frontend des Versicherten MUSS bei der Umsetzung der IHE XDS-Transaktion [ITI-41] zur Übertragung von Dokumenten eine Kodierung mittels MTOM/XOP [MTOM] gemäß [IHE-ITI-TF2x#V.3.6.] verwenden. [≤]

Das ePA-Aktensystem lehnt beim Einstellen von Dokumenten Requests ab, wenn die Summe der Größe der Dokumente in einem Submission Set 250 MB überschreitet. Das FdV kann Einstellversuche von Dokumentensets unterbinden, wenn diese von der Dokumentenverwaltung aufgrund der Größenbeschränkung abgelehnt würden.

6.2.3.4 Dokumentenset aus Dokumentenverwaltung herunterladen

Mit dieser Operation werden ein oder mehrere Dokumente anhand der Document Unique IDs aus den XDS-Metadaten aus dem Aktenkonto heruntergeladen.

A_15317 - ePA-Frontend des Versicherten: Dokumentenset aus Dokumentenverwaltung herunterladen

Das ePA-Frontend des Versicherten MUSS die Aktivität "Dokumentenset aus Dokumentenverwaltung herunterladen" gemäß TAB_FdV_112 umsetzen.

Tabelle 16: TAB_FdV_112 – Dokumentenset aus Dokumentenverwaltung herunterladen

I_Document_Management_Insurant : : RetrieveDocumentSet Request erstellen	Eingangsparameter: <ul style="list-style-type: none"> RetrieveDocumentSet_Message gemäß IHE XDS-Transaktion [ITI-43] AuthenticationAssertion aus Session-Daten
I_Document_Management_Insurant : : RetrieveDocumentSet Response verarbeiten	Rückgabedaten: <ul style="list-style-type: none"> RetrieveDocumentSetResponse_Message gemäß IHE XDS-Transaktion [ITI-43] RetrieveDocumentSetResponse_Message beinhaltet ein oder mehrere Dokumente. Jedes medizinisches Dokument ist mit einem individuellen

	Dokumentenschlüssel verschlüsselt. Der Dokumentenschlüssel ist mit dem Aktenschlüssel verschlüsselt.
<p>für jedes medizinische Dokument aus RetrieveDocumentSetResponse_Messag e: Plattformbaustein PL_TUC_SYMM_DECIPHER nutzen</p> <p>Hinweis: Der Begriff "medizinische Dokumente" umfasst alle Dokumente, welche durch LEI, KTR oder Versicherte in das ePA-Aktensystem eingestellt wurden. Davon abgegrenzt werden die technischen Dokumente (Policy Documents). Sie werden unverschlüsselt übertragen.</p>	<p>Für Vorgaben zum Entschlüsseln eines Dokumentes aus dem ePA-Aktensystem siehe [gemSpec_DM_ePA#2.4.2 Entschlüsselung].</p> <p>Dokumentenschlüssel mit PL_TUC_SYMM_DECIPHER entschlüsseln Eingangsdaten:</p> <ul style="list-style-type: none"> • verschlüsselter Dokumentenschlüssel aus EncryptedData\EncryptedKey\CipherData • Aktenschlüssel (RecordKey) aus Session-Daten • Der optionale Parameter AD wird nicht verwendet. <p>Rückgabedaten:</p> <ul style="list-style-type: none"> • entschlüsselter Dokumentenschlüssel <p>Dokument mit PL_TUC_SYMM_DECIPHER entschlüsseln Eingangsdaten:</p> <ul style="list-style-type: none"> • verschlüsseltes Dokument aus EncryptedData\CipherData • entschlüsselter Dokumentenschlüssel • Der optionale Parameter AD wird nicht verwendet. <p>Rückgabedaten:</p> <ul style="list-style-type: none"> • entschlüsseltes Dokument

[<=]

A_15318 - ePA-Frontend des Versicherten: IHE XDS-Transaktion [ITI-43]

Das ePA-Frontend des Versicherten MUSS für die Nutzung der Operation I_Document_Management_Insurant::RetrieveDocumentSet gemäß der in [IHE-ITI-TF] definierten IHE XDS-Transaktion [ITI-43] "Retrieve Document Set" als Akteur "Document Consumer" umsetzen.[<=]

A_16222 - ePA-Frontend des Versicherten: IHE XDS-Transaktion [ITI-43] - MTOM unterstützen

Das ePA-Frontend des Versicherten MUSS bei der Umsetzung der IHE XDS-Transaktion [ITI-43] die Übertragung von Dokumenten mit MTOM/XOP [MTOM] unterstützen.[<=]

6.2.3.5 Dokumentenset in Dokumentenverwaltung löschen

Mit dieser Operation werden ein oder mehrere Dokumente anhand der Document Unique IDs aus den XDS-Metadaten im Aktenkonto gelöscht. Die XDS-Metadaten wurden vorab mit einer Suche nach Dokumenten im ePA-Aktensystem ermittelt.

A_15319 - ePA-Frontend des Versicherten: Dokumentenset in Dokumentenverwaltung löschen

Das ePA-Frontend des Versicherten MUSS die Aktivität "Dokumentenset in Dokumentenverwaltung löschen" gemäß TAB_FdV_113 umsetzen.

Tabelle 17: TAB_FdV_113 – Dokumentenset in Dokumentenverwaltung löschen

I_Document_Management_Insurant::Remove Documents Request erstellen	Eingangsdaten: <ul style="list-style-type: none"> • AuthenticationAssertion aus Session-Daten • RemoveDocuments_Message gemäß IHE RMD-Transaktion [ITI-86]
I_Document_Management_Insurant::Remove Documents Response verarbeiten	Rückgabedaten: <ul style="list-style-type: none"> • RemoveDocumentsResponse_Message gemäß IHE RMD-Transaktion [ITI-86]

[<=]

A_15320 - ePA-Frontend des Versicherten: IHE RMD-Transaktion [ITI-86]

Das ePA-Frontend des Versicherten MUSS die Nutzung der Operation

I_Document_Management_Insurant::RemoveDocuments gemäß der in [IHE-ITI-TF] definierten IHE RMD-Transaktion [ITI-86] "Remove Documents" als Akteur "Document Administrator" umsetzen. [<=]

6.2.3.6 Suche nach Dokumenten in Dokumentenverwaltung

Mit dieser Operation wird eine Suchanfrage über die XDS-Metadaten der Dokumente im Aktenkonto an die Dokumentenverwaltung gesendet.

A_15321 - ePA-Frontend des Versicherten: Suche nach Dokumenten in Dokumentenverwaltung

Das ePA-Frontend des Versicherten MUSS die Aktivität "Suche nach Dokumenten in Dokumentenverwaltung" gemäß TAB_FdV_114 umsetzen.

Tabelle 18: TAB_FdV_114 – Suche nach Dokumenten in Dokumentenverwaltung

I_Document_Management_Insurant::RegistryStoredQuery Request erstellen	Eingangsparameter: <ul style="list-style-type: none"> • query:AdhocQueryRequest_Message gemäß IHE XDS-Transaktion [ITI-18] • AuthenticationAssertion aus Session-Daten
I_Document_Management_Insurant::RegistryStoredQuery Response verarbeiten	Rückgabedaten: <ul style="list-style-type: none"> • query:AdhocQueryResponse_Message gemäß IHE XDS-Transaktion [ITI-18]

[<=]

A_15322 - ePA-Frontend des Versicherten: IHE XDS-Transaktion [ITI-18]

Das ePA-Frontend des Versicherten MUSS für die Nutzung der Operation `I_Document_Management_Insurant::RegistryStoredQuery` gemäß der in [IHE-ITI-TF] definierten IHE XDS-Transaktion [ITI-18] "Registry Stored Query" als Akteur "Document Consumer" umsetzen.[<=]

A_17854 - ePA-Frontend des Versicherten: Nutzung des Anfragetyps "FindDocumentsByTitle"

Das ePA-Frontend des Versicherten MUSS den in [ITI-18] nicht enthaltenen zusätzlichen Anfragetyp "FindDocumentsByTitle" mit der Query-ID "urn:uuid:ab474085-82b5-402d-8115-3f37cb1e2405" und denselben Parameternutzungsvorgaben der Registry Stored Query "FindDocuments" gemäß [IHE-ITI-TF2a#3.18.4.1.2.3.7.1] in Verbindung mit dem zusätzlich zu [ITI-18] eingeführten Suchparameter `$XDSDocumentEntryTitle` nutzen können.[<=]

Der zusätzliche Parameter "`$XDSDocumentEntryTitle`" filtert die Suchergebnismenge über das Attribut `XDSDocumentEntry.title`. Dabei ist die Angabe von Platzhaltern (wie für Suchanfragen über den Parameter `$XDSDocumentEntryAuthorPerson`) möglich, die sich verhält wie das SQL Schlüsselwort "LIKE" in Kombination mit den anzugeben Wildcard-Zeichen "%", um jedes Zeichen und "_", um ein bestimmtes Zeichen zu finden.

6.2.3.7 Vergebene Berechtigungen bestimmen

Mit dieser Operation werden die für das Aktenkonto vergebenen Berechtigungen ermittelt. Für jede Berechtigung ist in der Komponente Autorisierung ein `AuthorizationKey` und in der Komponente Dokumentenverwaltung ein technisches Dokument (Policy Document) hinterlegt. Diese beinhalten die Parameter der Berechtigung.

A_15323 - ePA-Frontend des Versicherten: Vergebene Berechtigungen bestimmen

Das ePA-Frontend des Versicherten MUSS die Aktivität "Vergebene Berechtigungen bestimmen" gemäß `TAB_FdV_115` umsetzen.

Tabelle 19: TAB_FdV_115 – Vergebene Berechtigungen bestimmen

Standardablauf	Aktivitäten im Standardablauf
	<ol style="list-style-type: none"> 1. Schlüsselmaterial aller Berechtigten laden 2. Policy Documents suchen 3. Policy Documents herunterladen 4. Berechtigungen aus Policy Documents extrahieren

[<=]

A_17129 - ePA-Frontend des Versicherten: Berechtigung bestimmen - Schlüsselmaterial aller Berechtigten laden

Das ePA-Frontend des Versicherten MUSS für die Aktivität "Vergebene Berechtigungen bestimmen" die übergreifende Aktivität "Schlüsselmaterial aller Berechtigten aus ePA-Aktensystem laden" ausführen.[<=]

Dokumente im Aktenkonto werden mittels ihrer XDS-Metadaten identifiziert. Die Nutzungsvorgaben für XDS-Metadaten zur Kennzeichnung von Policy Documents sind in [\[gemSpec_DM_ePA#A_14961 - Nutzungsvorgaben für die Verwendung von XDS-Metadaten bei Policy Documents\]](#) beschrieben.

A_15324 - ePA-Frontend des Versicherten: Berechtigung bestimmen - Policy Documents suchen

Das ePA-Frontend des Versicherten MUSS für die Aktivität "Vergebene Berechtigungen bestimmen" zur Suche der Policy Documents die übergreifende Aktivität "Suche nach Dokumenten in Dokumentenverwaltung" mit einer query:AdhocQueryRequest_Message für Policy Documents ausführen.

[<=]

Das Ergebnis der Suchanfrage query:AdhocQueryResponse_Message liefert, falls Berechtigungen erteilt wurden, die XDS-Metadaten von einem oder mehreren Policy Documents (je ein Policy Document pro LEI, KTR bzw. Vertreter). Die XDS-Metadaten beinhalten die Document Unique ID (uniqueId) der Policy Documents. Mittels dieser werden die Policy Documents aus der Dokumentenverwaltung heruntergeladen.

A_15325 - ePA-Frontend des Versicherten: Berechtigung auflisten - Policy Dokuments herunterladen

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Vergebene Berechtigungen anzeigen" zum Herunterladen der Policy Documents die übergreifende Aktivität "Dokumentenset aus Dokumentenverwaltung herunterladen" mit einer RetrieveDocumentSet_Message für alle über die XDS-Metadaten ermittelten Identifikatoren von Policy Documents ausführen.[<=]

Als Ergebnis liegen, falls Berechtigungen erteilt wurden, ein oder mehrere AuthorizationKeys sowie Policy Documents für berechtigte LEI, KTR und für Vertreter vor.

Gemäß der Beschreibung in "5.3.1- Policy Documents" können folgende Informationen zu den Berechtigungen aus den Policy Documents ermittelt werden.

Berechtigung für LEI: TelematikID, Name der LEI, Berechtigung "erteilt am", Berechtigung "gültig bis", Berechtigung für den Zugriff auf durch Versicherte eingestellte Dokumente, Berechtigung für den Zugriff auf durch KTR eingestellte Dokumente.

Gemäß der Beschreibung in "6.2.3.8.1- Struktur AuthorizationKeyType " können folgende Informationen zu den Berechtigungen aus den AuthorizationKeys ermittelt werden.

Berechtigung für Vertreter: Versicherten-ID, Name des Vertreters

Berechtigung für KTR: TelematikID, Name des KTR

Die Policy Documents lassen sich auf Basis der Versicherten-ID des Vertreters bzw. der TelematikID der LEI oder KTR den AuthorizationKeys zuordnen.

6.2.3.8 AuthorizationKey

Der AuthorizationKey enthält Parameter zur Berechtigung sowie die für den Berechtigten verschlüsselten Akten- und Kontextschlüssel.

6.2.3.8.1 Struktur AuthorizationKeyType

Die Struktur AuthorizationKeyType ist in [AuthorizationService.xsd] beschrieben.

Das Attribut `validTo` beinhaltet die Gültigkeit des AuthorizationKey, d.h. den Zeitpunkt bis zu dem die Berechtigung erteilt wird. Für eine Berechtigung ohne zeitliche Begrenzung wird ein technisches Datum gleichbedeutend mit unendlich (z.B. 31.12.9999) verwendet.

Das Attribut `actorID` beinhaltet die ID des Berechtigenden, d.h. die Versicherten-ID für Aktenkontoinhaber und Vertreter bzw. die TelematikID für LEIs und KTR.

Das Element `DisplayName` beinhaltet den Klartextnamen des Berechtigten.

Das Element `AuthorizationType` beinhaltet den Berechtigungstyp. Siehe auch [\[gemSpec_Autorisierung#6.3 Berechtigungstypen der Autorisierung\]](#).

Das Element `phrs:AuthorizationKey/phrs:EncryptedKeyContainer` enthält das Chiffre mit dem 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.

6.2.3.8.2 Schlüsselableitung für Ver- und Entschlüsselung

Die Klartextpräsentation von Akten- und Kontextschlüssel im `AuthorizationKey` ist doppelt symmetrisch verschlüsselt. Die symmetrischen Schlüssel zur Ver- und Entschlüsselung von Akten- und Kontextschlüssel werden über die Schlüsselableitungsfunktion der Schlüsselgenerierungsdienste Typ 1 und 2 ermittelt. Die Funktionsweise der Schlüsselgenerierung wird in [\[gemSpec_SGD_ePA\]](#) beschrieben.

A_17842 - ePA-Frontend des Versicherten: Symmetrische Schlüssel für Akten- und Kontextschlüssel ermitteln

Das ePA-Frontend des Versicherten MUSS zur Schlüsselableitung den in [\[gemSpec_SGD_ePA#2.3 Basisablauf Kommunikation SGD-Client und SGD\]](#) festgelegten Ablauf in der Rolle Client durchführen.[<=]

Im Schritt 7 des Basisablaufs erfolgt der Aufruf für `KeyDerivation` abhängig vom Anwendungsfall:

Anwendungsfall im FdV	Akteur	Zweck	Anwendungsfall für SGD
Aktenkonto aktivieren Anbieter wechseln	Versicherter	Verschlüsseln	[gemSpec_SGD_ePA#2.4 Initiale Schlüsselableitung für den Kontoinhaber]
Berechtigung für LEI vergeben Vertretung einrichten Berechtigung für Kostenträger vergeben Berechtigung für LEI ändern	Versicherter	Verschlüsseln	[gemSpec_SGD_ePA#2.6 Schlüsselableitung für einen Berechtigungsempfänger]
Berechtigung für LEI vergeben Berechtigung für Kostenträger vergeben Berechtigung für LEI ändern	Vertreter	Verschlüsseln	[gemSpec_SGD_ePA#2.8 Schlüsselableitung für einen Berechtigungsempfänger durch einen Vertreter]
Login	Versicherter Vertreter	Entschlüsseln	Für das Entschlüsseln müssen keine Anwendungsfälle für SGD unterschieden werden.

			<p>Es wird das Element <code>AssociatedData</code> des ermittelten <code>AuthorizationKey</code> für den Aufruf der Operation <code>KeyDerivation</code> beim SGD wie folgt verwenden:</p> <pre>KeyDerivation <Teilstring aus AssociatedData für den entsprechenden SGD></pre>
--	--	--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Als Ergebnis bei einer erfolgreichen Schlüsselableitung zum Verschlüsseln erhält das FdV 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.

Zur Optimierung der Performance muss das FdV 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 SGD 2 in Basisablauf Schritt 7 können ebenfalls parallelisiert werden. 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_17994 - ePA-Frontend des Versicherten: Aufrufe zur Schlüsselableitung parallelisieren

Das ePA-Frontend des Versicherten MUSS die Schlüsselableitung mit SGD 1 und SGD 2 sowie das Erzeugen des ephemeren ECDH-Schlüsselpaares parallelisieren. [≤]

6.2.3.8.3 AuthorizationKey erstellen

Für den Aktenkontoinhaber, Vertreter und KTR wird die Berechtigung ohne zeitliche Begrenzung vergeben. Für LEI ist das Enddatum entsprechend der vom Nutzer gewählten Berechtigungsdauer zu setzen.

Der `DisplayName` und die `TelematikID` einer LEI oder eines KTR werden aus dem Verzeichnisdienst der TI bestimmt (siehe "6.2.3.15- Suchanfrage Verzeichnisdienst der TI").

Es werden bei der Autorisierung verschiedene Berechtigungstypen unterschieden. Siehe [\[gemSpec_Autorisierung#6.3 Berechtigungstypen der Autorisierung\]](#). Für Aktenkontoinhaber, Vertreter, LEIs und KTR wird immer ein Berechtigung mit Zugriff auf die Dokumente vergeben.

A_15328 - ePA-Frontend des Versicherten: AuthorizationKey erstellen - Berechtigungstyp DOCUMENT_AUTHORIZATION

Das ePA-Frontend des Versicherten MUSS beim Erstellen eines `AuthorizationKey` den `AuthorizationType` = `DOCUMENT_AUTHORIZATION` setzen, wenn dem zu Berechtigenden Zugriff auf Dokumente in der Dokumentenverwaltung gewährt werden soll. [≤]

Akten- und Kontextschlüssel werden mit den in der Schlüsselableitung erhaltenen Schlüssel symmetrisch verschlüsselt. Es gelten die Vorgaben aus [\[gemSpec_SGD_ePA#8 Interoperables Austauschformat\]](#) sowie [\[gemSpec_Krypt#A_17872 - Ver- und Entschlüsselung der Akten und Kontextschlüssel \(Schlüsselableitungsfunktionalität ePA\)\]](#).

A_17995 - ePA-Frontend des Versicherten: AuthorizationKey erstellen - Akten- und Kontextschlüssel verschlüsseln

Das ePA-Frontend des Versicherten MUSS beim Erstellen eines AuthorizationKeys den Akten- und Kontextschlüssel mit den von der Schlüsselableitung mit SGD 1 und SGD 2 erhaltenen symmetrischen Schlüssel gemäß [gemSpec_SGD_ePA] und [gemSpec_Krypt] verschlüsseln.

Tabelle 20 : TAB_FdV_179 – Akten- und Kontextschlüssel verschlüsseln

Plattformbaustein PL_TUC_SYMM_ENCI PHER nutzen	Eingangsdaten: <ul style="list-style-type: none"> • Doc: Klartextpräsentation von Akten- und Kontextschlüssel (siehe gemSpec_SGD_ePA#Tab_Austauschformat Akten- und Kontextschlüssel) • Cert: aus SGD1 abgeleiteter symmetrischer Schlüssel • AD: AD_{SGD1} = Anteil 'a' aus KeyDerivation Response des SGD1 Rückgabedaten: <ul style="list-style-type: none"> • Doc_{enc} Mit Doc_{enc} und AD_{SGD1} wird eine Struktur gemäß [gemSpec_SGD_ePA#Tab_erste_Verschlüsselungsschicht] gebildet -> Doc_{enc1}
Plattformbaustein PL_TUC_SYMM_ENCI PHER nutzen	Eingangsdaten: <ul style="list-style-type: none"> • Doc: Doc_{enc1} • Cert: aus SGD2 abgeleiteter symmetrischer Schlüssel • AD: AD_{SGD2} = Anteil 'a' aus KeyDerivation Response des SGD2 Rückgabedaten: <ul style="list-style-type: none"> • Doc_{enc} Mit Doc_{enc} , AD_{SGD1} und AD_{SGD2} wird der EncryptedKeyContainer des AuthorizationKey gebildet.

[<=]

6.2.3.8.4 AuthorizationKey entschlüsseln

Der AuthorizationKey für einen Versicherten (Aktenkontoinhaber oder Vertreter) enthält ein verschlüsseltes Schlüsselpaar (Akten- und Kontextschlüssel).

Der Aktenschlüssel wird benötigt, um die Dokumente aus dem ePA-Aktensystem zu ver- und entschlüsseln. Der Kontextschlüssel wird benötigt, um den Verarbeitungskontext der Dokumentenverwaltung zu öffnen.

Das Chifftrat

`phrs:AuthorizationKey/phrs:EncryptedKeyContainer/phrs:CipherText` ist doppelt symmetrisch verschlüsselt. Die für die Entschlüsselung des Chiffrats benötigten zwei AES-256-Schlüssel ruft das FdV von den Schlüsselgenerierungsdiensten Typ 1 und Typ 2 gemäß [gemSpec_SGD_ePA] ab. Siehe "6.2.3.8.2. Schlüsselableitung für Ver- und Entschlüsselung".

Es gelten für das Entschlüsseln die Vorgaben aus [\[gemSpec_SGD_ePA#8 Interoperables Austauschformat\]](#) sowie [\[gemSpec_Krypt#A_17872 - Ver- und Entschlüsselung der Akten und Kontextschlüssel \(Schlüsselableitungsfunktionalität ePA\)\]](#).

A_17843 - ePA-Frontend des Versicherten: Akten- und Kontextschlüssel entschlüsseln

Das ePA-Frontend des Versicherten MUSS beim Entschlüsseln des Akten- und Kontextschlüssel die bei der Schlüsselableitung mit SGD 1 und SGD 2 erhaltenen symmetrischen Schlüssel gemäß [gemSpec_SGD_ePA] und [gemSpec_Krypt] nutzen.

Tabelle 21 : TAB_FdV_180 – Akten- und Kontextschlüssel entschlüsseln

Plattformbaustein PL_TUC_SYMM_DEC IPHER nutzen	<p>Eingangsdaten:</p> <ul style="list-style-type: none"> • <code>Doc_{enc}</code>: EncryptedKeyContainer\Ciphertext aus AuthorizationKey • Cert: aus SGD2 abgeleiteter symmetrischer Schlüssel • AD: SGD2 Anteil aus EncryptedKeyContainer\AssociatedData aus AuthorizationKey <p>Rückgabedaten:</p> <ul style="list-style-type: none"> • Doc: <code>Doc_{enc}1</code> = einfach symmetrisch verschlüsselter Akten- und Kontextschlüssel (siehe <code>gemSpec_SGD_ePA#Tab_erste_Verschlüsselungsschicht</code>)
Plattformbaustein PL_TUC_SYMM_DEC IPHER nutzen	<p>Eingangsdaten:</p> <ul style="list-style-type: none"> • <code>Doc_{enc}</code>: EncryptedKeyContainer\Ciphertext aus <code>Doc_{enc}1</code> • Cert: aus SGD1 abgeleiteter symmetrischer Schlüssel • AD: EncryptedKeyContainer\AssociatedData aus <code>Doc_{enc}1</code> <p>Rückgabedaten:</p> <ul style="list-style-type: none"> • Doc: Klartextpräsentation von Akten- und Kontextschlüssel (siehe <code>gemSpec_SGD_ePA#Tab_Austauschformat Akten- und Kontextschlüssel</code>)

[<=]

6.2.3.9 Schlüsselmaterial aus ePA-Aktensystem laden

Mit dieser Operation wird die Autorisierung eines Nutzers des FdV für ein Aktenkonto geprüft und die Schlüssel eines berechtigten Nutzers (bspw. Aktenkontoinhaber,

berechtigter Vertreter, LEI) für den Zugriff auf die Dokumentenverwaltung heruntergeladen.

A_15330 - ePA-Frontend des Versicherten: Schlüsselmaterial aus ePA-Aktensystem laden

Das ePA-Frontend des Versicherten MUSS die Aktivität "Schlüsselmaterial aus ePA-Aktensystem laden" gemäß TAB_FdV_116 umsetzen.

Tabelle 22: TAB_FdV_116 – Schlüsselmaterial aus ePA-Aktensystem laden

Vorbedingung	AuthenticationAssertion liegt in Session-Daten vor
<code>I_Authorization_Insurant::getAuthorizationKey</code> Request erstellen	Eingangsparameter: <ul style="list-style-type: none"> • AuthenticationAssertion aus Session-Daten • RecordIdentifizier aus Session-Daten • DeviceID aus Gerät-Daten
<code>I_Authorization_Insurant::getAuthorizationKey</code> Response verarbeiten	Rückgabedaten: <ul style="list-style-type: none"> • AuthorizationKey • AuthorizationAssertion <p>Beinhaltet der Response keinen AuthorizationKey und keine AuthorizationAssertion, wird die Aktivität abgebrochen.</p> <p>Beinhaltet der Response einen AuthorizationKey und eine AuthorizationAssertion wird versucht, das Element (verschlüsseltes Schlüsselpaar) aus EncryptedKeyBackup zu entschlüsseln.</p> <p>(siehe Kapitel "6.2.3.8.4-<u>AuthorizationKey entschlüsseln</u>") Liefert das Entschlüsseln einen Fehler, dann stehen die Informationen RecordKey und ContextKey nicht für die weitere Verarbeitung zur Verfügung. Die Aktivität wird nicht abgebrochen.</p>
Nachbedingung	Nach Abarbeitung der Aktivität stehen folgende Informationen bereit: <ul style="list-style-type: none"> • AuthorizationKey (optional) • AuthorizationAssertion (optional) • RecordKey (optional) • ContextKey (optional) • Status der Entschlüsselung AuthorizationKey (erfolgreich/nicht erfolgreich)

[<=]

Besitzt der Nutzer, für den das Schlüsselmaterial angefragt wird, keine Autorisierung für den Zugriff auf das Aktenkonto, dann beinhaltet die Response den Fehler KEY_ERROR.

Wird versucht das Schlüsselmaterial für den Aktenkontoinhaber herunterzuladen und beinhaltet der Response eine AuthorizationAssertion aber kein AuthorizationKey, dann ist das Aktenkonto des Versicherten noch nicht aktiviert. Das Aktivieren kann über die Anwendungsfälle "Aktenkonto aktivieren" oder "Anbieter wechseln" erfolgen.

6.2.3.10 Schlüsselmaterial aller Berechtigten aus ePA-Aktensystem laden

Mit dieser Operation wird das Schlüsselmaterial für alle Berechtigten des Aktenkontos heruntergeladen. Im Response werden keine AuthorizationAssertion übertragen.

A_17130 - ePA-Frontend des Versicherten: Schlüsselmaterial aller Berechtigten aus ePA-Aktensystem laden

Das ePA-Frontend des Versicherten MUSS die Aktivität "Schlüsselmaterial aller Berechtigten aus ePA-Aktensystem laden" gemäß TAB_FdV_163 umsetzen.

Tabelle 23: TAB_FdV_163 – Schlüsselmaterial aller Berechtigten aus ePA-Aktensystem laden

I_Authorization_Management_Insurant:: getAuthorizationList Request erstellen	Eingangsparameter: <ul style="list-style-type: none"> • AuthenticationAssertion aus Session-Daten • RecordIdentifier aus Session-Daten • DeviceID aus Geräte-Daten
I_Authorization_Management_Insurant:: getAuthorizationList Response verarbeiten	Rückgabedaten: <ul style="list-style-type: none"> • Liste von AuthorizationKeys

[<=]

6.2.3.11 Schlüsselmaterial im ePA-Aktensystem speichern

Mit dieser Operation wird Schlüsselmaterial (AuthorizationKey) für den Aktenkontoinhaber, einen Vertreter oder eine LEI in der Komponente Autorisierung des ePA-Aktensystems gespeichert. Beim Operationsaufruf für einen Vertreter wird eine Benachrichtigungsadresse (E-Mail) für die Geräteautorisierung hinterlegt (Parameter NotificationInfoRepresentative).

A_15331 - ePA-Frontend des Versicherten: Schlüsselmaterial im ePA-Aktensystem speichern

Das ePA-Frontend des Versicherten MUSS die Aktivität "Schlüsselmaterial im ePA-Aktensystem speichern" gemäß TAB_FdV_117 umsetzen.

Tabelle 24: TAB_FdV_117 – Schlüsselmaterial im ePA-Aktensystem speichern

I_Authorization_Management_Insurant:: putAuthorizationKey Request erstellen	Eingangsparameter: <ul style="list-style-type: none"> • AuthenticationAssertion aus
--------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------

	Session-Daten <ul style="list-style-type: none"> • RecordIdentifier aus Session-Daten • AuthorizationKey • DeviceID aus Geräte-Daten • optional: NotificationInfoRepresentative
I_Authorization_Management_Insurant::putAuthorizationKey Response verarbeiten	HTTP OK ohne SOAP-Response oder gematik Fehlermeldung Für Fehler KEY_ERROR siehe "A_15332 - ePA-Frontend des Versicherten: Schlüsselmateriale im ePA-Aktensystem speichern KEY_ERROR"

[<=]

Wenn die Operation den Fehler KEY_ERROR meldet, dann ist bereits ein Schlüssel in der Autorisierung hinterlegt. Dies kann bspw. bei einer Berechtigung der Fall sein, wenn die Berechtigung bereits zuvor erfolgreich erteilt wurde, oder wenn bei einem vorherigen Versuch die Berechtigung einzurichten ein Fehler auftrat, nachdem Schlüsselmateriale erfolgreich hinterlegt wurde (bspw. das zugehörige Policy Document nicht erfolgreich in der Dokumentenverwaltung hinterlegt werden konnte).

A_15332 - ePA-Frontend des Versicherten: Schlüsselmateriale im ePA-Aktensystem speichern KEY_ERROR

Das ePA-Frontend des Versicherten MUSS, wenn die Aktivität "Schlüsselmateriale im ePA-Aktensystem speichern" den Fehler KEY_ERROR liefert, einmalig den Anwendungsfall nicht abbrechen, das bereits hinterlegte Schlüsselmateriale mit der Aktivität "Schlüsselmateriale im ePA-Aktensystem löschen" löschen und die Aktivität "Schlüsselmateriale im ePA-Aktensystem speichern" wiederholen.[<=]

6.2.3.12 Schlüsselmateriale im ePA-Aktensystem ersetzen

Mit dieser Operation wird vorhandenes Schlüsselmateriale (AuthorizationKey) für den Aktenkontoinhaber, einen Vertreter oder eine LEI in der Komponente Autorisierung des ePA-Aktensystems ersetzt.

A_15333 - ePA-Frontend des Versicherten: Schlüsselmateriale im ePA-Aktensystem ersetzen

Das ePA-Frontend des Versicherten MUSS die Aktivität "Schlüsselmateriale im ePA-Aktensystem ersetzen" gemäß TAB_FdV_118 umsetzen.

Tabelle 25 : TAB_FdV_118 – Schlüsselmateriale im ePA-Aktensystem ersetzen

I_Authorization_Management_Insurant::replaceAuthorizationKey Request erstellen	Eingangsparameter: <ul style="list-style-type: none"> • AuthenticationAssertion aus Session-Daten • RecordIdentifier aus Session-Daten • NewAuthorizationKey
--------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<ul style="list-style-type: none"> • DeviceID aus Gerät-Daten
I_Authorization_Management_Insurant:: replaceAuthorizationKey Response verarbeiten	HTTP OK ohne SOAP-Response oder gematik Fehlermeldung

[<=]

6.2.3.13 Schlüsselmaterial im ePA-Aktensystem löschen

Mit dieser Operation wird vorhandenes Schlüsselmaterial (AuthorizationKey) für einen Vertreter oder eine LEI in der Komponente Autorisierung des ePA-Aktensystems gelöscht.

A_15334 - ePA-Frontend des Versicherten: Schlüsselmaterial im ePA-Aktensystem löschen

Das ePA-Frontend des Versicherten MUSS die Aktivität "Schlüsselmaterial im ePA-Aktensystem löschen" gemäß TAB_FdV_119 umsetzen.

Tabelle 26: TAB_FdV_119 – Schlüsselmaterial im ePA-Aktensystem löschen

I_Authorization_Management_Insurant:: deleteAuthorizationKey Request erstellen	Eingangsparameter: <ul style="list-style-type: none"> • AuthenticationAssertion aus Session-Daten • RecordIdentifier aus Session-Daten • ActorID • DeviceID aus Gerät-Daten
I_Authorization_Management_Insurant:: deleteAuthorizationKey Response verarbeiten	HTTP OK ohne SOAP-Response oder gematik Fehlermeldung

[<=]

6.2.3.14 Leistungserbringerinstitution im Verzeichnisdienst der TI finden

Informationen zu Leistungserbringern und Leistungserbringerinstitutionen sind im Verzeichnisdienst (VZD) der TI-Plattform hinterlegt. Das FdV kann (bspw. für die Vergabe von Berechtigungen an LEI) mit verschiedenen Kriterien nach LE und LEI im VZD suchen und Informationen abrufen. Das Informationsmodell des Verzeichnisdienstes ist in [gemSpec_VZD#5] beschrieben.

In der aktuellen Stufe der Fachanwendung ePA wird nur die Vergabe von Berechtigungen für LEI unterstützt.

Die Suche nach LE oder LEIs erfolgt primär über den Namen oder Institutionennamen aber auch über zusätzliche Informationen wie Adressen, Fachgebiet oder Institutionstyp.

A_15335 - ePA-Frontend des Versicherten: Search Operation mittels LDAP-Directory Basisdatensatz Attribut

Das ePA-Frontend des Versicherten MUSS Leistungserbringerinstitutionen über Suchkriterien

- Namen,
- Postadresse,
- Institution,
- und Fachgebiet

in einer LDAP search Operation nach einem entsprechenden Basisdatensatz Attribut des LDAP-Directory gemäß TAB_FdV_120 suchen können.

Tabelle 27: TAB_FdV_120 – Suchkriterien LDAP Search

Suchkriterium	Beschreibung für die Suche nach Heilberuflern	Beschreibung der Suche nach Leistungserbringerinstitutionen	LDAP-Directory Basisdatensatz Attribut
Vollständiger Name	Der commonName enthält den vollständigen Namen des Inhabers, ohne akademischen Titel	Name der Institution (erste zwei Zeilen des Anschriftenfeldes)	cn
Vorname	Vorname Heilberufler		givenName
Nachname/Institutionsname	Nachname Heilberufler		sn
Anzeigename	Nachname, Vorname des Heilberuflers	Name der Organisation/Einrichtung des Gesundheitswesens	displayName
Titel	Der Titel des LE (z.B. Dr. med)		title
Institutionsname	Die Bezeichnung der Organisation des Gesundheitswesens (z.B. Arztpraxis Dr. Mustermann)	Name der Organisation/Einrichtung des Gesundheitswesens	organization
Strasse, Hausnummer	Straße, Hausnummer	Straße, Hausnummer	streetAddress
Postleitzahl	Postleitzahl	Postleitzahl	postalCode
Ort	Ort	Ort	localityName

Bundesland	Bundesland	Bundesland	stateOrProvinceName
Langname	Für die Verwendung von überlangen Namen von Heilberuflern	Für die Verwendung von überlangen Namen von Institutionen, z.B. Praxisgemeinschaften unter Aufzählung aller beteiligten Ärzte	otherName
Institution/Berufsgruppe	Berufsgruppe	Institution	professionOID
Fachgebiet	medizinisches Fachgebiet	Fachabteilung	specialization
TelematikID	Eindeutige ID des Heilberuflers in der TI	Eindeutige ID der Institution in der TI	telematikID

[<=]

Da nur Leistungserbringerinstitutionen und keine einzelnen Leistungserbringer für den Zugriff auf ein Aktenkonto berechtigt werden können, müssen die durch den Nutzer eingegebenen Suchparameter ggf. für die VZD-Abfrage so ergänzt werden, dass nur Informationen zu Leistungserbringerinstitutionen abgefragt werden. Dies kann anhand des Parameters professionOID erfolgen, welcher auf die Werte gemäß [gemSpec_VZD#Tab_VZD_Mapping_Eintragstyp Eingangstyp 3] beschränkt sein muss.

Die VZD-Abfrage wird gemäß der übergreifenden Aktivität "Suchanfrage Verzeichnisdienst der TI" durchgeführt.

A_17435 - ePA-Frontend des Versicherten: LEI in Verzeichnisdienst der TI finden

Das ePA-Frontend des Versicherten MUSS die Leistungserbringer mittels der Aktivität "Suchanfrage Verzeichnisdienst der TI" ermitteln, wobei mindestens als Suchkriterium (professionOID aus {[gemSpec_VZD#Tab_VZD_Mapping_Eintragstyp Eingangstyp 3]}) zu verwenden ist.

[<=]

6.2.3.15 Suchanfrage Verzeichnisdienst der TI

Der VZD der TI ist für Suchoperationen des FdV über das Zugangsgateway des Versicherten erreichbar, welches als LDAP-Proxy agiert. Das FdV nutzt zur Abfrage des VZD den Standard Directory Services Markup Language v2.0 [DSML2.0].

A_15336 - ePA-Frontend des Versicherten: Suchanfrage Verzeichnisdienst der TI

Das ePA-Frontend des Versicherten MUSS die Aktivität "Suchanfrage Verzeichnisdienst der TI" gemäß TAB_FdV_121 umsetzen.

Tabelle 28: TAB_FdV_121 – Abfrage Verzeichnisdienst

dsmlEnvelopeRequest mit searchRequest erstellen	
-------------------------------------------------	--

I_Proxy_Directory_Query::Search Request erstellen	Eingabedaten: <ul style="list-style-type: none"> searchRequest: Suchanfrage formuliert in DSML
I_Proxy_Directory_Query::Search Response verarbeiten	Rückgabedaten: <ul style="list-style-type: none"> searchResponse gemäß DSML mit Liste von searchResultEntry

[<=]

Für ein Beispiel für eine Suchanfrage und ein Ergebnis siehe [\[gemSpec Zugangsgateway Vers#6.2.2.3 Nutzung\]](#).

Die Anzahl der Einträge im Ergebnis der Suchabfrage ist auf maximal 10 beschränkt. Wenn die Suchkriterien zu mehr als 10 Einträgen im VZD passen, dann wird im Response zusätzlich der LDAP Fehler adminLimitExceeded übermittelt.

A_15337 - ePA-Frontend des Versicherten: Hinweis zusätzliche Ergebniseinträge im Verzeichnisdienst

Das ePA-Frontend des Versicherten MUSS, wenn im I_Proxy_Directory_Query::Search Response der Fehler adminLimitExceeded übermittelt wurde, den Nutzer informieren, dass entsprechend den Suchkriterien zusätzliche Einträge im Verzeichnisdienst vorliegen.[<=]

Durch eine Verfeinerung der Suchkriterien kann die Ergebnismenge so verkleinert werden, dass alle Einträge übermittelt werden.

Die Anzahl der möglichen Anfragen an den Verzeichnisdienst ist begrenzt (default: 10 Anfragen pro Minute). Wird die Anzahl überschritten, beinhaltet der HTTP-Response des Zugangsgateway des Versicherten den HTTP-Statuscode 429 entsprechend RFC6585 Kapitel 4 "429 Too Many Requests". Der Response mit dem HTTP-Statuscode 429 stellt keinen Fehler dar. Der Anwendungsfall wird nicht abgebrochen. Das FdV muss den Nutzer informieren, dass der nächste Request erst nach einer Verzögerung möglich ist.

Die im dsmlEnvelopeResponse gelieferten Informationen beinhalten die Informationen zur TelematikID und Name der Institution, welche für die Vergabe von Berechtigungen weiterverarbeitet werden.

6.2.3.16 PIN-Eingabe für eGK durch Nutzer

Mit dieser Operation wird der Nutzer zur fachlich motivierten PIN-Eingabe für seine eGK aufgefordert.

Zusätzlich kann bei Nutzung einer eGK eine PIN-Eingabe für die Berechtigung zum Zugriff auf Daten auf der eGK notwendig sein. In dem Fall wird die Aufforderung zur PIN-Eingabe durch den CardProxy ausgelöst.

A_15338 - ePA-Frontend des Versicherten: PIN-Eingabe für eGK durch Nutzer

Das ePA-Frontend des Versicherten MUSS die Aktivität "PIN-Eingabe durch Nutzer" gemäß TAB_FdV_122 umsetzen.

Tabelle 29: TAB_FdV_122 – PIN-Eingabe durch Nutzer

Plattformbaustein PL_TUC_CARD_VERIFY_PIN	Durch den Plattformbaustein PL_TUC_CARD_INFORMATION wird eine Nutzerverifikation durchgeführt.
Eingangsdaten	<ul style="list-style-type: none"> • Identifikator = MRPIN.home • Nutzerhinweis für PIN-Eingabe default: "EingabePIN:"
Beschreibung	Der Nutzerhinweis wird bei Aufruf der Umgebungsoperation ENV_TUC_SECRET_INPUT im Nutzerinterface (GUI) bzw. bei Nutzung eines Kartenterminal Sicherheitsklasse 3 im Display des Kartenterminals angezeigt.
Rückgabedaten	<ul style="list-style-type: none"> • OK - PIN erfolgreich verifiziert Es wird mit der folgenden Aktivität fortgefahren
Varianten/Alternativen	<ul style="list-style-type: none"> • WrongSecretWarning.X - PIN falsch, noch X Versuche Die verbleibende Anzahl der Eingabeversuche bis zur Sperrung der PIN wird dem Nutzer zurückgemeldet. Der Nutzer hat die Wahl die PIN erneut einzugeben oder den Anwendungsfall zu beenden. • PasswordBlocked - PIN ist durch Fehleingaben blockiert Dem Nutzer wird der Anwendungsfall "PIN der eGK entsperren" angeboten.

[<=]

A_15339 - ePA-Frontend des Versicherten: Abbruch Anwendungsfall nach fehlgeschlagener Nutzerverifikation

Das ePA-Frontend des Versicherten MUSS, wenn die Nutzerverifikation in der Operation "PIN-Eingabe durch Nutzer" fehlschlägt, den Anwendungsfall abbrechen, in dem die Operation aufgerufen wurde.[<=]

6.2.4 Nutzerzugang ePA

6.2.4.1 Login Aktensession

Mit diesem Anwendungsfall wird die Aktensession eines Nutzers im FdV gestartet. Der Sessionstart erfolgt implizit, falls die Verbindung zum ePA-Aktensystem bei Ausführung eines fachlichen Anwendungsfalles der ePA erforderlich ist und nicht besteht oder explizit beim Start des FdV durch den Nutzer.

Für die Anmeldung des Nutzers mit seiner eGK wird eine 2-Faktor-Authentisierung (eGK + PIN) verwendet. Als weitere Möglichkeit kann die alternative Versichertenidentität genutzt werden. Nach erfolgreicher Authentisierung inklusive Gültigkeitsprüfung der eGK und Autorisierung wird je nach bestehender Berechtigung des Nutzers das empfängerverschlüsselte Schlüsselmaterial heruntergeladen und das Öffnen des

Aktenkontextes in der Komponente "Dokumentenverwaltung" für das referenzierte Aktenkonto durchgeführt.

A_13695 - ePA-Frontend des Versicherten: Login Aktensession

Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "UC 1.1 - Login durch einen Versicherten" aus [gemSysL_ePA] gemäß TAB_FdV_123 umsetzen.

Tabelle 30: TAB_FdV_123 – Login Aktensession

Name	Login Aktensession
Auslöser	<ul style="list-style-type: none"> • Der Akteur möchte einen fachlichen Anwendungsfall mit Datenzugriff auf das ePA-Aktensystem ausführen. • optional: Start des FdV
Akteur	Versicherter oder berechtigter Vertreter
Vorbedingung	RecordIdentifier des Versicherten oder des zu Vertretenden ist im FdV bekannt und ausgewählt. Die eGK des Nutzers steckt im Kartenleser.
Nachbedingung	Für die Aktensession liegen gültige Session-Daten im FdV vor.
Standardablauf	<p>Aktivitäten im Standardablauf</p> <ol style="list-style-type: none"> 1. Session-Daten für RecordIdentifier prüfen 2. optional: wenn Authentisieren mittels eGK <ol style="list-style-type: none"> a. Einlesen der Karte 3. Authentisieren des Nutzers 4. Autorisieren des Nutzers 5. Status des Aktenkontos prüfen 6. Aktenkontext öffnen 7. optional: Benachrichtigungen anzeigen
Varianten/Alternativen	<p>Wenn nach der Aktivität "Autorisieren des Nutzers" ein Autorisierungstoken mit <code>RecordState = REGISTERED</code> vorliegt, dann wird der Anwendungsfall "Login Aktensession" ohne Fehler abgebrochen und der Anwendungsfall "Aktenkonto aktivieren" gestartet.</p> <p>Wenn nach der Aktivität "Autorisieren des Nutzers" ein Autorisierungstoken mit <code>RecordState = REGISTERED_FOR_MIGRATION</code> vorliegt, dann wird der Anwendungsfall "Login Aktensession" abgebrochen, der Nutzer darauf hingewiesen, dass zuerst eine Datenmigration vom Aktenkonto des alten Anbieters durchzuführen ist und der Anwendungsfall "Logout Aktensession" gestartet.</p> <p>In allen – nicht behebbaren – Fehlerfällen wird der Anwendungsfall abgebrochen und der Anwendungsfall "Logout" gestartet.</p>

[<=]

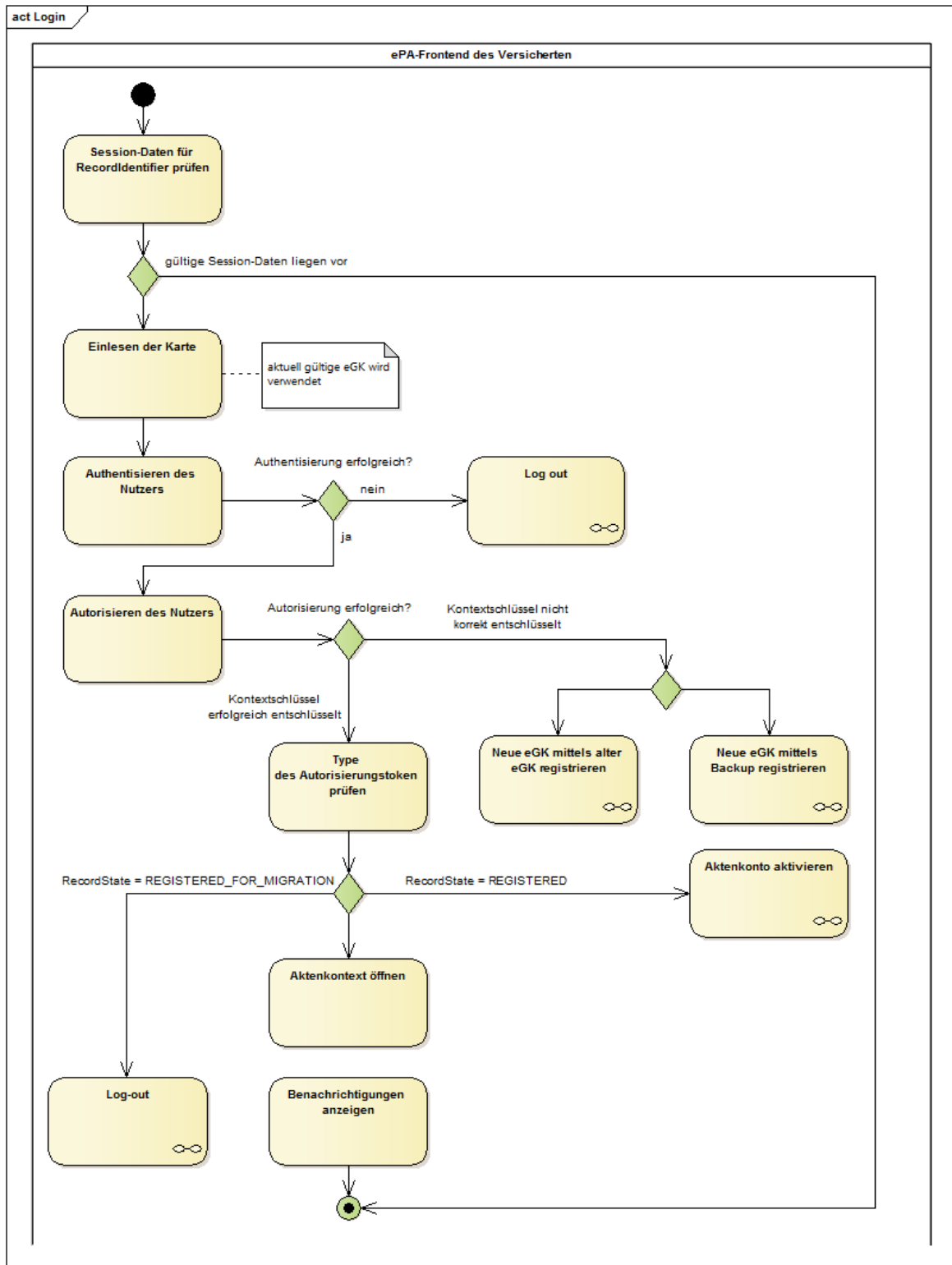


Abbildung 2: Aktivitätsdiagramm "Login Aktensession"

A_15340 - ePA-Frontend des Versicherten: Login - Session-Daten für RecordIdentifier prüfen

Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "Login Aktensession" ohne Fehler abbrechen, wenn gültige Session-Daten zu dem RecordIdentifier vorliegen. [≤]

Gültige Session-Daten liegen vor, wenn die Session-Daten einen Authentisierungstoken und einen Autorisierungstoken beinhalten. Auf eine Prüfung der zeitlichen Gültigkeit der Token wird verzichtet, da eine Synchronität der Systemzeit in der Ablaufumgebung des FdV mit der den Token ausstellenden Komponente nicht sichergestellt werden kann. Antwortet das ePA-Aktensystem auf einen Operationsaufruf mit dem Fehler, dass ein Token ungültig ist, dann löscht das FdV die Token aus den Session-Daten (siehe "A_15310 - ePA-Frontend des Versicherten: Fehlerbehandlung ungültiger Token").

A_15341 - ePA-Frontend des Versicherten: Login - Einlesen der Karte

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Login Aktensession", wenn die Authentisierung mittels eGK erfolgt, die Aktivität "Einlesen der Karte" gemäß TAB_FdV_124umsetzen.

Tabelle 31: TAB_FdV_124 – Login - Einlesen der Karte

Plattformbaustein PL_TUC_CARD_INFORMATION	Durch den Plattformbaustein PL_TUC_CARD_INFORMATION werden Statusinformationen der Karte bereitgestellt.
Eingangsdaten	eGK
Beschreibung	<p>Das FdV MUSS die Karteninformationen in PL_TUC_CARD_INFORMATION auswerten hinsichtlich</p> <ul style="list-style-type: none"> • Kartentyp = Typ eGK • Produkttypversion des Objektsystems = G2 oder höher <p>und bei unpassenden Kartendaten den Anwendungsfall mit einem Fehler beenden.</p> <p>Die folgenden Informationen der Karte werden in die Session-Daten übernommen:</p> <ul style="list-style-type: none"> • C.CH.AUT * • Versicherten-ID

* für eGK G2 das RSA-Zertifikat (R2048) und für eGK einer höheren Generation (bspw. G2.1) das ECC-Zertifikat (E256)
[≤]

A_15342 - ePA-Frontend des Versicherten: Login - Abbruch bei Karte lesen

Das ePA-Frontend des Versicherten MUSS, wenn der Anwendungsfall "Login Aktensession" aufgrund der Prüfungen beim Einlesen der Karte abbricht, den Nutzer darauf hinweisen, seine aktuell gültige eGK zu stecken. [≤]

Authentisieren und Autorisieren

A_15343 - ePA-Frontend des Versicherten: Login - Authentisieren des Nutzers

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Login Aktensession" die übergreifende Aktivität "Authentisieren des Nutzers" ausführen. [≤]

Während der Entschlüsselung des Akten- und Kontextschlüssels werden Zertifikate der TI geprüft. Zuvor ist die Aktualität des Vertrauensraumes der TI sicher zu stellen. Siehe "6.1.5- Zertifikatsprüfung".

A_15344 - ePA-Frontend des Versicherten: Login - Autorisieren des Nutzers - Schlüsselmaterial aus ePA-Aktensystem laden

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Login Aktensession" zum Autorisieren des Nutzers die übergreifende Aktivität "Schlüsselmaterial aus ePA-Aktensystem laden" ausführen. Wenn die Aktivität die Informationen AuthenticationAssertion, AuthorizationAssertion, RecordKey (Aktenschlüssel) oder ContextKey (Kontextschlüssel) liefert, dann werden diese in die Session-Daten übernommen.

[<=]

Aktivieren und Migration

Wenn die Autorisierung eine AuthorizationAssertion aber kein AuthorizationKey liefert, dann ist das Aktenkonto des Versicherten noch nicht aktiviert. Das Aktivieren kann über die Anwendungsfälle "Aktenkonto aktivieren" oder "Anbieter wechseln" erfolgen.

Der Status des Aktenkontos (RecordState) lässt sich aus dem Autorisierungstoken Attribut Assertion/AttributeStatement/Attribute mit dem Namen "Zustand des Kontos" ermitteln. Die Information wird in die Session-Daten übernommen.

A_15346 - ePA-Frontend des Versicherten: Login - Autorisieren des Nutzers - Aktenkontostatus REGISTERED

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Login Aktensession" den Aktenzustand aus dem Autorisierungstoken ermitteln und bei RecordState = REGISTERED den Anwendungsfall ohne Fehler abbrechen und den Anwendungsfall "Aktenkonto aktivieren" starten.

[<=]

A_15681 - ePA-Frontend des Versicherten: Login - Autorisieren des Nutzers - Aktenkontostatus REGISTERED_FOR_MIGRATION

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Login Aktensession" den Aktenzustand aus dem Autorisierungstoken prüfen und bei RecordState = REGISTERED_FOR_MIGRATION den Anwendungsfall mit Fehler abbrechen und dem Nutzer den Hinweis geben, dass vor der Nutzung des Aktenkontos beim neuen Anbieter eine Migration der Daten aus dem Aktenkonto des alten Anbieters durchgeführt werden muss.

[<=]

Verbindung zur Dokumentenverwaltung

Für die Aktivität "Aktenkonto öffnen" wird zuerst ein sicherer Kanal auf Inhaltsebene zwischen dem FdV und der VAU der Dokumentenverwaltung aufgebaut. Dafür wird die Schnittstelle I_Document_Management_Connect der Komponente Dokumentenverwaltung genutzt (siehe auch [\[gemSpec_Dokumentenverwaltung#Schnittstelle I_Document_Management_Connect\]](#)).

A_15347 - ePA-Frontend des Versicherten: Login - Aktenkontext öffnen - Aufbau sicherer Kanal zu Dokumentenverwaltung

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Login Aktensession" in der Aktivität "Aktenkontext öffnen" für die Schnittstellen zur Komponente Dokumentenverwaltung das Kommunikationsprotokoll gemäß den Vorgaben aus [\[gemSpec_Krypt#ePA-spezifische Vorgaben\]](#)

und [gemSpec_Krypt#Kommunikationsprotokoll zwischen VAU und ePA-Clients] umsetzen. ePA-Frontend des Versicherten: Login - Aktenkontext öffnen - Erweiterung des sicheren Verbindungsprotokolls

Das ePA-Frontend des Versicherten MUSS beim Aufbau des sicheren Kanals zur Dokumentenverwaltung die AuthorizationAssertion aus den Session-Daten der vom FdV aufgerufenen Operation als Parameter

gemäß [gemSpec_Dokumentenverwaltung#A_15592] übergeben.[<=]

Das FdV nutzt den abgeleiteten Sitzungsschlüssel, um alle fachlichen Eingangs- und Ausgangsnachrichten zur Dokumentenverwaltung zu ver- bzw. entschlüsseln. Siehe "A_15304 - ePA-Frontend des Versicherten: Umsetzung sicherer Kanal zur Dokumentenverwaltung".

A_15348 - ePA-Frontend des Versicherten: Login - Aktenkontext öffnen - Operation OpenContext

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Login Aktensession" in der Aktivität "Aktenkontext öffnen" das Übersenden des Kontextschlüssels gemäß TAB_FdV_126 umsetzen.

Tabelle 32: TAB_FdV_126 – Login - Aktenkontext öffnen - Operation OpenContext

Vorbedingung	AuthorizationAssertion und entschlüsselter Kontextschlüssel liegen in Session-Daten vor.
I_Document_Management_Connect::OpenContext Request erstellen	Eingangsdaten: <ul style="list-style-type: none"> Kontextschlüssel (ContextKey) aus Session-Daten
I_Document_Management_Connect::OpenContext Response verarbeiten	Rückgabedaten: <ul style="list-style-type: none"> OK oder gematik Fehler

[<=]

Benachrichtigungen

Die Anzeige von Benachrichtigungen im Anwendungsfall "Login Aktensession" ist optional gemäß den Konfigurationsdaten. Wird das Login nicht explizit mit dem Start des FdV ausgeführt, sondern erst bei Ausführung eines Anwendungsfalls mit Zugriff auf das ePA-Aktensystem, dann muss der Nutzer zuerst bestätigen, ob die Benachrichtigungen innerhalb des aufgerufenen Anwendungsfalls angezeigt werden sollen.

A_15350 - ePA-Frontend des Versicherten: Login - Benachrichtigungen anzeigen optional

Das ePA-Frontend des Versicherten MUSS, wenn die Konfiguration Benachrichtigungen aktivieren = nein gesetzt ist die Aktivitäten zum Anzeigen von Benachrichtigungen ignorieren.[<=]

A_15351 - ePA-Frontend des Versicherten: Login - Benachrichtigungen anzeigen unterdrücken

Das ePA-Frontend des Versicherten MUSS, wenn die Konfiguration Benachrichtigungen aktivieren = ja gesetzt ist und der Anwendungsfall "Login Aktensession" nicht zum Start des FdV durchgeführt wird, sondern implizit durch einen anderen Anwendungsfall getriggert wird, beim Nutzer abfragen, ob die Benachrichtigungen angezeigt werden sollen.[<=]

A_15352 - ePA-Frontend des Versicherten: Login - Protokolldaten Dokumentenverwaltung abfragen

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Login Aktensession", wenn die Konfiguration Benachrichtigungen aktivieren = ja gesetzt ist, die Protokolldaten der Komponente Dokumentenverwaltung gemäß "A_15486 - ePA-Frontend des Versicherten: Protokoll einsehen - Dokumentenverwaltung abfragen" abfragen und das Ergebnis gemäß der Konfiguration Benachrichtigungszeitraum filtern und anzeigen.[<=]

A_15353 - ePA-Frontend des Versicherten: Login - Benachrichtigungen-Anzeige

Das ePA-Frontend des Versicherten MUSS eine Anzeige für Benachrichtigungen umsetzen, in der die Protokolleinträge für folgende Zugriffe übersichtlich dargestellt werden:

- Folgende Anwendungsfälle aus dem § 291a-konformen Zugriffsprotokoll der Dokumentenverwaltung
 - Dokumente einstellen aus der ärztlichen Umgebung
 - Dokumente löschen aus der ärztlichen Umgebung
 - Dokumente einstellen aus der privaten Umgebung
 - Dokumente löschen aus der privaten Umgebung

[<=]

Es gelten folgende Anforderungen aus dem Anwendungsfall "Protokolldaten einsehen" für die Darstellung der Benachrichtigung: "A_15493 - ePA-Frontend des Versicherten: Ergebnisliste Protokolldaten", "A_15494 - ePA-Frontend des Versicherten: Ergebnisliste Protokolldaten drucken" und "A_15495 - ePA-Frontend des Versicherten: Protokolldaten lokal speichern".

A_15354 - ePA-Frontend des Versicherten: Konfiguration letzte Anmeldung

Das ePA-Frontend des Versicherten MUSS nach erfolgreichem Login den Wert "Letzte Anmeldung zum Aktenkonto" für das Aktenkonto in den Konfigurationsdaten aktualisieren.[<=]

6.2.4.2 Logout Aktensession

Dieser Anwendungsfall beendet eine Aktensession.

A_15355 - ePA-Frontend des Versicherten: Logout Aktensession

Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "UC 1.3 - Logout durch einen Nutzer" aus [gemSysL_ePA] gemäß TAB_FdV_127 umsetzen.

Tabelle 33: TAB_FdV_127 – Logout Aktensession

Name	Logout Aktensession
Auslöser	<ul style="list-style-type: none"> • Aufruf des Anwendungsfalls in der GUI • Der Akteur war innerhalb seiner Aktensession über einen maximalen Zeitraum hinaus inaktiv. • Fehler im Anwendungsfall "Login Aktensession"
Akteur	Versicherter, berechtigter Vertreter
Vorbedingung	Es besteht eine Aktensession mit gültigen Session-Daten.
Nachbedingung	Die Session-Daten sind gelöscht.

Standardablauf	Aktivitäten im Standardablauf <ol style="list-style-type: none"> 1. Aktenkontext schließen 2. Authentisierungstoken abmelden 3. optional: wenn eine alternative Versichertenidentität für die Authentisierung genutzt wurde <ol style="list-style-type: none"> a. Freischaltung des Signaturdienstes beenden 4. Session-Daten löschen
----------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

[<=]

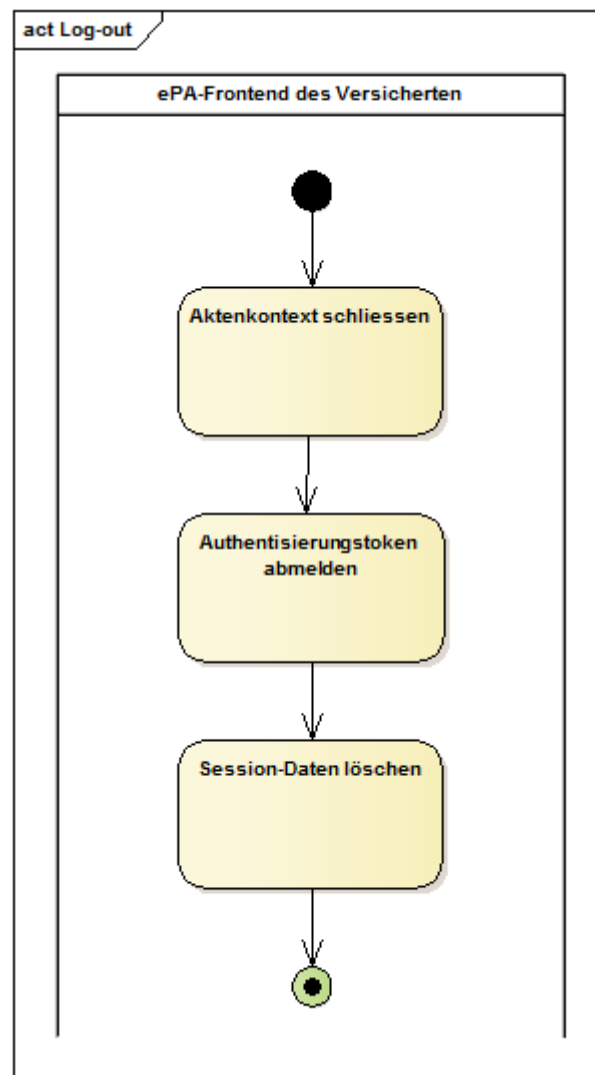


Abbildung 3: Aktivitätsdiagramm "Logout Aktensession"

A_15356 - ePA-Frontend des Versicherten: Logout - Aktenkontext schließen

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Logout Aktensession", wenn ein sicherer Kanal zur Dokumentenverwaltung aufgebaut und der Aktenkontext erfolgreich geöffnet wurde, die Aktivität "Aktenkontext schließen" gemäß TAB_FdV_128 umsetzen.

Tabelle 34: TAB_FdV_128 – Logout - Aktenkontext schließen

Vorbedingung	AuthorizationAssertion in Session-Daten
I_Document_Management_Connect::CloseContext Request erstellen	
I_Document_Management_Connect::CloseContext Response verarbeiten	HTTP OK oder gematik-Fehlermeldung

[<=]

A_17542 - ePA-Frontend des Versicherten: Logout - Authentisierungstoken abmelden

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Logout Aktensession", wenn ein Authentisierungstoken in den Session-Daten gespeichert ist, die Aktivität "Authentisierungstoken abmelden" gemäß TAB_FdV_172 umsetzen.

Tabelle 35: TAB_FdV_172 – Logout - Authentisierungstoken abmelden

Vorbedingung	AuthenticationAssertion in Session-Daten
I_Authentication_Insurant::LogoutToken Request erstellen	Eingangsdaten: <ul style="list-style-type: none"> CancelTarget: AuthenticationAssertion aus Session-Daten
I_Authentication_Insurant::LogoutToken Response verarbeiten	Keine Verarbeitung notwendig

[<=]

A_17766 - ePA-Frontend des Versicherten: Logout - Freischaltung des Signaturdienstes beenden

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Logout Aktensession", wenn für die Authentisierung eine alternative Versichertenidentität genutzt wurde und die Schnittstelle I_Remote_Sign_Operations::sign_Data freigeschaltet wurde, den Signaturdienst aufrufen, um eine Freischaltung des Signaturdienstes für den Nutzer zu beenden.

[<=]

Eine Beschreibung der signaturdienstspezifischen Schnittstelle für diese Operation ist in [vesta].

A_15358 - ePA-Frontend des Versicherten: Logout - Session-Daten löschen

Das ePA-Frontend des Versicherten MUSS zum Abschluss des Anwendungsfall "Logout Aktensession" alle Session-Daten aus dem lokalen Speicher löschen.[<=]

Die Session-Daten sind in "7.- Informationsmodell" beschrieben.

6.2.5 Aktenkontoverwaltung

6.2.5.1 Aktenkonto aktivieren

Der Anwendungsfall "Aktenkonto aktivieren" wird automatisch gestartet, wenn sich beim Login nach der Autorisierung ergibt, dass das Aktenkonto den Status "beantragt" hat.

Der Anwendungsfall kann in der GUI auswählbar sein. Dann ist vorab der Anwendungsfall "Login Aktensession" auszuführen.

A_15359 - ePA-Frontend des Versicherten: Aktenkonto aktivieren über GUI

Das ePA-Frontend des Versicherten MUSS, wenn der Versicherte den Anwendungsfall "Aktenkonto aktivieren" über die GUI auswählt, den Anwendungsfall "Login Aktensession" starten.[<=]

Im Rahmen des Login wird eine Authentisierung und Autorisierung des Nutzers durchgeführt.

A_15360 - ePA-Frontend des Versicherten: Aktenkonto aktivieren

Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "UC 2.1 - Aktenkonto einrichten" aus [gemSysL_ePA] gemäß TAB_FdV_130 umsetzen.

Tabelle 36: TAB_FdV_130 – Aktenkonto aktivieren

Name	Aktenkonto aktivieren
Auslöser	<ul style="list-style-type: none"> über Anwendungsfall "Login Aktensession"
Akteur	Versicherter
Vorbedingung	In den Session-Daten liegt ein Authentisierungstoken und ein Autorisierungstoken mit <code>RecordState = REGISTERED</code> vor.
Nachbedingung	Das Aktenkonto ist aktiviert. Es können fachliche Anwendungsfälle mit dem Aktenkonto durchgeführt werden.
Standardablauf	Aktivitäten im Standardablauf <ol style="list-style-type: none"> 1. Aktenschlüssel erzeugen 2. Kontextschlüssel erzeugen 3. AuthorizationKey erzeugen 4. Schlüsselmaterial in ePA-Aktensystem laden 5. Schlüsselmaterial aus ePA-Aktensystem laden 6. Aktenkontext öffnen

[<=]

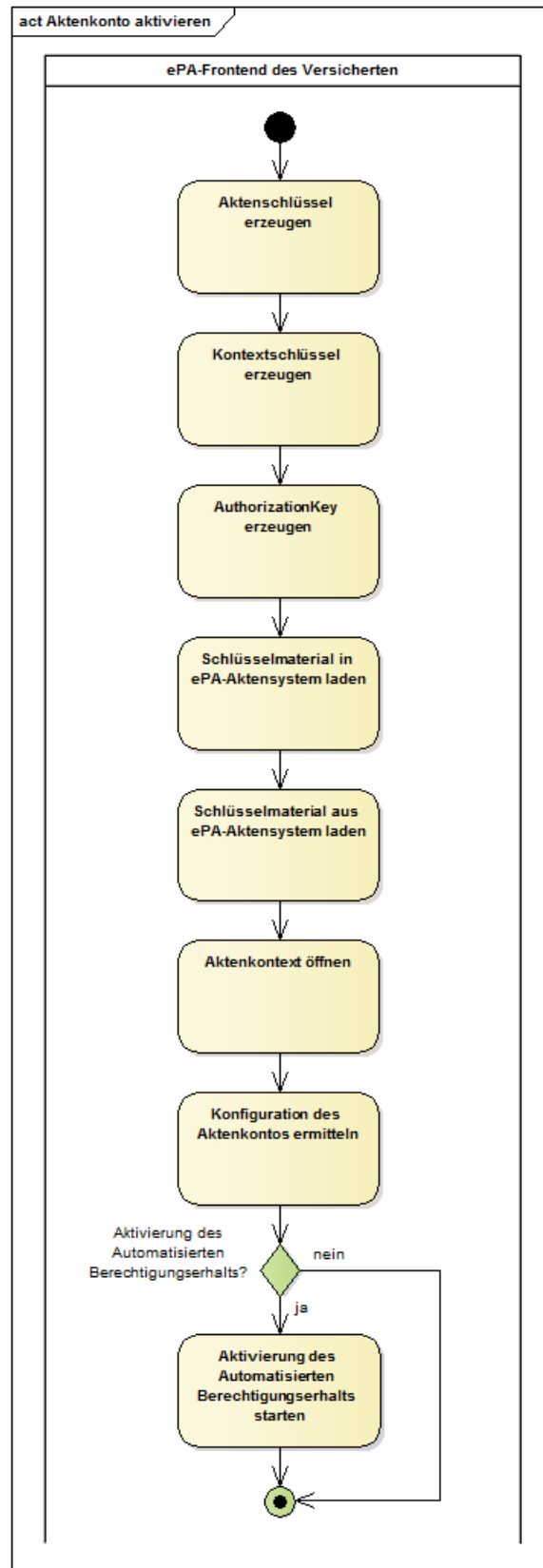


Abbildung 4: Aktivitätsdiagramm "Aktenkonto aktivieren"

A_15362 - ePA-Frontend des Versicherten: Aktenkonto aktivieren - Aktenschlüssel erzeugen

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Aktenkonto aktivieren" den Aktenschlüssel erzeugen.[<=]

A_15363 - ePA-Frontend des Versicherten: Aktenkonto aktivieren - Kontextschlüssel erzeugen

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Aktenkonto aktivieren" den Kontextschlüssel erzeugen.[<=]

Für das Erzeugen von Schlüsseln ist [\[gemSpec Krypt#GS-A 4368 - Schlüsselerzeugung\]](#) und [\[gemSpec Krypt#A 15705 - Vorgaben Aktenschlüssel \(RecordKey\) und Kontextschlüssel \(ContextKey\)\]](#) zu beachten.

A_15364 - ePA-Frontend des Versicherten: Aktenkonto aktivieren - AuthorizationKey erstellen

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Aktenkonto aktivieren" einen AuthorizationKey mit

- den erzeugten Aktenschlüssel und Kontextschlüssel,
- dem Namen und der Versicherten-ID aus dem Authentisierungszertifikat
- sowie `AuthorizationType = DOCUMENT_AUTHORIZATION`

für den Versicherten erstellen.[<=]

A_15365 - ePA-Frontend des Versicherten: Aktenkonto aktivieren - Schlüsselmaterial im ePA-Aktensystem speichern

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Aktenkonto aktivieren" für das Hochladen des Schlüsselmaterials in das ePA-Aktensystem die übergreifende Aktivität "Schlüsselmaterial im ePA-Aktensystem speichern" mit dem Eingangsparameter `AuthorizationKey = erstellter AuthorizationKey` ausführen. Der optionale Parameter `NotificationInfoRepresentative` wird nicht belegt.[<=]

Nach erfolgreichem Aufruf dieser Operation hat das Aktenkonto den Status aktiviert. Die folgenden Aktivitäten ermöglichen, dass der Nutzer ohne erneutes Login fachliche Anwendungsfälle (bspw. Berechtigung vergeben, Dokument einstellen) mit dem Aktenkonto ausführen kann.

Das Laden des Schlüsselmaterial aus ePA-Aktensystem laden erfolgt gemäß "A_15344 - ePA-Frontend des Versicherten: Login - Autorisieren des Nutzers - Schlüsselmaterial aus ePA-Aktensystem laden".

Das Öffnen des Aktenkontext erfolgt gemäß "A_15347 - ePA-Frontend des Versicherten: Login - Aktenkontext öffnen - Aufbau sicherer Kanal zu Dokumentenverwaltung" und "A_15348 - ePA-Frontend des Versicherten: Login - Aktenkontext öffnen - Operation OpenContext".

6.2.5.2 Anbieter wechseln

Ein Versicherter kann mit diesem Anwendungsfall den Anbieter seines Aktenkontos wechseln und alle Inhalte zu einem neuen Anbieter übertragen. Hierfür sind mehrere Aktionen durch den Versicherten durchzuführen.

- Kündigung des bestehenden Aktenkontos beim alten Anbieter
- Registrierung eines neuen Aktenkontos bei einem neuen Anbieter
- Bestätigung vom neuen Anbieter erhalten, dass das neue Aktenkonto zur Datenübernahme vorbereitet ist

- Übernahme der Daten vom Aktenkonto des alten Anbieters zum neuen Anbieter im FdV

Wenn der Anbieterwechsel im Rahmen eines Wechsels der Krankenkasse erfolgt, erhält der Versicherte eine neue eGK. Die Registrierung der neuen eGK erfolgt mit dem Login im FdV oder im Rahmen der Vergabe einer Ad-hoc-Berechtigung bei einem LEI.

A_15369 - ePA-Frontend des Versicherten: Anbieter wechseln - Hinweis Verwaltungsprotokoll

Das ePA-Frontend des Versicherten MUSS vor Start des Anwendungsfalls "Anbieter wechseln" den Versicherten darauf hinweisen, dass das Verwaltungsprotokoll nicht zum neuen Anbieter übertragen wird, der Versicherte sich das Verwaltungsprotokoll lokal speichern muss, falls es weiterhin verfügbar sein soll und dem Versicherten ermöglichen den Anwendungsfall "Protokolldaten einsehen" zu starten.[<=]

A_15370 - ePA-Frontend des Versicherten: Anbieter wechseln

Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "UC 2.5 - Anbieter wechseln" aus [gemSysL_ePA] gemäß TAB_FdV_131 umsetzen.

Tabelle 37: TAB_FdV_131 – Anbieter wechseln

Name	Anbieter wechseln
Auslöser	<ul style="list-style-type: none"> • Aufruf des Anwendungsfalls in der GUI
Akteur	Versicherter
Vorbedingung	Der Versicherte hat ein neues Aktenkonto bei einem anderen Anbieter eröffnet. Das neue Aktenkonto ist bereit für den Datenimport. Der Versicherte ist im Aktenkonto des alten Anbieters angemeldet. Aktenschlüssel und Kontextschlüssel liegen unverschlüsselt in den Session-Daten vor.
Nachbedingung	Das Aktenkonto beim alten Anbieter befindet sich im Status „suspended“. Es ist nur noch ein lesender Zugriff möglich. Der neue Anbieter ist informiert, dass zeitnah ein Transferpaket für den Import in das Aktenkonto vom alten Anbieter bereitgestellt wird. Die Berechtigungen sind ggf. vom Aktenkonto des alten in das des neuen Anbieters übernommen.
Standardablauf	Aktivitäten im Standardablauf <ol style="list-style-type: none"> 1. Information zu neuen Anbieter ermitteln 2. Zugriffsberechtigungen anzeigen und Umzug bestätigen 3. Altes Aktenkonto in Exportzustand versetzen 4. Login beim Anbieter des neuen Aktenkontos 5. Daten in neues Aktenkonto importieren 6. Schlüsselmaterial für Versicherten in ePA-Aktensystem laden 7. Autorisierung aktualisieren 8. optional für jeden Berechtigten: Schlüsselmaterial im ePA-

	Aktensystem speichern
--	-----------------------

[<=]

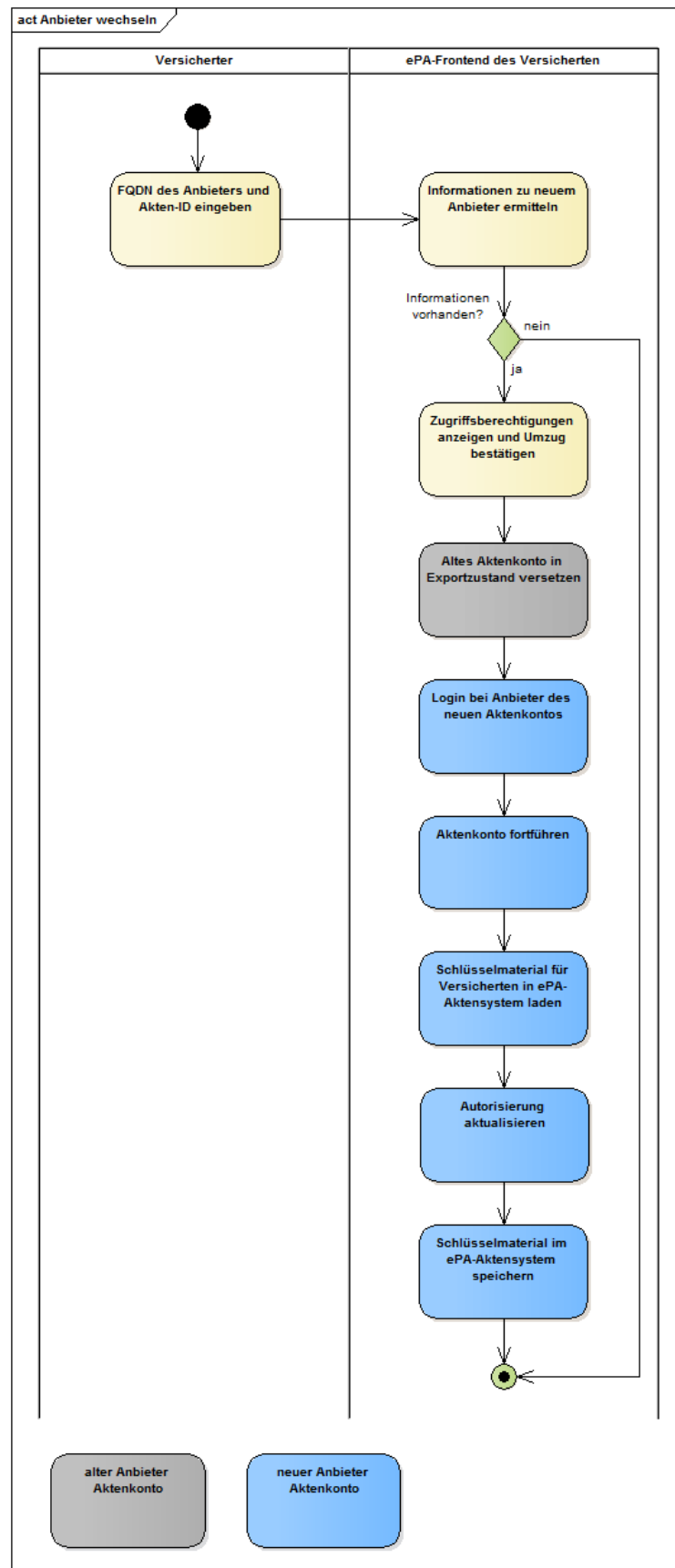


Abbildung 5: Aktivitätsdiagramm "Anbieter wechseln"

A_15371 - ePA-Frontend des Versicherten: Anbieter wechseln - Informationen zu neuen Anbieter

Das ePA-Frontend des Versicherten MUSS vom Versicherten im Anwendungsfall "Anbieter wechseln" die folgenden Registrierungsinformationen des neuen Anbieters abfragen:

- Akten-ID
- FQDN des Anbieters

und abbrechen, wenn die Informationen nicht vollständig vorliegen.[<=]

A_15372 - ePA-Frontend des Versicherten: Anbieter wechseln - Zugriffsberechtigungen anzeigen und Umzug bestätigen

Das ePA-Frontend des Versicherten MUSS dem Versicherten im Anwendungsfall "Anbieter wechseln" die zugriffsberechtigten Leistungserbringerinstitutionen, Vertreter und Kostenträger aus dem ePA-Aktensystem des alten Anbieters anzeigen und dem Versicherten die Möglichkeit geben, zu entscheiden, ob die bestehenden Berechtigungen in das ePA-Aktensystem des neuen Anbieters übernommen werden sollen.

[<=]

Die Anzeige der zugriffsberechtigten LEIs, Vertreter und KTR erfolgt mittels Anwendungsfall "Vergebene Berechtigungen anzeigen". Das Ergebnis der Operation `I_Authorization_Management_Insurant::getAuthorizationList` wird im weiteren Verlauf für die Einrichtung der Berechtigungen im neuen Aktenkonto genutzt.

A_15377 - ePA-Frontend des Versicherten: Anbieter wechseln - Aktenkonto in Exportzustand versetzen

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Anbieter wechseln" die Aktivität "Aktenkonto in Exportzustand versetzen" gemäß TAB_FdV_132 umsetzen.

Tabelle 38: TAB_FdV_132 – Anbieter wechseln - Aktenkonto in Exportzustand versetzen

<code>I_Account_Management_Insurant::SuspendAccount</code> Request erstellen	Eingangsparameter: <ul style="list-style-type: none"> • <code>AuthenticationAssertion</code> aus Session-Daten
<code>I_Account_Management_Insurant::SuspendAccount</code> Response verarbeiten	Rückgabedaten: <ul style="list-style-type: none"> • <code>PackageURL</code> Die URL ist ein Link auf ein Transportpaket, über den der Anbieter des neuen Aktenkontos ein Paket mit den Akteninhalten vom alten Anbieter herunterladen kann.

[<=]

Nachdem das Aktenkonto den Zustand SUSPENDED ("bereit für Anbieterwechsel") erhalten hat, kann der Versicherte oder ein berechtigter Nutzer nur noch lesend auf die Dokumente im Aktenkonto zugreifen.

A_15378 - ePA-Frontend des Versicherten: Anbieter wechseln - Login neues Aktenkonto

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Anbieter wechseln" die folgenden Aktivitäten aus dem Anwendungsfall "Login Aktensession" mit den Daten des

Aktenkontos beim neuen Anbieter ausführen, um sich beim neuen Aktenkonto einzuloggen:

- Authentisieren des Nutzers
- Autorisieren des Nutzers
- Sicheren Kanal zur Dokumentenverwaltung aufbauen
- Aktenkontext öffnen

[<=]

Das Authentisieren des Nutzers erfolgt mittels der übergreifenden Aktivität "Authentisieren des Nutzers". Wenn der Versicherte seine alternative Versichertenidentität nutzt, dann ist mit dieser auch die Authentisierung am neuen Aktensystem möglich.

Die Autorisierung des Nutzers erfolgt gemäß "A_15344 - ePA-Frontend des Versicherten: Login - Autorisieren des Nutzers - Schlüsselmaterial aus ePA-Aktensystem laden". Die Operation `getAuthorizationKeys` liefert ein Autorisierungstoken mit `RecordState = REGISTERED_FOR_MIGRATION` und kein Schlüsselmaterial.

Der Aufbau des sicheren Kanals zur Dokumentenverwaltung erfolgt gemäß "A_15347 - ePA-Frontend des Versicherten: Login - Aktenkontext öffnen - Aufbau sicherer Kanal zu Dokumentenverwaltung".

Das Öffnen des Aktenkontextes erfolgt gemäß "A_15348 - ePA-Frontend des Versicherten: Login - Aktenkontext öffnen - Operation `OpenContext`" unter Nutzung des Autorisierungstoken mit `RecordState = REGISTERED_FOR_MIGRATION` und dem Kontextschlüssel des Aktenkontos des alten Anbieters.

Der Versicherte lässt anschließend mittels der folgenden Operation seine Daten vom neuen Anbieter importieren.

A_15379 - ePA-Frontend des Versicherten: Anbieter wechseln - Aktenkonto fortführen

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Anbieter wechseln" die Aktivität "Aktenkonto fortführen" gemäß TAB_FdV_133 beim Aktenkonto des neuen Anbieters umsetzen.

Tabelle 39: TAB_FdV_133 – Anbieter wechseln - Aktenkonto fortführen

I_Account_Management_Insurant::ResumeAccount Request erstellen	Eingangsparameter: <ul style="list-style-type: none"> • PackageURL aus suspendAccount Operation • AuthenticationAssertion aus Session-Daten
I_Account_Management_Insurant::ResumeAccount Response verarbeiten	Rückgabedaten: <ul style="list-style-type: none"> • HTTP OK oder gematik SOAP-Fault

[<=]

Der Vorgang des Anbieterwechsels erfolgt aktensystemseitig asynchron, d. h. die Operation ist aus Sicht des FdV nach kurzer Zeit abgeschlossen, läuft im Backend jedoch weiter. Der Nutzer ist darauf hinzuweisen, dass er Zugriff auf sein Aktenkonto erst nach Abschluss der Datenmigration erhalten kann und dass diese länger dauern kann.

A_15374 - ePA-Frontend des Versicherten: Anbieter wechseln - AuthorizationKey für Aktenkontoinhaber erstellen

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Anbieter wechseln" einen AuthorizationKey mit dem für den Versicherten gesicherten Aktenschlüssel und Kontextschlüssel sowie `AuthorizationType = DOCUMENT_AUTHORIZATION` für den Versicherten erstellen.

[<=]

A_15375 - ePA-Frontend des Versicherten: Anbieter wechseln - Schlüsselmaterial für Aktenkontoinhaber im ePA-Aktensystem speichern

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Anbieter wechseln" für das Hochladen des Schlüsselmaterials in das ePA-Aktensystem des neuen Anbieters die übergreifende Aktivität "Schlüsselmaterial im ePA-Aktensystem speichern" mit dem Eingangsparameter `AuthorizationKey = erstellter AuthorizationKey` ausführen. Der optionale Parameter `NotificationInfoRepresentative` wird nicht belegt.[<=]

Nach erfolgreichem Aufruf dieser Operation ist das Aktenkonto aktiviert.

Nach erfolgreichem Aktivieren des Aktenkontos wird der Autorisierungstoken aktualisiert. Dies erfolgt durch das Laden des Schlüsselmaterial aus ePA-Aktensystem gemäß "A_15344 - ePA-Frontend des Versicherten: Login - Autorisieren des Nutzers - Schlüsselmaterial aus ePA-Aktensystem laden".

Wenn die bestehenden Berechtigungen in das ePA-Aktensystem des neuen Anbieters übernommen werden sollen, dann richtet das FdV die Berechtigungen ein.

A_15598 - ePA-Frontend des Versicherten: Anbieter wechseln - Berechtigung LEI und KTR erteilen

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Anbieter wechseln", wenn die Berechtigungen in das Aktenkonto des neuen Anbieters übernommen werden sollen, für jede aus dem Aktenkonto des alten Anbieters ermittelte Berechtigung einer LEI und KTR einen AuthorizationKey erstellen und das Schlüsselmaterial in das ePA-Aktensystem des neuen Anbieters laden.

[<=]

Die Berechtigung für einen Vertreter kann nur übernommen werden, wenn dem Versicherten die E-Mailadresse des Vertreters für die Geräteautorisierung bekannt ist. Hierbei wird davon ausgegangen, dass es sich bei dem Vertreter um eine Vertrauensperson handelt und der Versicherte die Daten kennen könnte. Anderenfalls kann die Berechtigung für den Vertreter nicht übernommen werden und muss mittels dem Anwendungsfall "Vertretung einrichten" zusammen mit dem Vertreter neu eingerichtet werden.

A_15635 - ePA-Frontend des Versicherten: Anbieter wechseln - Benachrichtigungsadresse Vertreter erfassen

Das ePA-Frontend des Versicherten MUSS es dem Nutzer im Anwendungsfall "Anbieter wechseln" ermöglichen, wenn die Berechtigungen in das Aktenkonto des neuen Anbieters übernommen werden sollen, für jeden Vertreter die Benachrichtigungsadresse für den Geräteautorisierung zu erfassen.[<=]

A_15636 - ePA-Frontend des Versicherten: Anbieter wechseln - Berechtigung Vertreter erteilen

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall „Anbieter wechseln“, wenn die Berechtigungen in das Aktenkonto des neuen Anbieters übernommen werden sollen und die Benachrichtigungsadresse des Vertreters für die Geräteautorisierung

bekannt ist, für jede aus dem Aktenkonto des alten Anbieters heruntergeladene Berechtigung eines Vertreters das Schlüsselmaterial in das ePA-Aktensystem laden.[<=]

Das Hochladen des Schlüsselmaterials in das ePA-Aktensystem erfolgt mit der übergreifende Aktivität "Schlüsselmaterial im ePA-Aktensystem speichern" mit dem Eingangsparameter `AuthorizationKey` = erstellter `AuthorizationKey` . Der optionale Parameter `NotificationInfoRepresentative` wird für LEI und KTR nicht belegt.

Die Information, welche Geräte durch Nutzer autorisiert sind, wird nicht übertragen. D.h. der Nutzer muss bei der nächsten Anmeldung am Aktenkonto des neuen Anbieters sein GdV autorisieren.

6.2.6 Berechtigungsverwaltung und Berechtigungserhalt

Dieses Kapitel beschreibt Anwendungsfälle zur Vergabe und Administration von Berechtigungen zum Zugriff auf das Aktenkonto sowie Anwendungsfälle zum Berechtigungserhalt, d.h. von Möglichkeiten, wie der Versicherte eine neu erhaltene eGK im Aktenkonto registriert.

6.2.6.1 Berechtigung für LEI vergeben

Mit diesem Anwendungsfall richtet ein Versicherter oder ein berechtigter Vertreter Zugriffsberechtigungen auf das Aktenkonto für Leistungserbringerinstitutionen ein.

Im FdV können nur Berechtigungen an LEI vergeben werden, die im Verzeichnisdienst (VZD) der TI registriert sind.

A_15380 - ePA-Frontend des Versicherten: Suche Leistungserbringerinstitution in Verzeichnisdienst

Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, eine oder mehrere LEI im Verzeichnisdienst zu suchen und für die Vergabe von Berechtigungen auszuwählen.[<=]

Für die Umsetzung der Suche siehe "6.2.3.14- Leistungserbringerinstitution im Verzeichnisdienst der TI finden ".

Aus dem Ergebnis der Abfrage bestimmt das FdV die TelematikID und den Namen der zu berechtigenden LEIs.

A_15381 - ePA-Frontend des Versicherten: Auswahl Berechtigungskonfiguration

Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, für jede Leistungserbringerinstitution, für die eine Berechtigung vergeben oder geändert werden soll, die folgenden Parameter festzulegen:

- Option Berechtigungsdauer: 1 Tag, 28 Tage [default], 18 Monate oder flexibel 1-540 Tage
- Option Zugriff auf durch LEI eingestellte Dokumente und leistungserbringeräquivalente Dokumente [default = ja]
- Option Zugriff auf durch den Versicherten oder einen Vertreter eingestellte Dokumente [default = nein]
- Option Zugriff auf durch Krankenkassen eingestellte Dokumente [default = nein]

[<=]

A_15382 - ePA-Frontend des Versicherten: Bestätigung Berechtigungskonfiguration

Das ePA-Frontend des Versicherten MUSS, bevor es eine Berechtigung an eine LEI vergibt oder ändert, eine Bestätigung der gewählten Berechtigungskonfiguration vom Nutzer einholen.[<=]

A_15383 - ePA-Frontend des Versicherten: Berechtigung an LEI für Aktenkonto vergeben

Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "UC 3.1 - Berechtigung durch einen Versicherten vergeben" aus [gemSysL_ePA] für jede LEI, für die eine Berechtigung vergeben werden soll, gemäß TAB_FdV_134 umsetzen.

Tabelle 40: TAB_FdV_134 – Berechtigung an LEI für Aktenkonto vergeben

Name	Berechtigung an LEI für Aktenkonto vergeben
Auslöser	<ul style="list-style-type: none"> Aufruf des Anwendungsfalls in der GUI
Akteur	Versicherter oder berechtigter Vertreter
Vorbedingung	<p>Es besteht eine Aktensession mit gültigen Session-Daten.</p> <p>Die TelematikID und der Name der LEI sind bekannt. Der Nutzer hat die Parameter für die Berechtigungen ausgewählt und die Vergabe der Berechtigung bestätigt.</p>
Nachbedingung	<p>Die LEI ist zum Zugriff auf das Aktenkonto berechtigt. Das notwendige Schlüsselmateriale ist in der Autorisierung hinterlegt. Ein Policy Document für den LEI ist in der Dokumentenverwaltung hinterlegt.</p>
Standardablauf	<p>Aktivitäten im Standardablauf</p> <ol style="list-style-type: none"> 1. AuthorizationKey für LEI erstellen 2. Schlüsselmateriale im ePA-Aktensystem speichern 3. Policy Document für LEI erstellen 4. Policy Document in Dokumentenverwaltung laden

[<=]

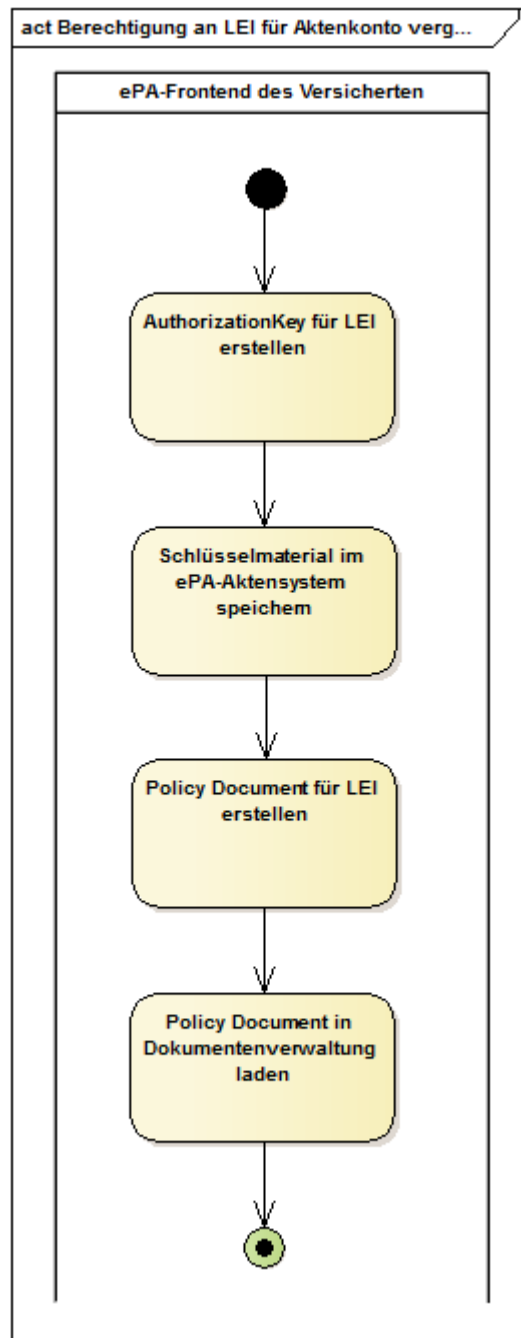


Abbildung 6: Aktivitätsdiagramm "Berechtigung an LEI für Aktenkonto vergeben"

A_15384 - ePA-Frontend des Versicherten: Berechtigung an LEI vergeben - AuthorizationKey erstellen

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Berechtigung an LEI für Aktenkonto vergeben" einen AuthorizationKey mit `AuthorizationType = DOCUMENT_AUTHORIZATION` und `validTo` entsprechend der vom Nutzer festgelegten Berechtigungsdauer für die zu berechtigende LEI erstellen.[<=]

A_15385 - ePA-Frontend des Versicherten: Berechtigung an LEI vergeben - Schlüsselmaterial im ePA-Aktensystem speichern

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Berechtigung an LEI für Aktenkonto vergeben" für das Hochladen des Schlüsselmaterials in das ePA-Aktensystem die übergreifende Aktivität "Schlüsselmaterial im ePA-Aktensystem speichern" mit dem Eingangsparameter `AuthorizationKey = erstellter AuthorizationKey` ausführen. Der optionale Parameter `NotificationInfoRepresentative` wird nicht belegt.[<=]

A_15386 - ePA-Frontend des Versicherten: Berechtigung an LEI vergeben - Policy Document erstellen

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Berechtigung an LEI für Aktenkonto vergeben" ein Policy Document für den zu Berechtigenden entsprechend den für die Berechtigung ausgewählten Parametern erstellen.[<=]

Für Informationen zu Policy Documents und deren Nutzungsvorgaben siehe "5.3.1.- Policy Documents".

A_15387 - ePA-Frontend des Versicherten: Berechtigung an LEI vergeben - Policy Document hochladen

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Berechtigung an LEI für Aktenkonto vergeben" zum Hochladen des Policy Documents in die Dokumentenverwaltung die übergreifende Aktivität "Dokumentenset in Dokumentenverwaltung hochladen" mit einer Provide And Register Document Set-b Message für Policy Documents ausführen.[<=]

6.2.6.2 Vertretung einrichten

Mit diesem Anwendungsfall richtet ein Versicherter (Aktenkontoinhaber) eine Zugriffsberechtigung für einen Vertreter ein. Dieser Vertreter muss über eine eigene gültige eGK verfügen und den PIN seiner eGK kennen oder eine alternative Authentisierung für ein geeignetes FdV auf seinem GdV eingerichtet haben. Der Anwendungsfall steht einem berechtigten Vertreter nicht zur Verfügung.

Zur Verbesserung des Datenschutzes muss die Vertretung zusätzlich über eine E-Mail durch den Versicherten bestätigt werden.

Vor der Berechtigung müssen der Name, die Versicherten-ID sowie die E-Mailadresse des Vertreters für die Geräteautorisierung erfasst werden.

A_15389 - ePA-Frontend des Versicherten: Daten des Vertreters

Das ePA-Frontend des Versicherten MUSS es dem Nutzer im Anwendungsfall "Vertretung einrichten" ermöglichen, den Namen, die Versicherten-ID und eine Benachrichtigungsadresse (E-Mail) für die Geräteautorisierung des Vertreters zu erfassen.
[<=]

Die Berechtigungsdauer für Vertreter kann nicht zeitlich begrenzt werden. Wenn ein Vertreter berechtigt ist auf die Dokumente zuzugreifen, dann kann der Vertreter auf alle Dokumente im Aktenkonto zugreifen.

A_15391 - ePA-Frontend des Versicherten: Vertretung einrichten

Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "UC 3.2 - Vertretung durch einen Versicherten einrichten" aus [gemSysL_ePA] gemäß TAB_FdV_135 umsetzen.

Tabelle 41: TAB_FdV_135 – Vertretung einrichten

Name	Vertretung einrichten
Auslöser	Aufruf des Anwendungsfalls in der GUI
Akteur	Versicherter
Vorbedingung	Die Versicherten-ID, der Name und die Benachrichtigungsadresse des Vertreters für die Geräteautorisierung sind bekannt. Es besteht eine Aktensession mit gültigen Session-Daten.
Nachbedingung	Der Vertreter ist zum Zugriff auf das Aktenkonto berechtigt. Das notwendige Schlüsselmaterial ist in der Autorisierung hinterlegt. Die Policy Document für den Vertreter ist in der Dokumentenverwaltung hinterlegt.
Standardablauf	Aktivitäten im Standardablauf <ol style="list-style-type: none"> 1. AuthorizationKey für Vertreter erstellen 2. Schlüsselmaterial im ePA-Aktensystem speichern 3. Policy Document für Vertreter erstellen 4. Policy Document in Dokumentenverwaltung laden

[<=]

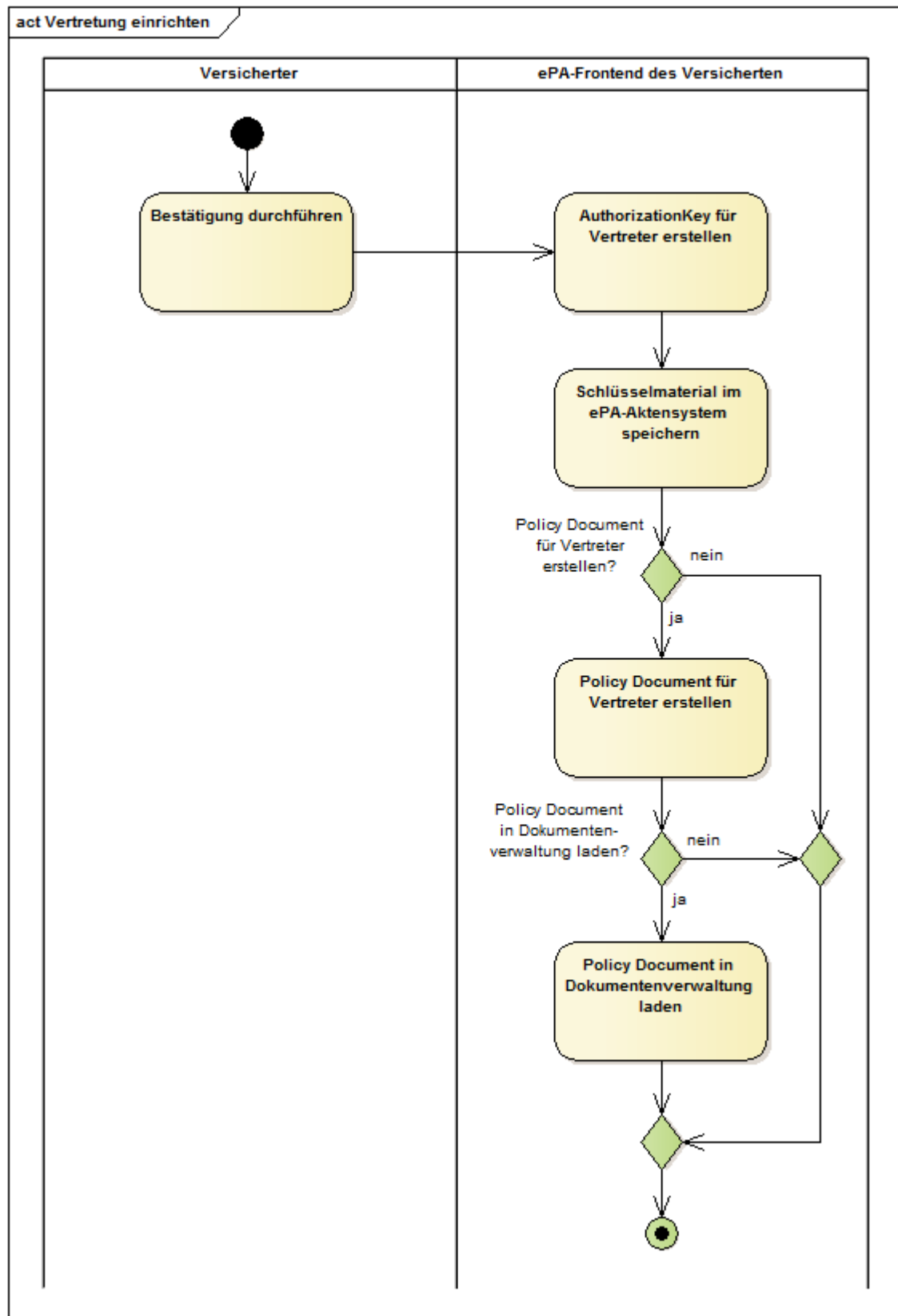


Abbildung 7: Aktivitätsdiagramm "Vertretung einrichten"

A_15396 - ePA-Frontend des Versicherten: Vertretung einrichten - AuthorizationKey erstellen

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Vertretung einrichten" einen AuthorizationKey für den Vertreter mit AuthorizationType = DOCUMENT_AUTHORIZATION erstellen.
[<=]

Falls der Vertreter die Vertretung nicht ausschließlich in einer LEI sondern auch an einem FdV wahrnehmen möchte, muss in der folgende Aktivität die Benachrichtigungsadresse des Vertreters für die Geräteautorisierung an das Aktensystem übergeben werden, da der Vertreter sich ansonsten von seinem FdV nicht autorisieren kann.

A_15397 - ePA-Frontend des Versicherten: Vertretung einrichten - Schlüsselmaterial im ePA-Aktensystem speichern

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Vertretung einrichten" für das Hochladen des Schlüsselmaterials des Vertreters in das ePA-Aktensystem die übergreifende Aktivität "Schlüsselmaterial im ePA-Aktensystem speichern" mit den Eingangsparametern AuthorizationKey = erstellter AuthorizationKey und NotificationInfoRepresentative = Benachrichtigungsadresse für die Geräteautorisierung ausführen.[<=]

A_15398 - ePA-Frontend des Versicherten: Vertretung einrichten - Policy Document erstellen

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Vertretung einrichten", ein Policy Document für den zu berechtigenden Vertreter erstellen.[<=]

Für Informationen zu Policy Documents und deren Nutzungsvorgaben siehe "5.3.1.- Policy Documents".

A_15399 - ePA-Frontend des Versicherten: Vertretung einrichten - Policy Document hochladen

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Vertretung einrichten" zum Hochladen des Policy Documents in die Dokumentenverwaltung die übergreifende Aktivität "Dokumentenset in Dokumentenverwaltung hochladen" mit einer Provide And Register Document Set-b Message für Policy Documents ausführen.[<=]

Dem Versicherten kann ein Hinweis angezeigt werden, dass zum Abschluss eine Autorisierung der Vertretung über eine E-Mail erfolgen muss, welche dem Versicherten vom Aktensystem zugesandt wird.

Nach der Einrichtung der Vertretung teilt der Versicherte dem Vertreter die Informationen mit, welche der Vertreter in seinem FdV konfigurieren muss, um auf das Aktenkonto zugreifen zu können. Diese Informationen können der Konfiguration des FdV entnommen werden.

A_15400 - ePA-Frontend des Versicherten: PDF mit Information für Vertretung

Das ePA-Frontend des Versicherten MUSS dem Versicherten die Möglichkeit geben, ein druckbares PDF mit den Informationen für die Vertretung zu erzeugen. Das Dokument muss die folgenden Informationen des Versicherten, welcher vertreten wird, beinhalten:

- Versicherten-ID
- FQDN des Anbieter

[<=]

Zur Unterstützung kann das FdV bspw. zusätzlich eine E-Mail (an die Benachrichtigungsadresse zur Geräteautorisierung) bereitstellen, um die Informationen zu übermitteln.

6.2.6.3 Berechtigung für Kostenträger vergeben

Mit diesem Anwendungsfall richtet ein Versicherter oder ein berechtigter Vertreter Zugriffsberechtigungen auf das Aktenkonto für einen Kostenträger ein. Der Zugriff eines KTR ist auf das Einstellen von Dokumenten beschränkt.

Voraussetzung ist, dass die TelematikID (siehe [gemSpec_PKI#Tab_SMCB_TID_GKVSU]) des KTR bekannt ist. Diese kann über eine Abfrage im Verzeichnisdienst der TI ermittelt werden oder in einem gekoppelten FdV fest vorgegeben werden.

A_17436 - ePA-Frontend des Versicherten: Kostenträger in Verzeichnisdienst der TI finden

Das ePA-Frontend des Versicherten SOLL es dem Nutzer mittels der Aktivität "Suchanfrage Verzeichnisdienst der TI" ermöglichen, einen Kostenträger im Verzeichnisdienst zu suchen und für die Vergabe von Berechtigungen auszuwählen.[<=]

Für die Suche ist mindestens das Kriterium (`entryType= "Kostenträger Betriebsstätte"`) zu verwenden.

Die Suche kann Suche automatisiert werden, wenn das Institutionskennzeichen der Krankenkasse des Aktenkontoinhabers bekannt ist und für die Suche das Kriterium (`domainID = IK-Nummer`) verwenden. Die IK-Nummer ist das 9-stellige Institutionskennzeichen des Kostenträgers, das als Organizational Unit Name im Subject Distinguished Name des C.CH.AUT- bzw. C.CH.AUT_ALT-Zertifikates des Aktenkontoinhabers zu finden ist.

A_17188 - ePA-Frontend des Versicherten: Bestätigung Berechtigung für Kostenträger

Das ePA-Frontend des Versicherten MUSS, bevor es eine Berechtigung an einen Kostenträger vergibt, eine Bestätigung vom Nutzer einholen. Hierbei ist der Name des zu berechtigenden Kostenträgers kenntlich zu machen.[<=]

A_17189 - ePA-Frontend des Versicherten: Berechtigung an Kostenträger für Aktenkonto vergeben

Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "UC 3.1 - Berechtigung durch einen Versicherten vergeben" aus [gemSysL_ePA] für den Kostenträger, für den eine Berechtigung vergeben werden soll, gemäß TAB_FdV_171 umsetzen.

Tabelle 42: TAB_FdV_171 – Berechtigung an Kostenträger für Aktenkonto vergeben

Name	Berechtigung an Kostenträger für Aktenkonto vergeben
Auslöser	<ul style="list-style-type: none"> Aufruf des Anwendungsfalls in der GUI
Akteur	Versicherter oder berechtigter Vertreter
Vorbedingung	Es besteht eine Aktensession mit gültigen Session-Daten. Der Name und die TelematikID des KTR sind bekannt.

	Der Nutzer hat die Vergabe der Berechtigung bestätigt.
Nachbedingung	Der Kostenträger ist zum Zugriff auf das Aktenkonto berechtigt. Das notwendige Schlüsselmaterial ist in der Autorisierung hinterlegt. Ein Policy Document für den Kostenträger ist in der Dokumentenverwaltung hinterlegt.
Standardablauf	Aktivitäten im Standardablauf <ol style="list-style-type: none"> 1. AuthorizationKey für Kostenträger erstellen 2. Schlüsselmaterial im ePA-Aktensystem speichern 3. Policy Document für Kostenträger erstellen 4. Policy Document in Dokumentenverwaltung laden

[<=]

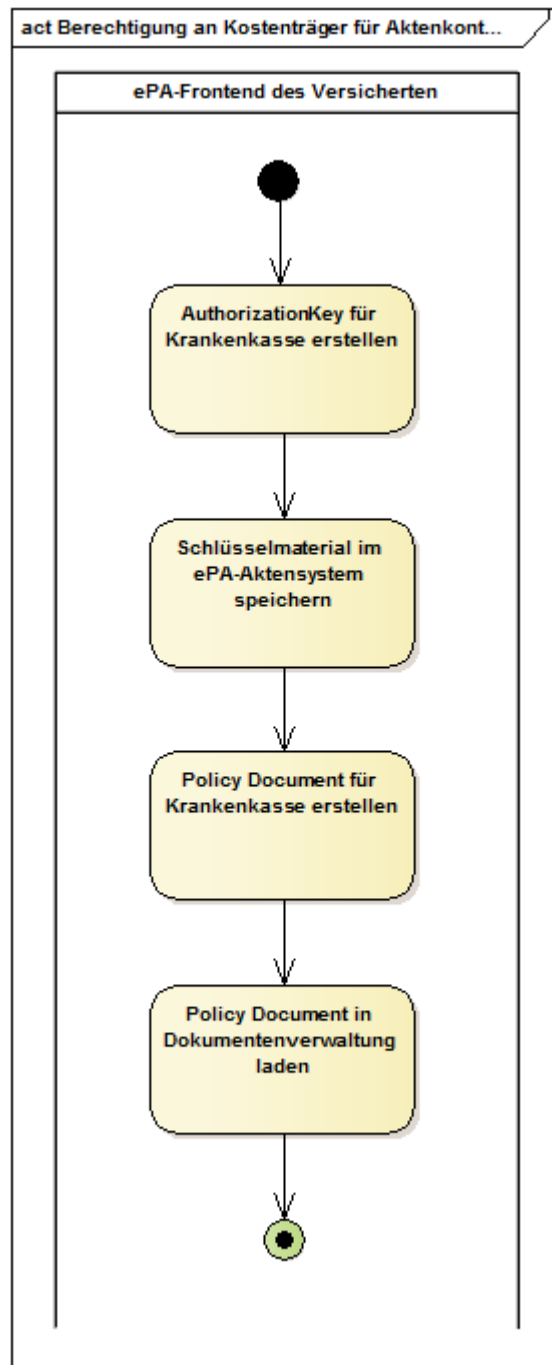


Abbildung 8 Berechtigung an Kostenträger für Aktenkonto vergeben

A_17190 - ePA-Frontend des Versicherten: Berechtigung Kostenträger vergeben - AuthorizationKey erstellen

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Berechtigung an Kostenträger für Aktenkonto vergeben" einen AuthorizationKey mit `AuthorizationType = DOCUMENT_AUTHORIZATION` für den zu berechtigenden Kostenträger erstellen.[<=]

A_17191 - ePA-Frontend des Versicherten: Berechtigung Kostenträger vergeben - Schlüsselmateriale im ePA-Aktensystem speichern

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Berechtigung an Kostenträger für Aktenkonto vergeben" für das Hochladen des Schlüsselmateriale in das ePA-Aktensystem die übergreifende Aktivität "Schlüsselmateriale im ePA-Aktensystem speichern" mit dem Eingangsparameter `AuthorizationKey` = erstellter

`AuthorizationKey` ausführen. Der optionale Parameter `NotificationInfoRepresentative` wird nicht belegt.[<=]

A_17192 - ePA-Frontend des Versicherten: Berechtigung Kostenträger vergeben - Policy Document erstellen

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Berechtigung an Kostenträger für Aktenkonto vergeben" ein Policy Document für den zu Berechtigenden erstellen.[<=]

Für Informationen zu Policy Documents und deren Nutzungsvorgaben siehe "5.3.1.- Policy Documents".

A_17193 - ePA-Frontend des Versicherten: Berechtigung Kostenträger vergeben - Policy Document hochladen

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Berechtigung an Kostenträger für Aktenkonto vergeben" zum Hochladen des Policy Documents in die Dokumentenverwaltung die übergreifende Aktivität "Dokumentenset in Dokumentenverwaltung hochladen" mit einer Provide And Register Document Set-b Message für Policy Documents ausführen.[<=]

6.2.6.4 Vergebene Berechtigungen anzeigen

Mit diesem Anwendungsfall kann ein Nutzer eine Liste der für das Aktenkonto vergebenen Berechtigungen anzeigen lassen. Diese Liste beinhaltet die zugriffsberechtigten Leistungserbringer, die berechtigten Vertreter und den Aktenkontoinhaber selbst sowie die Details zu Berechtigung (für LEI: Berechtigungsdauer, Zugriff auf durch den Versicherten eingestellte Dokumente).

A_15401 - ePA-Frontend des Versicherten: Vergebene Berechtigungen anzeigen

Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "UC 3.5 - Berechtigungen durch einen Versicherten auflisten" aus [gemSysL_ePA] gemäß TAB_FdV_137 umsetzen.

Tabelle 43: TAB_FdV_137 – Vergebene Berechtigungen anzeigen

Name	Vergebene Berechtigungen anzeigen
Auslöser	<ul style="list-style-type: none"> • Aufruf des Anwendungsfalls in der GUI • Anwendungsfall "Anbieter wechseln"
Akteur	Versicherter bzw. ein berechtigter Vertreter
Vorbedingung	Es besteht eine Aktensession mit gültigen Session-Daten.
Nachbedingung	Die Liste der für das Aktenkonto vergebenen Berechtigungen wird angezeigt und kann durch den Nutzer bearbeitet werden.

Standardablauf	Aktivitäten im Standardablauf 1. Vergebene Berechtigungen bestimmen 2. Liste zum Anzeigen aufarbeiten
----------------	-------------------------------------------------------------------------------------------------------------

[<=]

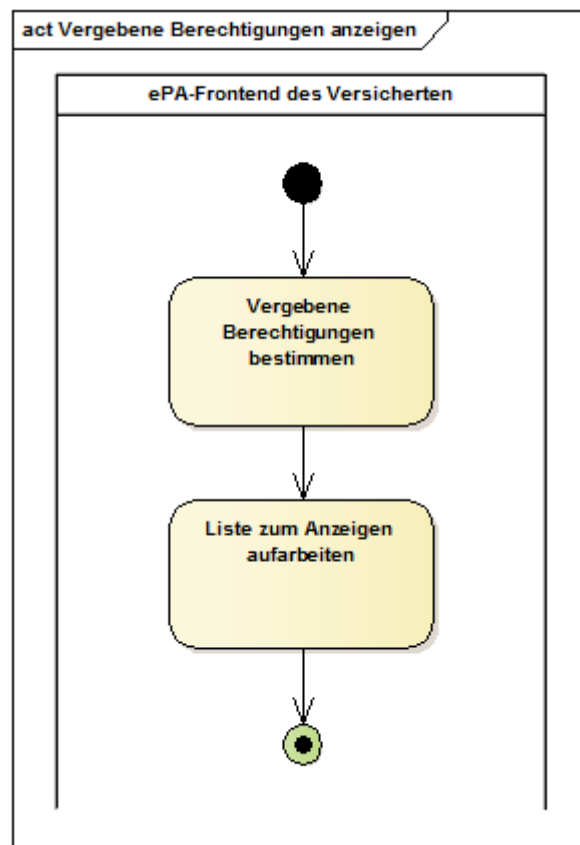


Abbildung 9: Aktivitätsdiagramm "Vergebene Berechtigungen anzeigen"

A_15402 - ePA-Frontend des Versicherten: Berechtigungen anzeigen - Berechtigungen bestimmen

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Vergebene Berechtigungen anzeigen" die übergreifende Aktivität "Vergebene Berechtigungen bestimmen" ausführen.[<=]

A_15403 - ePA-Frontend des Versicherten: Ergebnisliste Berechtigungen Felder

Das ePA-Frontend des Versicherten MUSS im Ergebnis der Suche nach Berechtigungen mindestens

- Name der Leistungserbringerinstitution, des Kostenträgers bzw. des Vertreters im Klartext,
- für LEI: Zugriff auf durch LEI eingestellte Dokumente und leistungserbringeräquivalente Dokumente erlaubt,
- für LEI: Zugriff auf durch Versicherte eingestellte Dokumente erlaubt,

- für LEI: Zugriff auf durch Kostenträger eingestellte Dokumente erlaubt,
- für LEI: eingestellte und verbleibende Berechtigungsdauer

anzeigen.[<=]

Das Ergebnis der Suche soll für den Nutzer sortierbar und filterbar dargestellt werden.

A_15405 - ePA-Frontend des Versicherten: Ergebnisliste Berechtigungen drucken und speichern

Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, das Ergebnis der Suche nach Berechtigungen auszudrucken und lokal zu speichern.[<=]

Das lokale Speichern kann im PDF-Format angeboten werden.

Das FdV ermöglicht es dem Nutzer, Einträge in der Ergebnisliste Berechtigungen zu bearbeiten oder zu löschen.

6.2.6.5 Eingerichtete Vertretungen anzeigen

Mit diesem Anwendungsfall kann ein Nutzer eine Liste der Versicherten anzeigen lassen, für die im FdV die Wahrnehmung der Vertretung durch ihn konfiguriert ist ("*ich bin Vertreter für*"). Es wird dabei nicht geprüft, ob im Aktenkonto des zu Vertretenden auch tatsächlich eine Berechtigung für den Nutzer vorliegt.

A_15406 - ePA-Frontend des Versicherten: Liste "ich bin Vertreter für" anzeigen

Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, eine Liste mit den im FdV für ihn konfigurierten Vertretungen anderer Versicherter anzuzeigen.[<=]

6.2.6.6 Bestehende Berechtigungen verwalten

6.2.6.6.1 Berechtigung für LEI ändern

Mit diesem Anwendungsfall kann ein Versicherter bzw. ein berechtigter Vertreter die Parameter für eine berechtigte LEI ändern.

A_15407 - ePA-Frontend des Versicherten: Konfiguration LEI ändern

Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, für die für den Zugriff auf das Aktenkonto berechtigten LEI die Konfiguration für die Berechtigungsdauer sowie dafür, ob der Zugriff auf durch LEI, Versicherte oder Kostenträger eingestellte Dokumente erlaubt ist, zu ändern.
[<=]

Die zum Zugriff auf das Aktenkonto berechtigten LEIs werden mit der übergreifende Aktivität "Vergebene Berechtigungen bestimmen" ermittelt.

A_15408 - ePA-Frontend des Versicherten: Berechtigung für LEI ändern

Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "UC 3.6 - Bestehende Berechtigungen durch einen Versicherten verwalten" aus [gemSysL_ePA] für jede LEI, für die Konfiguration seiner Berechtigung geändert werden soll, gemäß TAB_FdV_138 umsetzen.

Tabelle 44: TAB_FdV_138 – Berechtigung für LEI ändern

Name	Berechtigung für LEI ändern
Auslöser	<ul style="list-style-type: none"> • Aufruf der Aktion zum Ändern der Berechtigung in der GUI
Akteur	Versicherter oder berechtigter Vertreter

Vorbedingung	<p>Es besteht eine Aktensession mit gültigen Session-Daten.</p> <p>Der Nutzer hat die Konfiguration für eine Berechtigung geändert und die Änderung der Einstellung bestätigt. Das Policy Document und der AuthorizationKey für die LEI stehen zur Verfügung.</p>
Nachbedingung	<p>Die geänderten Einstellungen für die Berechtigung der LEI sind als Policy Document in der Dokumentenverwaltung hinterlegt. Die Gültigkeitsdauer des Schlüsselmaterials in der Autorisierung ist ggf. aktualisiert.</p>
Standardablauf	<p>Aktivitäten im Standardablauf</p> <ol style="list-style-type: none"> 1. Policy Document für LEI anpassen 2. Wenn die Berechtigungsdauer geändert wurde <ol style="list-style-type: none"> a. AuthorizationKey für LEI erstellen b. Schlüsselmaterial im ePA-Aktensystem ersetzen 3. Neues Policy Document in Dokumentenverwaltung laden

[<=]

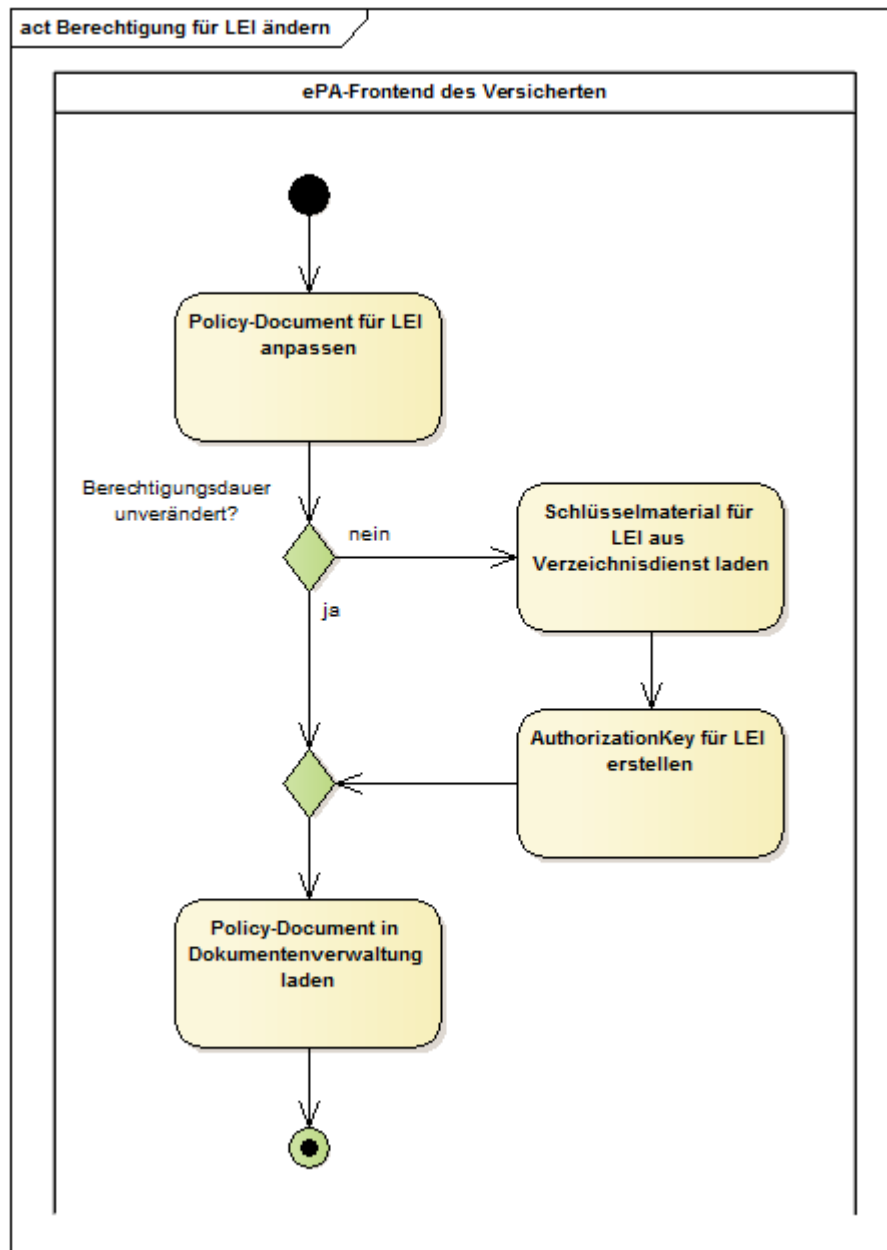


Abbildung 10: Aktivitätsdiagramm "Berechtigung für LEI ändern"

Das Policy Document der LEI steht aus der Aktivität "Vergebene Berechtigungen bestimmen" zur Verfügung.

A_15409 - ePA-Frontend des Versicherten: Berechtigung für LEI ändern - Policy Document anpassen

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Berechtigung für LEI ändern" das Policy Document entsprechend der gewählten Einstellungen für Berechtigungsdauer und/oder Aktenanteil anpassen.[<=]

Die Anpassung des AuthorizationKey muss nur erfolgen, wenn die Berechtigungsdauer für die LEI geändert wurde.

Die TelematikID der LEI lässt sich aus dem Policy Document bestimmen.

A_15412 - ePA-Frontend des Versicherten: Berechtigung für LEI ändern - AuthorizationKey für LEI erstellen

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Berechtigung für LEI ändern", wenn die Einstellung für Berechtigungsdauer geändert wurde, einen AuthorizationKey mit AuthorizationType = DOCUMENT_AUTHORIZATION und validTo entsprechend der vom Nutzer festgelegten Berechtigungsdauer für die zu berechtigende LEI erstellen.

[<=]

A_15413 - ePA-Frontend des Versicherten: Berechtigung für LEI ändern - Schlüsselmaterial im ePA-Aktensystem ersetzen

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Berechtigung für LEI ändern", wenn die Einstellung für Berechtigungsdauer geändert wurde, für das Hochladen des Schlüsselmaterials in das ePA-Aktensystem die übergreifende Aktivität "Schlüsselmaterial im ePA-Aktensystem ersetzen" mit den Eingangsparametern NewAuthorizationKey = geänderter AuthorizationKey ausführen.[<=]

A_15414 - ePA-Frontend des Versicherten: Berechtigung für LEI ändern - Policy Document in Dokumentenverwaltung laden

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Berechtigung für LEI ändern" für das Hochladen des Policy Documents in die Dokumentenverwaltung die übergreifende Aktivität "Dokumentenset in Dokumentenverwaltung hochladen" mit einer Provide And Register Document Set-b Message für das angepasste Policy Documents ausführen.[<=]

Die Dokumentenverwaltung verarbeitet das Policy Document und überschreibt die vorher geltenden Regeln.

6.2.6.6.2 Berechtigung für LEI löschen

Mit diesem Anwendungsfall kann ein Versicherter bzw. ein berechtigter Vertreter einer berechtigten LEI die Berechtigung entziehen.

A_15415 - ePA-Frontend des Versicherten: LEI zum Entzug der Berechtigung markieren

Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, berechtigte LEI für den Entzug der Berechtigung auszuwählen.[<=]

Die zum Zugriff auf das Aktenkonto berechtigten LEIs werden mit der übergreifende Aktivität "Vergebene Berechtigungen bestimmen" ermittelt.

A_15416 - ePA-Frontend des Versicherten: Berechtigung für LEI löschen

Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "UC 3.6 - Bestehende Berechtigungen durch einen Versicherten verwalten" aus [gemSysL_ePA] für jeden berechtigten LEI, dessen Berechtigung entzogen werden soll, gemäß TAB_FdV_139 umsetzen.

Tabelle 45: TAB_FdV_139 – Berechtigung löschen

Name	Berechtigung für LEI löschen
Auslöser	<ul style="list-style-type: none"> Aufruf der Aktion zum Löschen der Berechtigung in der GUI

Akteur	Versicherter oder berechtigter Vertreter
Vorbedingung	<p>Es besteht eine Aktensession mit gültigen Session-Daten.</p> <p>Der Nutzer hat eine LEI zum Löschen der Berechtigung ausgewählt und das Löschen bestätigt.</p> <p>Das Policy Document und Informationen zum AuthorizationKey der LEI stehen zur Verfügung.</p>
Nachbedingung	Die LEI ist nicht mehr für den Zugriff auf das Aktenkonto autorisiert.
Standardablauf	<p>Aktivitäten im Standardablauf</p> <ol style="list-style-type: none"> 1. Policy Document in Dokumentenverwaltung löschen 2. Schlüsselmaterial in ePA-Aktensystem löschen

[<=]

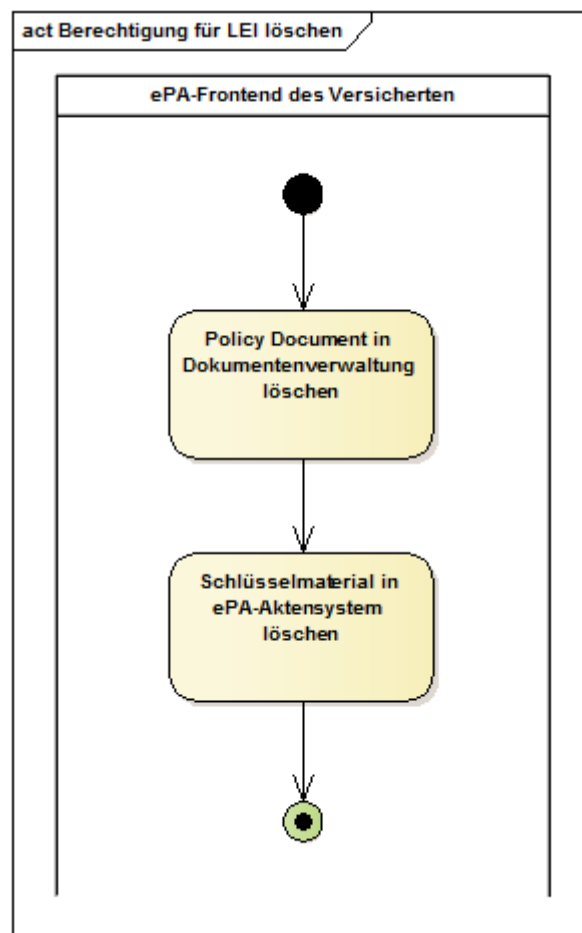


Abbildung 11: Aktivitätsdiagramm "Berechtigung für LEI löschen"

A_15417 - ePA-Frontend des Versicherten: Berechtigung für LEI löschen - Policy Document in Dokumentenverwaltung löschen

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Berechtigung für LEI löschen" für das Löschen des Policy Document in die Dokumentenverwaltung die übergreifende Aktivität "Dokumentenset in Dokumentenverwaltung löschen" mit einer RemoveDocuments_Message für den über die XDS-Metadaten ermittelten Dokument Identifier des Policy Documents der LEI ausführen.[<=]

Die TelematikID der LEI kann aus dem Policy Document bestimmt werden.

A_15418 - ePA-Frontend des Versicherten: Berechtigung für LEI löschen - Schlüsselmaterial in ePA-Aktensystem löschen

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Berechtigung für LEI löschen" für das Löschen des Schlüsselmaterials die übergreifende Aktivität "Schlüsselmaterial im ePA-Aktensystem löschen" mit dem EingangsparameterActorID = TelematikID der LEI ausführen.
[<=]

6.2.6.6.3 Berechtigung für Vertreter löschen

Mit diesem Anwendungsfall kann ein Versicherter einem berechtigten Vertreter die Berechtigung entziehen.

A_16044 - ePA-Frontend des Versicherten: Vertreter zum Entzug der Berechtigung markieren

Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, berechtigte Vertreter für den Entzug der Berechtigung auszuwählen.[<=]

Die zum Zugriff auf das Aktenkonto berechtigten Vertreter werden mit der übergreifende Aktivität "Vergebene Berechtigungen bestimmen" ermittelt.

A_16045 - ePA-Frontend des Versicherten: Berechtigung für Vertreter löschen

Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "UC 3.6 - Bestehende Berechtigungen durch einen Versicherten verwalten" aus [gemSysL_ePA] für jeden berechtigten Vertreter, dessen Berechtigung entzogen werden soll, gemäß TAB_FdV_168 umsetzen.

Tabelle 46: TAB_FdV_168 – Berechtigung Vertreter löschen

Name	Berechtigung für Vertreter löschen
Auslöser	<ul style="list-style-type: none"> Aufruf der Aktion zum Löschen der Berechtigung in der GUI
Akteur	Versicherter
Vorbedingung	<p>Es besteht eine Aktensession mit gültigen Session-Daten.</p> <p>Der Nutzer hat einen Vertreter zum Löschen der Berechtigung ausgewählt und das Löschen bestätigt. Informationen zum AuthorizationKey und ggf. das Policy Document des Vertreters stehen zur Verfügung.</p>
Nachbedingung	Der Vertreter ist nicht mehr für den Zugriff auf das Aktenkonto autorisiert.

Standardablauf	Aktivitäten im Standardablauf <ol style="list-style-type: none"> 1. Wenn dem Vertreter der Zugriff auf Dokumente gewährt wurde <ol style="list-style-type: none"> a. Policy Document in Dokumentenverwaltung löschen 2. Schlüsselmaterial in ePA-Aktensystem löschen
----------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

[<=]

A_16046 - ePA-Frontend des Versicherten: Berechtigung für Vertreter löschen - Policy Document in Dokumentenverwaltung löschen

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Berechtigung für Vertreter löschen", falls der Vertreter Zugriff auf die Dokumente des Aktenkontos besitzt (`AuthorizationType = DOCUMENT_AUTHORIZATION`), für das Löschen des Policy Document in die Dokumentenverwaltung die übergreifende Aktivität "Dokumentenset in Dokumentenverwaltung löschen" mit einer `RemoveDocuments_Message` für den über die XDS-Metadaten ermittelten Dokument Identifier des Policy Documents des Vertreters ausführen.

[<=]

Die Versicherten-ID für den Vertreter kann aus dem `AuthorizationKey` bestimmt werden.

A_16047 - ePA-Frontend des Versicherten: Berechtigung für Vertreter löschen - Schlüsselmaterial in ePA-Aktensystem löschen

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Berechtigung für Vertreter löschen" für das Löschen des Schlüsselmaterials die übergreifende Aktivität "Schlüsselmaterial im ePA-Aktensystem löschen" mit dem Eingangsparameter `ActorID` = Versicherten-ID für Vertreter ausführen.

[<=]

6.2.6.6.4 Berechtigung für Kostenträger löschen

Mit diesem Anwendungsfall kann ein Versicherter bzw. ein berechtigter Vertreter dem Kostenträger die Berechtigung entziehen.

A_17194 - ePA-Frontend des Versicherten: Kostenträger zum Entzug der Berechtigung markieren

Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, berechtigte Kostenträger für den Entzug der Berechtigung auszuwählen.[<=]

Die zum Zugriff auf das Aktenkonto berechtigten KTR werden mit der übergreifende Aktivität "Vergebene Berechtigungen bestimmen" ermittelt.

A_17195 - ePA-Frontend des Versicherten: Berechtigung für Kostenträger löschen

Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "UC 3.6 - Bestehende Berechtigungen durch einen Versicherten verwalten" aus [gemSysL_ePA] für den Kostenträger, deren Berechtigung entzogen werden soll, gemäß TAB_FdV_166 umsetzen.

Tabelle 47: TAB_FdV_166 – Berechtigung für Kostenträger löschen

Name	Berechtigung für Kostenträger löschen
Auslöser	<ul style="list-style-type: none"> • Aufruf der Aktion zum Löschen der Berechtigung in der GUI
Akteur	Versicherter oder berechtigter Vertreter

Vorbedingung	Es besteht eine Aktensession mit gültigen Session-Daten. Der Nutzer hat einen Kostenträger zum Löschen der Berechtigung ausgewählt und das Löschen bestätigt. Das Policy Document und Informationen zum AuthorizationKey des Kostenträgers stehen zur Verfügung.
Nachbedingung	Der Kostenträger ist nicht mehr für den Zugriff auf das Aktenkonto autorisiert.
Standardablauf	Aktivitäten im Standardablauf <ol style="list-style-type: none"> 1. Policy Document in Dokumentenverwaltung löschen 2. Schlüsselmaterial in ePA-Aktensystem löschen

[<=]

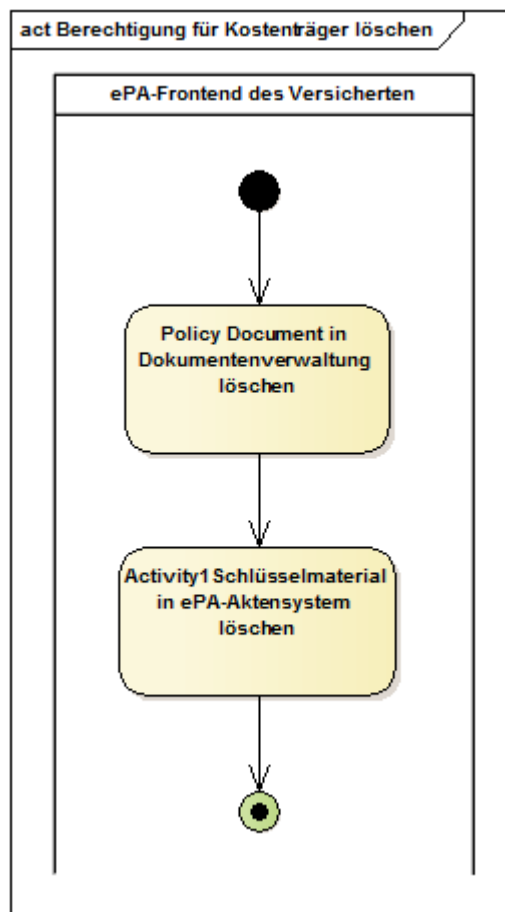


Abbildung 12: Berechtigung für Kostenträger löschen

A_17196 - ePA-Frontend des Versicherten: Berechtigung für Kostenträger löschen - Policy Document in Dokumentenverwaltung löschen

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Berechtigung für Kostenträger löschen" für das Löschen des Policy Document in die Dokumentenverwaltung die übergreifende Aktivität "Dokumentenset in Dokumentenverwaltung löschen" mit einer RemoveDocuments_Message für den über die

XDS-Metadaten ermittelten Dokument Identifier des Policy Documents des Kostenträgers ausführen.[<=]

Die TelematikID des Kostenträgers kann aus dem Policy Document bestimmt werden.

A_17197 - ePA-Frontend des Versicherten: Berechtigung für Kostenträger löschen - Schlüsselmateriale in ePA-Aktensystem löschen

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Berechtigung für Kostenträger löschen" für das Löschen des Schlüsselmateriale die übergreifende Aktivität "Schlüsselmateriale im ePA-Aktensystem löschen" mit dem Eingangsparameter ActorID = TelematikID des Kostenträgers ausführen.

[<=]

6.2.7 Dokumentenverwaltung

6.2.7.1 Dokumente einstellen

Mit diesem Anwendungsfall kann ein Versicherter bzw. ein berechtigter Vertreter Dokumente in die ePA hochladen.

A_15464 - ePA-Frontend des Versicherten: Dokumente einstellen - Zugriffsberechtigungen anzeigen und bestätigen

Das ePA-Frontend des Versicherten MUSS, wenn die Option "Dokumente einstellen: Berechtigte anzeigen" aktiv ist, dem Nutzer vor dem Anwendungsfall "Dokumente einstellen" alle für die Dokumente potentiell zugriffsberechtigten Leistungserbringerinstitutionen anzeigen und eine Bestätigung vom Nutzer einholen.

[<=]

Die für die Dokumente potentiell zugriffsberechtigten LEI werden mittels der übergreifenden Aktivität "Vergebene Berechtigung bestimmen" ermittelt.

Optional können zusätzlich auch die zugriffsberechtigten Vertreter angezeigt werden. Die Abfrage dient der Kontrolle der vergebenen Zugriffsberechtigungen durch den Nutzer.

Zugriffsberechtigt sind alle Vertreter und alle LEI mit der Berechtigung für vom Versicherten eingestellte Dokumente. (siehe auch "A_15381 - ePA-Frontend des Versicherten: Auswahl Berechtigungskonfiguration")

A_15465 - ePA-Frontend des Versicherten: Dokumente einstellen - Hinweis Änderung Zugriffsberechtigungen

Das ePA-Frontend des Versicherten MUSS es ermöglichen, die Anwendungsfälle zum Verwalten von Berechtigungen auszuführen, wenn der Nutzer vor dem Anwendungsfall "Dokumente einstellen" die Zugriffsberechtigungen nicht bestätigt.[<=]

A_15458 - ePA-Frontend des Versicherten: Dokumente einstellen

Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "UC 4.2 - Dokumente durch einen Versicherten einstellen" aus [gemSysL_ePA] gemäß TAB_FdV_146 umsetzen.

Tabelle 48: TAB_FdV_146 – Dokumente einstellen

Name	Dokumente einstellen
Auslöser	<ul style="list-style-type: none"> Aufruf des Anwendungsfalls in der GUI
Akteur	Versicherter bzw. ein berechtigter Vertreter

Vorbedingung	Es besteht eine Aktensession mit gültigen Session-Daten. Die hochzuladenden Dokumente sind im lokal eingebundenen Speicher verfügbar.
Nachbedingung	Die Dokumente sind in der ePA für alle Berechtigten verfügbar.
Standardablauf	Aktivitäten im Standardablauf <ol style="list-style-type: none"> 1. Auswahl der Dokumente aus dem lokalen Dateisystem durch den Nutzer 2. Prüfung auf zulässige Dateigröße 3. Eingabe der Metadaten zu Dokumenten 4. für jedes Dokument <ol style="list-style-type: none"> a. Dokument verschlüsseln b. Dokumentenschlüssel löschen 5. Dokumentenset in Dokumentenverwaltung hochladen

[<=]

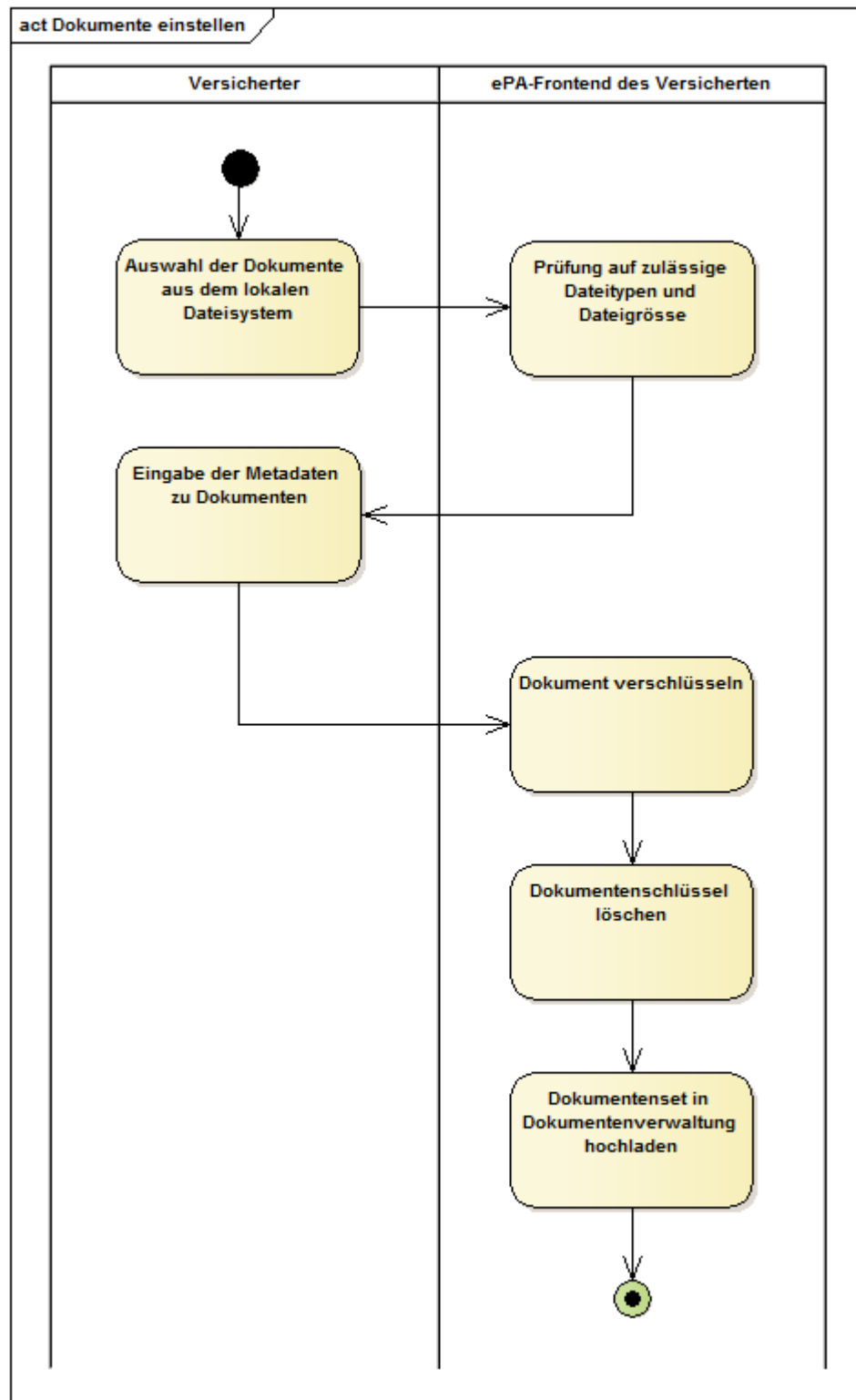


Abbildung 13: Aktivitätsdiagramm "Dokumente einstellen"

Das ePA-Aktensystem unterstützt nur Dokumente mit bestimmten MIME Types. Die initial zulässigen Typen sind in [\[gemSpec_DM_ePA#A_14760\]](#) beschrieben. Die Dokumentenverwaltung prüft jedes Dokument anhand der Metadaten beim Hochladen der Dokumente und antwortet mit einem Fehler, wenn der Dokumententyp nicht unterstützt wird.

A_15461 - ePA-Frontend des Versicherten: Dokumente einstellen - Prüfung**Dateigröße**

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Dokumente einstellen" die Größe jedes durch den Nutzer ausgewählten Dokuments prüfen und ablehnen, wenn es die Größe von 25 MB überschreitet.[<=]

A_15462 - ePA-Frontend des Versicherten: Dokumente einstellen - Eingabe der Metadaten zu Dokumenten

Das ePA-Frontend des Versicherten MUSS dem Nutzer im Anwendungsfall "Dokumente einstellen" ermöglichen, zu jedem ausgewählten Dokument Metadaten einzugeben.[<=]

Für Festlegungen zur Eingabe von Metadaten siehe "5.4.4- Eingabe Metadaten für einzustellende Dokumente".

A_15463 - ePA-Frontend des Versicherten: Dokumente einstellen - Prüfung XDS-Metadaten

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Dokumente einstellen" nach Eingabe der XDS-Metadaten durch den Nutzer, diese auf Vollständigkeit prüfen und bei fehlenden oder fehlerhaften Werten den Nutzer zur Eingabe und Korrektur auffordern.[<=]

Zum Verschlüsseln des Dokuments wird dieses mit einem Dokumentenschlüssel symmetrisch verschlüsselt. Der Dokumentenschlüssel wird dann symmetrisch mit dem Aktenschlüssel verschlüsselt. Für Vorgaben zum Verschlüsseln eines Dokuments für das ePA-Aktensystem siehe [\[gemSpec DM ePA#2.4.1 Verschlüsselung\]](#).

A_15466 - ePA-Frontend des Versicherten: Dokumente einstellen - Dokument verschlüsseln

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Dokumente einstellen" für jedes zu übermittelnde Dokument die Aktivität "Dokument verschlüsseln" gemäß TAB_FdV_147umsetzen.

Tabelle 49: TAB_FdV_147 – Dokumente einstellen - Dokument verschlüsseln

Plattformbaustein PL_TUC_SYMM_ENCIPHER für Dokument nutzen	Dokument mit PL_TUC_SYMM_ENCIPHER verschlüsseln Eingangsdaten: <ul style="list-style-type: none"> • Dokument • Der optionalen Parameter Cert und AD werden nicht verwendet. Rückgabedaten: <ul style="list-style-type: none"> • verschlüsseltes Dokument • Dokumentenschlüssel Der Dokumentenschlüssel wird in der Aktivität erzeugt und an den Aufrufer zurückgegeben
Plattformbaustein PL_TUC_SYMM_ENCIPHER für Dokumentenschlüssel nutzen	Dokumentenschlüssel mit PL_TUC_SYMM_ENCIPHER verschlüsseln Eingangsdaten: <ul style="list-style-type: none"> • Dokument: Dokumentenschlüssel • Aktenschlüssel aus Session-Daten • Der optionale Parameter AD wird nicht verwendet.

	Rückgabedaten: <ul style="list-style-type: none"> • verschlüsselter Dokumentschlüssel
--	------------------------------------------------------------------------------------------------------

[<=]

Die Dokumentenschlüssel dürfen nicht persistent gespeichert werden und müssen nach ihrer Verwendung gelöscht werden.

A_15467 - ePA-Frontend des Versicherten: Dokumente einstellen - Dokumentenschlüssel löschen

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Dokumente einstellen" in der Aktivität "Dokument verschlüsseln" erstellte Dokumentenschlüssel nach dem Ende der Aktivität löschen.[<=]

Auf Basis der verschlüsselten Dokumente und den durch den Nutzer für jedes Dokument eingegebenen Metadaten wird eine Provide And Register Document Set-b Message für die einzustellende Versichertendokumente erstellt.

Für Nutzungsvorgaben siehe Kapitel "[Versichertendokumente](#)".

A_15468 - ePA-Frontend des Versicherten: Dokumente einstellen - Dokumentenset in Dokumentenverwaltung hochladen

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Dokumente einstellen" zum Hochladen des Dokumentenset in die Dokumentenverwaltung die übergreifende Aktivität "Dokumentenset in Dokumentenverwaltung hochladen" mit einer Provide And Register Document Set-b Message für Versichertendokumente ausführen.[<=]

6.2.7.2 Dokumente suchen

Mit diesem Anwendungsfall kann ein Versicherter oder ein berechtigter Vertreter nach Dokumenten oder Dokumentensets im ePA-Aktensystem auf Basis der XDS-Metadaten der Dokumente suchen. Als Ergebnis der Suchanfrage liefert das ePA-Aktensystem eine Liste von XDS-Metadaten zu Dokumenten.

A_15469 - ePA-Frontend des Versicherten: Suchparameter für Dokumente

Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, Suchparameter auf Basis der XDS-Metadaten für eine Suchanfrage einzugeben. Für Suchparameter mit fest vorgegebenem Wertebereich muss der Nutzer eine Auswahlliste nutzen können.[<=]

Folgende Suchanfragen sollen mindestens möglich sein:

- Suche nach allen medizinischen Dokumenten im Aktenkonto
- Suche nach Ersteller bzw. Einstellendem (`XDSDocumentEntry.author`)
- Suche nach in einem Zeitraum erstellten bzw. eingestellten Dokumenten (`XDSDocumentEntry.creationTime` / `XDSSubmissionSet.creationTime`)
- Suche nach Dokumententitel
(siehe [\[gemSpec_Dokumentenverwaltung#A_17185\]](#) und "A_17854 - ePA-Frontend des Versicherten: Nutzung des Anfragetyps "FindDocumentsByTitle" ")
- Suche nach durch LEIs bereitgestellte Dokumente sowie Dokumente mit Kennzeichnung "leistungserbringeräquivalent"(`XDSDocumentEntry.confidentialityCode="LEI" OR "LEÄ"`)

- Suche nach Dokumenten mit Kennzeichnung "Versicherteninformation"(siehe [\[gemSpec_DM_ePA#A_14986\]](#))
- Suche nach durch Krankenkassen bereitgestellte Informationen (`XDSDocumentEntry.confidentialityCode="KTR"`)

A_15470 - ePA-Frontend des Versicherten: Dokumente suchen

Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "UC 4.4 - Dokumente durch einen Versicherten suchen" aus [gemSysL_ePA] gemäß TAB_FdV_148 umsetzen.

Tabelle 50: TAB_FdV_148 – Dokumente suchen

Name	Dokumente suchen
Auslöser	<ul style="list-style-type: none"> • Auswahl der Aktion zur Suche von Dokumenten in der GUI
Akteur	Versicherter bzw. ein berechtigter Vertreter
Vorbedingung	Es besteht eine Aktensession mit gültigen Session-Daten.
Nachbedingung	Falls die Anfrage eine nicht-leere Ergebnismenge liefert, stehen die XDS-Metadaten der Dokumente zur Auflistung für den Nutzer bereit.
Standardablauf	Aktivitäten im Standardablauf <ol style="list-style-type: none"> 1. Suchanfrage ausführen 2. Suchergebnisse als Liste aufbereiten und anzeigen

[<=]

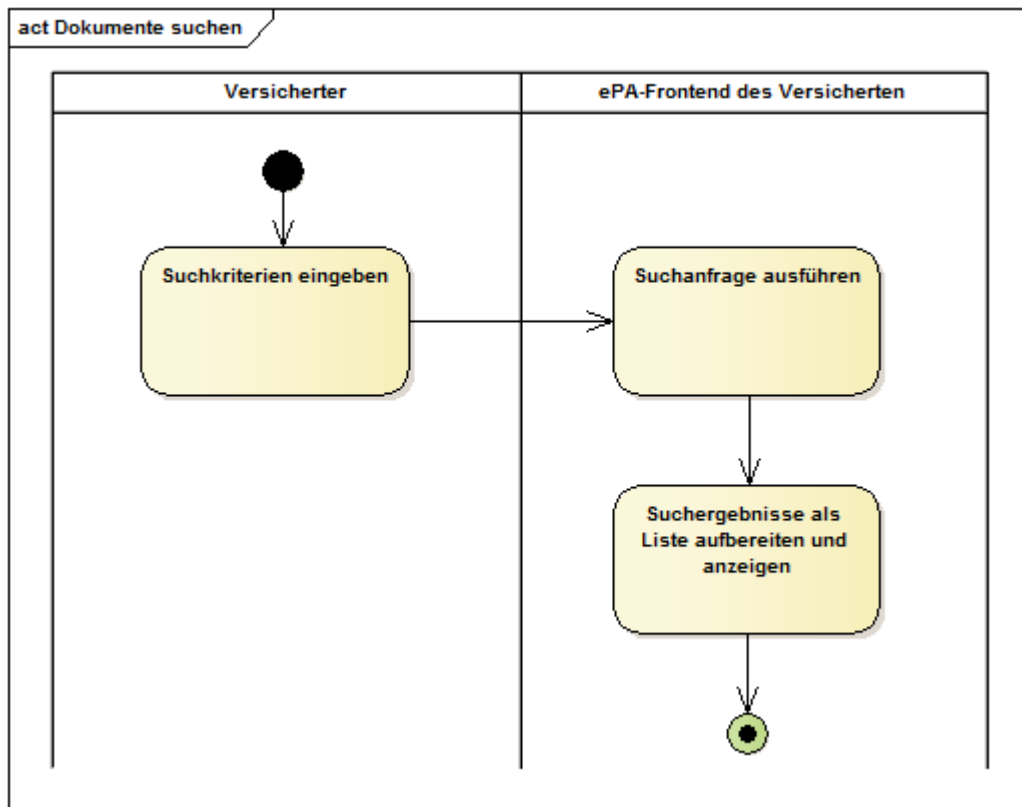


Abbildung 14: Aktivitätsdiagramm "Dokumente suchen"

A_15471 - ePA-Frontend des Versicherten: Dokumente suchen - Suchanfrage ausführen

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Dokumente suchen" zum Ausführen der Suchanfrage die übergreifende Aktivität "Suche nach Dokumenten in Dokumentenverwaltung" mit einer query:AdhocQueryRequest_Message entsprechend der von Nutzer vorgegebenen Suchkriterien ausführen.

[<=]

A_15472 - ePA-Frontend des Versicherten: Ergebnisliste Dokumente anzeigen

Das ePA-Frontend des Versicherten MUSS dem Nutzer das Ergebnis der Suche nach Dokumenten anzeigen.[<=]

Das Ergebnis der Suche soll für den Nutzer sortierbar und filterbar dargestellt werden.

A_15473 - ePA-Frontend des Versicherten: Ergebnisliste Dokumente drucken und speichern

Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, das Ergebnis der Suche nach Dokumenten auszudrucken und lokal zu speichern.[<=]

Das lokale Speichern kann im PDF Format angeboten werden.

A_15474 - ePA-Frontend des Versicherten: Suche verfeinern

Das ePA-Frontend des Versicherten MUSS die Ergebnisse einer Suchanfrage zusammen mit den zur Suche verwendeten Parameter anzeigen und es dem Nutzer ermöglichen, die Suchparameter anzupassen und die Suchanfrage erneut auszuführen.[<=]

6.2.7.3 Dokument herunterladen

Mit diesem Anwendungsfall kann ein Versicherter bzw. ein berechtigter Vertreter Dokumente aus dem Aktenkonto zum Anzeigen oder lokalen Speichern herunterladen.

A_15475 - ePA-Frontend des Versicherten: Dokumente zum Herunterladen markieren

Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, Dokumente aus dem Ergebnis einer Suchanfrage zum Herunterladen (bspw. für die Anzeige oder lokales Speichern) zu markieren.[<=]

A_15476 - ePA-Frontend des Versicherten: Dokumente herunterladen

Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "UC 4.10 - Dokumente durch einen Versicherten anzeigen" aus [gemSysL_ePA] gemäß TAB_FdV_149 umsetzen.

Tabelle 51: TAB_FdV_149 – Dokumente aus Aktenkonto herunterladen

Name	Dokumente herunterladen
Auslöser	<ul style="list-style-type: none"> Auswahl der Aktion zum Herunterladen, Anzeigen oder lokalen Speichern für markierte Dokumente in einer Suchanfrage in der GUI
Akteur	Versicherter bzw. ein berechtigter Vertreter
Vorbedingung	<p>Es besteht eine Aktensession mit gültigen Session-Daten. Es wurde eine Suchanfrage nach Dokumenten in der Dokumentenverwaltung durchgeführt. Die Dokumente sind im Ergebnis einer Suchanfrage selektiert. Die Identifier der Dokumente (uniqueId) sind aus den Metadaten der Suchanfrage bekannt.</p>
Nachbedingung	Die Dokumente liegen unverschlüsselt temporär in einem Speicher im Gerät des Versicherten vor.
Standardablauf	<p>Aktivitäten im Standardablauf</p> <ol style="list-style-type: none"> markierte Dokumente herunterladen und entschlüsseln

[<=]

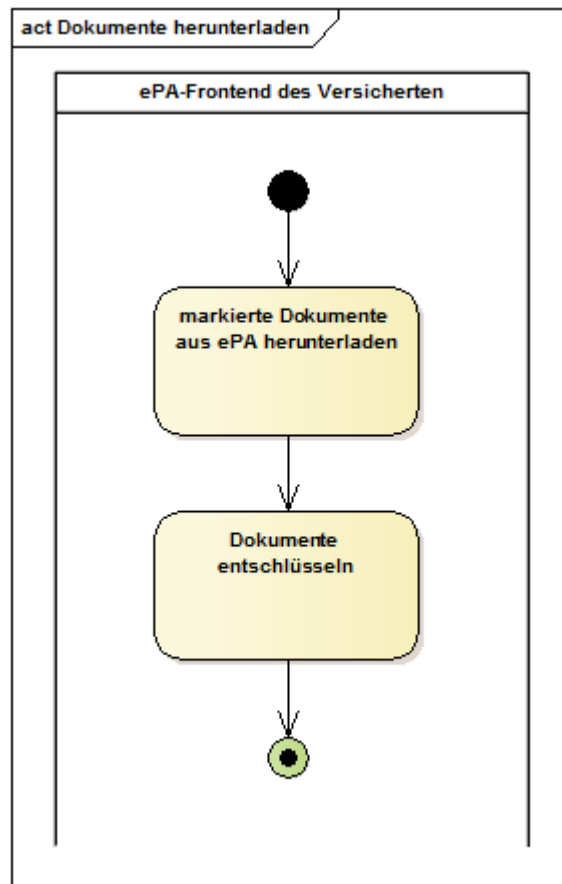


Abbildung 15: Aktivitätsdiagramm "Dokumente herunterladen"

A_15477 - ePA-Frontend des Versicherten: Dokumente herunterladen - Herunterladen und Entschlüsseln

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Dokumente herunterladen" zum Herunterladen und Entschlüsseln der Dokumente die übergreifende Aktivität "Dokumentenset aus Dokumentenverwaltung herunterladen" mit einer RetrieveDocumentSet_Message für alle über die XDS-Metadaten ermittelten Dokument Identifier der ausgewählten Dokumente ausführen.[<=]

A_15478 - ePA-Frontend des Versicherten: Dokument lokal speichern

Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, ein aus dem Aktenkonto heruntergeladenes Dokument im lokalen Speicher persistent abzulegen.[<=]

A_15479 - ePA-Frontend des Versicherten: Dokument mit Standardprogramm anzeigen

Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, wenn für einen gegebenen Dateitypen ein Standardprogramm verfügbar ist, ein aus dem Aktenkonto heruntergeladenes Dokument mit dem Standardprogramm anzuzeigen.[<=]

6.2.7.4 Dokumente im Aktenkonto löschen

Mit diesem Anwendungsfall kann ein Versicherter bzw. ein berechtigter Vertreter Dokumente im Aktenkonto löschen. Die Dokumente sind damit unwiederbringlich aus dem ePA-Aktensystem entfernt.

A_15480 - ePA-Frontend des Versicherten: Dokumente zum Löschen markieren

Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, Dokumente aus dem Ergebnis einer Suchanfrage zum Löschen zu markieren.[<=]

A_15481 - ePA-Frontend des Versicherten: Dokumente löschen

Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "UC 4.8 - Dokumente durch einen Versicherten löschen" aus [gemSysL_ePA] gemäß TAB_FdV_150 umsetzen.

Tabelle 52: TAB_FdV_150 – Dokumente löschen

Name	Dokumente löschen
Auslöser	<ul style="list-style-type: none"> Auswahl der Aktion Löschen für zum Löschen markierte Dokument in einer Suchanfrage in der GUI
Akteur	Versicherter bzw. ein berechtigter Vertreter
Vorbedingung	<p>Es besteht eine Aktensession mit gültigen Session-Daten. Es wurde eine Suchanfrage nach Dokumenten in der Dokumentenverwaltung durchgeführt. Die zu löschenden Dokumente sind im Ergebnis einer Suchanfrage selektiert. Die Identifier für die Dokumente sind aus den Metadaten der Suchanfrage bekannt.</p>
Nachbedingung	Die Dokumente sind im Aktenkonto unwiederbringlich gelöscht.
Standardablauf	<p>Aktivitäten im Standardablauf</p> <ol style="list-style-type: none"> 1. Bestätigung zum Löschen einholen 2. Dokumentenset in Dokumentenverwaltung löschen

[<=]

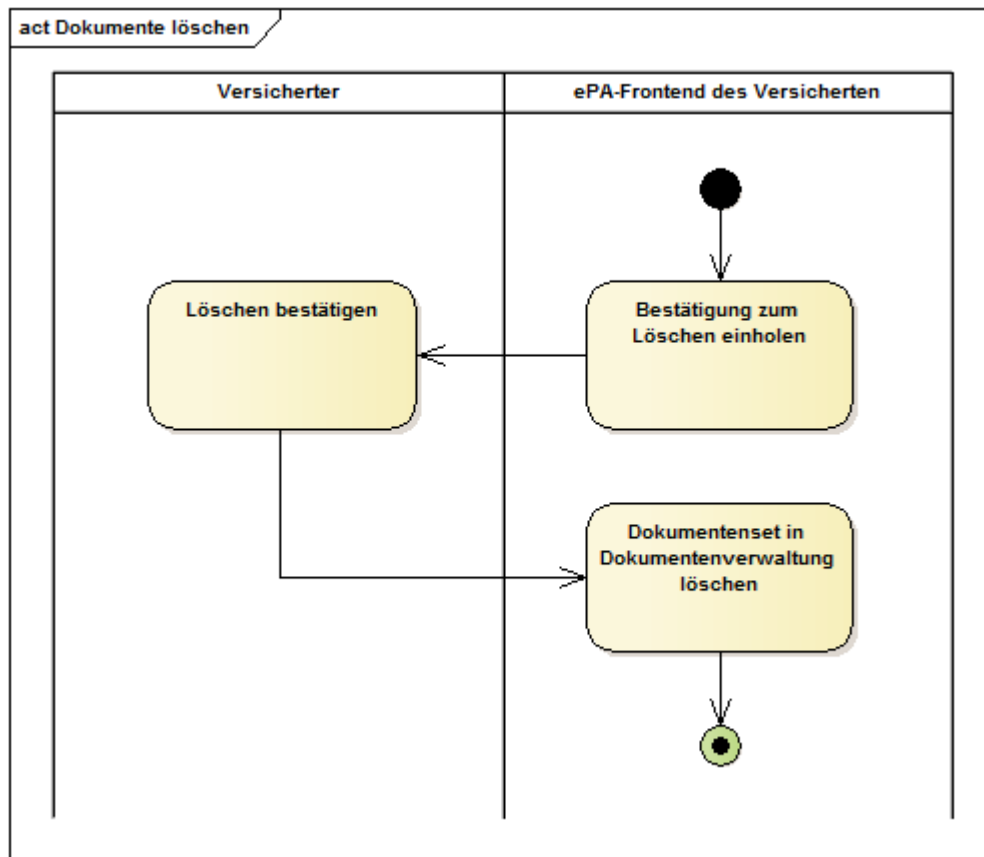


Abbildung 16: Aktivitätsdiagramm "Dokumente löschen"

A_15482 - ePA-Frontend des Versicherten: Dokumente löschen - Bestätigung

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Dokumente löschen" vom Nutzer eine Bestätigung einholen, dass die markierten Dokumente gelöscht werden sollen und die Möglichkeit geben, das Löschen abubrechen. [≤]

A_15483 - ePA-Frontend des Versicherten: Dokumente löschen - Löschrequest Dokumentenverwaltung

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Dokumente löschen" zum Löschen der Dokumente die übergreifende Aktivität "Dokumentenset in Dokumentenverwaltung löschen" mit einer RemoveDocuments_Message für alle über die XDS-Metadaten ermittelten Dokument Identifier der ausgewählten Dokumente ausführen. [≤]

6.2.8 Protokollverwaltung**6.2.8.1 Zugriffsprotokoll einsehen**

Bei der Nutzung eines Aktenkontos durch LEI, durch berechnigte Vertreter oder den Aktenkontoinhaber werden Aktivitäten protokolliert, damit der Aktenkontoinhaber oder ein berechtigter Vertreter diese Aktivitäten nachvollziehen kann. Dazu zählen Zugriffe auf die Dokumente und seine Metadaten (§ 291a-konformes Zugriffsprotokoll) sowie auch Aktivitäten mit administrativem Charakter (Verwaltungsprotokoll).

Die verschiedenen Aktivitäten sind in [\[gemSpec_DM_ePA#A_14505 - Event Codes für Protokollereignisse\]](#) gelistet. Aktivitäten des § 291a-konformen Zugriffsprotokolls sind:

- PHR-510 (Hinzufügen eines Dokuments aus der ärztlichen Umgebung)
- PHR-520 (Suchanfrage aus der ärztlichen Umgebung)
- PHR-530 (Löschen eines Dokuments aus der ärztlichen Umgebung)
- PHR-540 (Abruf eines Dokuments aus der ärztlichen Umgebung)
- PHR-610 (Hinzufügen eines Dokuments aus der privaten Umgebung)
- PHR-620 (Suchanfrage aus der privaten Umgebung)
- PHR-630 (Löschen eines Dokuments aus der privaten Umgebung)
- PHR-640 (Abruf eines Dokuments aus der privaten Umgebung)
- PHR-710 (Hinzufügen eines Dokuments aus der Kostenträger-Umgebung)

Alle anderen Aktivitäten sind dem Verwaltungsprotokoll zugeordnet.

Die Protokolldaten des § 291a-konformen Zugriffsprotokolls werden im Aktenkonto abgelegt. Die Protokolldaten des Verwaltungsprotokolls werden in verschiedenen Komponenten des ePA-Aktensystems vorgehalten. Die Daten müssen für eine Anzeige separat abgefragt werden.

Mit diesem Anwendungsfall kann ein Versicherter bzw. ein berechtigter Vertreter die Protokolldaten über die Zugriffe auf das Aktenkonto des Versicherten einsehen.

A_15484 - ePA-Frontend des Versicherten: Protokoll einsehen - Hilfetext

Das ePA-Frontend des Versicherten MUSS dem Nutzer ermöglichen, den folgenden Text zur Erläuterung des Anwendungsfalls anzuzeigen.

"Sie können die Protokolldaten aller Zugriffe auf Ihr Aktenkonto einsehen. Dies umfasst

- Suche nach Dokumenten
- Einstellen, Herunterladen und Löschen von Dokumenten
- Vergabe, Ändern und Löschen von Berechtigungen
- Login

Die Protokolleinträge werden am Ende des auf ihre Generierung folgenden Jahres gelöscht. Ausnahme: Die 50 jüngsten Protokolleinträge werden auch dann nicht gelöscht, wenn die o.g. Frist erreicht bzw. überschritten ist."[<=]

A_15485 - ePA-Frontend des Versicherten: Protokolldaten einsehen

Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "UC 6.1 - Protokolldaten durch einen Versicherten einsehen" aus [gemSysL_ePA] gemäß TAB_FdV_151 umsetzen.

Tabelle 53: TAB_FdV_151 – Protokolldaten einsehen

Name	Protokolldaten einsehen
Auslöser	<ul style="list-style-type: none"> • Auswahl der Aktion zum Anzeigen der Protokolldaten in der GUI
Akteur	Versicherter bzw. ein berechtigter Vertreter
Vorbedingung	Es besteht eine Aktensession mit gültigen Session-Daten.
Nachbedingung	Die Protokolldaten werden dem Nutzer angezeigt.

Standardablauf	Aktivitäten im Standardablauf <ol style="list-style-type: none"> 1. Protokolldaten Dokumentenverwaltung abfragen 2. Protokolldaten Autorisierung abfragen 3. Protokolldaten Authentisierung abfragen 4. Daten aufbereiten und anzeigen
----------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

[<=]

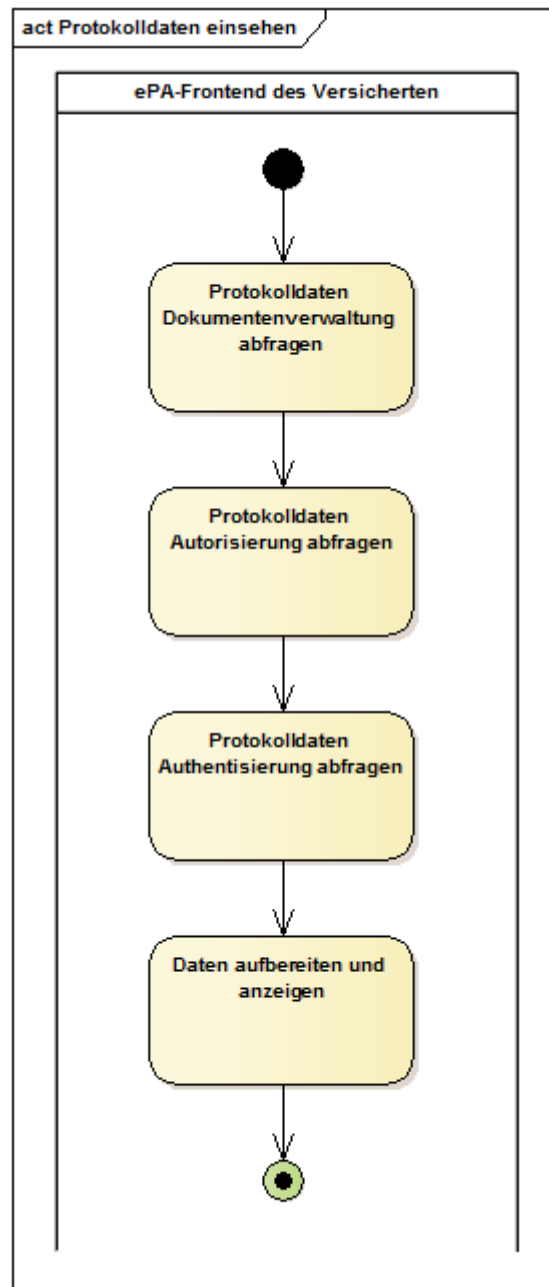


Abbildung 17: Aktivitätsdiagramm "Protokolldaten einsehen"

A_15486 - ePA-Frontend des Versicherten: Protokoll einsehen - Dokumentenverwaltung abfragen

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Protokolldaten einsehen" die Aktivität "Protokolldaten Dokumentenverwaltung abfragen" gemäß TAB_FdV_152 umsetzen.

Tabelle 54: TAB_FdV_152 – Protokolldaten einsehen - Dokumentenverwaltung abfragen

I_Account_Management_Insurant::GetAuditEvents Request erstellen	Eingangsdaten: <ul style="list-style-type: none"> • AuthenticationAssertion aus Session-Daten
I_Account_Management_Insurant::GetAuditEvents Response verarbeiten	Rückgabedaten: <ul style="list-style-type: none"> • Audit Event List

[<=]

A_15487 - ePA-Frontend des Versicherten: Protokoll einsehen - Autorisierung abfragen

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Protokolldaten einsehen" die Aktivität "Protokolldaten Autorisierung abfragen" gemäß TAB_FdV_153 umsetzen.

Tabelle 55: TAB_FdV_153 – Protokolldaten einsehen - Autorisierung abfragen

I_Authorization_Management_Insurant::getAuditEvents Request erstellen	Eingangsdaten: <ul style="list-style-type: none"> • AuthenticationAssertion aus Session-Daten • RecordIdentifier aus Session-Daten • DeviceID aus Gerät-Daten
I_Authorization_Management_Insurant::getAuditEvents Response verarbeiten	Rückgabedaten: <ul style="list-style-type: none"> • AuditMessage[0..*]

[<=]

A_15488 - ePA-Frontend des Versicherten: Protokoll einsehen - Authentisierung abfragen

Das ePA-Frontend des Versicherten MUSS im Anwendungsfall "Protokolldaten einsehen" die Aktivität "Protokolldaten Authentisierung abfragen" gemäß TAB_FdV_154 umsetzen.

Tabelle 56: TAB_FdV_154 – Protokolldaten einsehen - Zugangsgateway des Versicherten abfragen

I_Authentication_Insurant::getAuditEvents Request erstellen	Eingangsdaten: <ul style="list-style-type: none"> • AuthenticationAssertion aus Session-Daten
I_Authentication_Insurant::getAuditEvents Response verarbeiten	Rückgabedaten: <ul style="list-style-type: none"> • AuditMessage[0..*]

Varianten/Alternativen	Wenn in der Abarbeitung der Operation ein Fehler auftritt und kein Resultset vorliegt, kann der Anwendungsfall fortgesetzt werden, denn dieses Resultset ist nicht Teil der Standard-Anzeige. Der Nutzer ist darauf hinzuweisen, dass keine Protokolleinträge zur Authentisierung abgerufen werden konnten.
------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

[<=]

Die Ergebnisse der Abfragen an die Komponenten des ePA-Aktensystems werden vereint.

Die Information eines Protokolleintrages sind in [\[gemSpec_DM_ePA#A_14471 - Objektstruktur Eintrag für Protokoll\]](#) beschrieben.

Tabelle 57: TAB_FdV_155 – Felder im Protokolleintrag

Protokolldatum	Bezeichnung in GUI	Hinweis zur Anzeige	optional in Standard-Anzeige
Aufgerufene Operation	Art des Zugriffs auf das Aktenkonto	DisplayName anzeigen	
Datum und Uhrzeit des Zugriffs	Zeitpunkt des Zugriffs		
Ergebnis der aufgerufenen Operation	Ergebnis Zugriff	0 - erfolgreich 1 - nicht erfolgreich	
UserID	Identifizier des Nutzers		x
UserName	Name des Nutzers		
ObjectID	Identifizier des Objektes, auf das zugegriffen wurde		x
ObjectName	Bezeichner des Objektes, auf das zugegriffen wurde		
DeviceID	Geräteerkennung		x
Home-CommunityID des ePA-Aktensystems	ID des Aktenanbieters		x

Name des Aktenanbieters	Name des Aktenanbieters		x
-------------------------	-------------------------	--	---

A_15489 - ePA-Frontend des Versicherten: Standard-Anzeige für Protokolldaten

Das ePA-Frontend des Versicherten MUSS eine Standard-Anzeige für die Protokolldaten umsetzen, in der die Protokolleinträge für folgende Zugriffe übersichtlich dargestellt werden:

- Alle Anwendungsfälle des § 291a-konformen Zugriffsprotokolls der Dokumentenverwaltung
 - PHR-510 (Hinzufügen eines Dokuments aus der ärztlichen Umgebung)
 - PHR-520 (Suchanfrage aus der ärztlichen Umgebung)
 - PHR-530 (Löschen eines Dokuments aus der ärztlichen Umgebung)
 - PHR-540 (Abruf eines Dokuments aus der ärztlichen Umgebung)
 - PHR-610 (Hinzufügen eines Dokuments aus der privaten Umgebung)
 - PHR-620 (Suchanfrage aus der privaten Umgebung)
 - PHR-630 (Löschen eines Dokumentes aus der privaten Umgebung)
 - PHR-640 (Abruf eines Dokuments aus der privaten Umgebung)
 - PHR-710 (Hinzufügen eines Dokuments aus der Kostenträger-Umgebung)
- Folgende Anwendungsfälle aus dem Verwaltungsprotokoll der Autorisierung
 - PHR-310 (Hinzufügen des Empfängerschlüssels aus der ärztlichen Umgebung)
 - PHR-320 (Ersetzen des Empfängerschlüssels aus der ärztlichen Umgebung)
 - PHR-410 (Hinzufügen des Empfängerschlüssels aus der privaten Umgebung)
 - PHR-420 (Löschen des Empfängerschlüssels aus der privaten Umgebung)
 - PHR-430 (Ersetzen des Empfängerschlüssels aus der privaten Umgebung)

[<=]

A_15490 - ePA-Frontend des Versicherten: Erweiterte-Anzeige für Protokolldaten

Das ePA-Frontend des Versicherten MUSS eine Erweiterte-Anzeige für die Protokolldaten umsetzen, in der alle Protokolleinträge der vom ePA-Aktensystem erstellten Protokolle (§ 291a-konformes Zugriffsprotokoll und Verwaltungsprotokolle der Komponenten) übersichtlich dargestellt werden.[<=]

Das FdV kann in der Standard-Anzeige die gemäß TAB_FdV_155 optionalen Felder verbergen. Der Nutzer muss dann die Möglichkeit haben, sich die verborgenen Felder anzeigen zu lassen.

A_15491 - ePA-Frontend des Versicherten: Felder Protokolldaten

Das ePA-Frontend des Versicherten MUSS es dem Nutzer in der Standard-Anzeige und in der Erweiterte-Anzeige für die Protokolldaten ermöglichen alle Felder aus TAB_FdV_155 darzustellen.[<=]

Das ePA-Frontend des Versicherten soll in der Standard-Anzeige und in der Erweiterte-Anzeige für die Protokolldaten die Bezeichnung der Felder sinngemäß zu TAB_FdV_155 verwenden.

Das FdV kann es dem Nutzer über einen Link in der Anzeige ermöglichen, das referenzierte Dokument direkt herunterzuladen.

Die Protokolldaten sollen für den Nutzer sortierbar und filterbar dargestellt werden. Der Nutzer soll die Protokolldaten durchsuchen können.

A_15494 - ePA-Frontend des Versicherten: Ergebnisliste Protokolldaten drucken

Das ePA-Frontend des Versicherten MUSS es dem Nutzer für die Standard- und Erweiterte-Anzeige der Protokolle ermöglichen die Einträge auszudrucken.[<=]

A_15495 - ePA-Frontend des Versicherten: Protokolldaten lokal speichern

Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, die Protokolldaten lokal im Format AuditEventList aus der getAuditEvents Response abzuspeichern.[<=]

A_15496 - ePA-Frontend des Versicherten: lokal gespeicherte Protokolldaten anzeigen

Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, die lokal abgespeicherten Protokolldaten einzulesen und in der Standard- und Erweiterte-Anzeige anzuzeigen.[<=]

6.2.9 Verwaltung eGK**6.2.9.1 PIN der eGK ändern**

Mit diesem Anwendungsfall kann der Nutzer das Geheimnis der PIN einer eGK ändern.

A_15497 - ePA-Frontend des Versicherten: PIN der eGK ändern

Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "PIN der eGK ändern" gemäß TAB_FdV_156 umsetzen.

Tabelle 58: TAB_FdV_156 – PIN der eGK ändern

Name	PIN der eGK ändern
Auslöser	<ul style="list-style-type: none"> Auswahl des Anwendungsfalls in der GUI
Akteur	Versicherter oder berechtigter Vertreter
Vorbedingung	Die eGK des Nutzers ist im Kartenleser gesteckt.
Nachbedingung	PIN wurde geändert
Standardablauf	<p>Die Umsetzung ist in TAB_FdV_157 beschrieben</p> <ol style="list-style-type: none"> 1. PL_TUC_CARD_CHANGE_PIN nutzen 2. PL_TUC_CARD_CHANGE_PIN Ergebnis verarbeiten 3. Ergebnis anzeigen

Tabelle 59: TAB_FdV_157 – Ablaufaktivitäten – PIN der eGK ändern

1. PL_TUC_CARD_CHANGE_PIN nutzen	
Plattformoperation	PL_TUC_CARD_CHANGE_PIN
<i>Eingangsdaten</i>	

Identifikator	MRPIN.home
Benutzerhinweis am Kartenterminaldisplay (Sicherheitsklasse 3) bzw. im FdV-Benutzerinterface bei Aufruf der Umgebungsoperation ENV_TUC_SECRET_INPUT	Alte PIN: "Eingabe alte PIN: " bzw. Neue PIN: "Eingabe neue PIN: "
<i>Beschreibung</i>	Der Plattformbaustein wird zur Änderung den PIN genutzt.
2. Rückgabewert von PL_TUC_CARD_CHANGE_PIN verarbeiten	
<i>Rückgabedaten</i>	
OK	PIN erfolgreich geändert
Fehlerfälle	Siehe Beschreibung PL_TUC_CARD_CHANGE_PIN
<i>Beschreibung</i>	<p>Das Ändern einer PIN auf der eGK basiert auf der parametrisierten Plattformbaustein PL_TUC_CARD_CHANGE_PIN. Diese liefert ein <u>Ergebnis</u> zurück. Zur Änderung muss zwingend die Eingabe der alten PIN erfolgen.</p> <p>Wird durch den Versicherten ein falsches altes PIN-Geheimnis eingegeben, wird die verbleibende Anzahl der Eingabeversuche bis zur Sperrung des PINs zurückgemeldet. Im Fehlerfall wird eine Fehlermeldung entsprechenden Details zurückgegeben.</p>
3. Ergebnis anzeigen	
<i>Hinweis an den Versicherten</i>	<p>Die Rückgabedaten des Plattformbausteins enthalten Informationen über den Erfolg der Operation auf der eGK des Versicherten. Im Fehlerfall wird der Versicherte in verständlicher Form über den Fehler informiert. Im Erfolgsfall ist dem Versicherten eine Bestätigung zur Anzeige zu bringen.</p> <p>Falls eine Warnung aufgetreten ist, wird diese dem Versicherten in verständlicher Form angezeigt.</p> <p>Bei einer Fehleingabe der PIN des Versicherten wird dem Versicherten die verbleibende Anzahl der Eingabeversuche bis zur Sperrung der PIN zurückgemeldet.</p>

[<=]

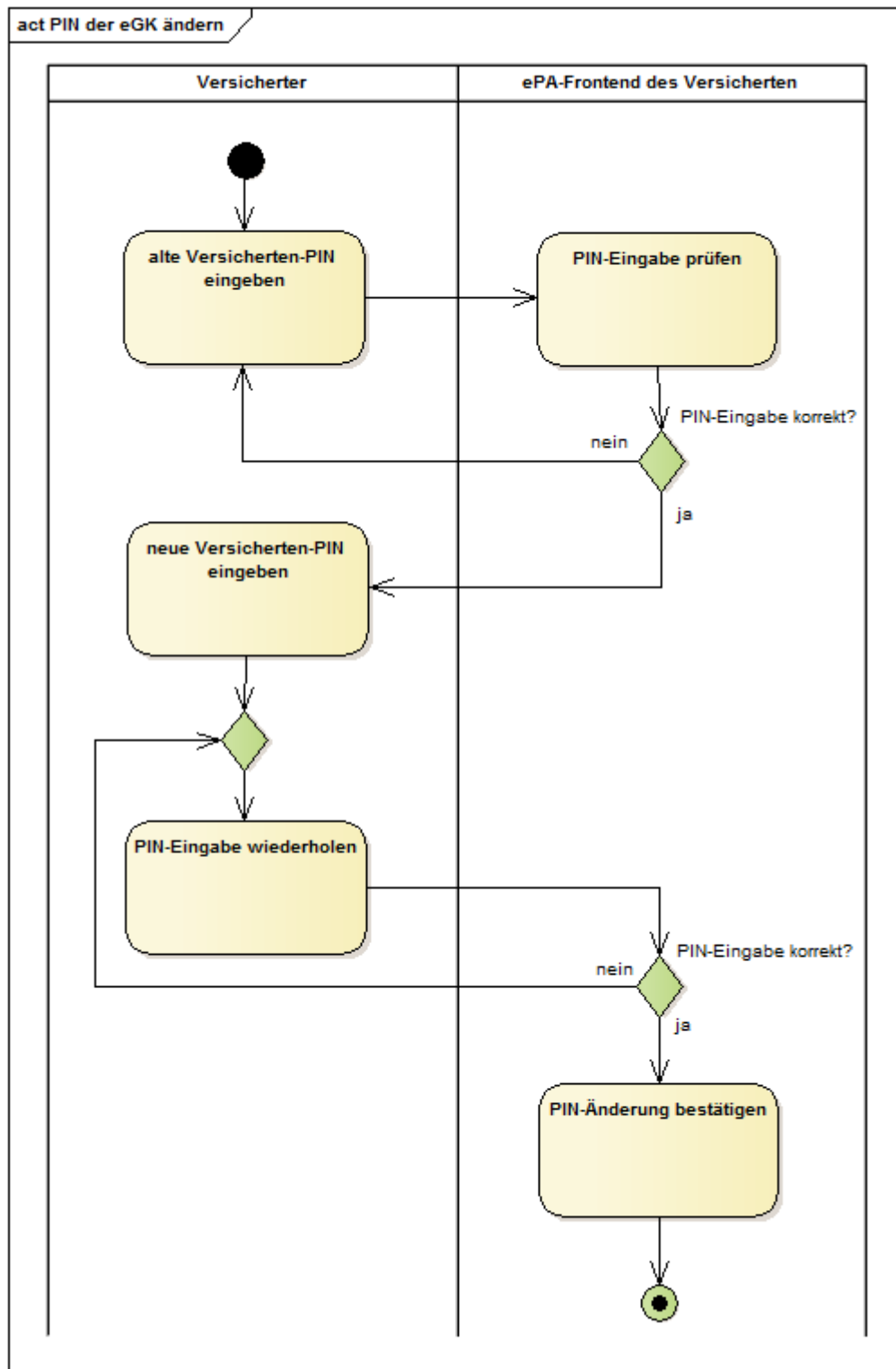


Abbildung 18: Aktivitätsdiagramm "PIN der eGK ändern"

6.2.9.2 PIN der eGK entsperren

Mit diesem Anwendungsfall kann der Nutzer den gesperrten PIN einer eGK mit der PUK entsperren.

A_15498 - ePA-Frontend des Versicherten: PIN der eGK entsperren

Das ePA-Frontend des Versicherten MUSS den Anwendungsfall "PIN der eGK entsperren" gemäß TAB_FdV_158 umsetzen.

Tabelle 60: TAB_FdV_158 – PIN der eGK entsperren

Name	PIN der eGK entsperren
Auslöser	<ul style="list-style-type: none"> Auswahl des Anwendungsfalls in der GUI
Akteur	Versicherter oder berechtigter Vertreter
Vorbedingung	Die eGK des Nutzers ist im Kartenleser gesteckt. Die PIN der eGK (MRPIN.home) ist gesperrt.
Nachbedingung	PIN des Versicherten wurde entsperrt.
Standardablauf	Die Umsetzung ist in TAB_FdV_159 beschrieben <ol style="list-style-type: none"> 1. PL_TUC_CARD_UNBLOCK_PIN nutzen 2. PL_TUC_CARD_UNBLOCK_PIN Ergebnis verarbeiten 3. Ergebnis anzeigen

Tabelle 61: TAB_FdV_159 – Ablaufaktivitäten – PIN der eGK entsperren

1. PL_TUC_CARD_UNBLOCK_PIN aufrufen	
Plattformbaustein	PL_TUC_CARD_UNBLOCK_PIN
<i>Eingangsdaten</i>	
Identifikator	MRPIN.home
Benutzerhinweis am Kartenterminaldisplay (Sicherheitsklasse 3) bzw. im FdV-Benutzerinterface bei Aufruf der Umgebungsoperation ENV_TUC_SECRET_INPUT	PUK: "Eingabe PUK: " bzw. Neue PIN: "Eingabe neue PIN: "
Beschreibung	Für das Entsperren der PIN wird ein Plattformbaustein genutzt.
2. PL_TUC_CARD_UNBLOCK_PIN Ergebnis verarbeiten	

<i>Rückgabedaten</i>	
OK	PIN wurde entsperrt.
PasswordBlocked	Die PUK wurde wegen zu häufiger Nutzung gesperrt. Der Versicherte muss darüber in verständlicher Form informiert und auf die Notwendigkeit einer neuen eGK hingewiesen werden.
Weitere Fehlerfälle	Siehe Beschreibung PL_TUC_CARD_UNBLOCK_PIN
<i>Beschreibung</i>	<p>Das Entsperren einer PIN auf der eGK basiert auf dem parametrisierten Plattformbaustein PL_TUC_CARD_UNBLOCK_PIN. Zum Entsperren muss zwingend die Eingabe einer PUK erfolgen.</p> <p>Wird durch den Versicherten ein falsches PUK-Geheimnis eingegeben, wird die verbleibende Anzahl der Eingabeversuche bis zur Sperrung des PUKs zurückgemeldet. Im Fehlerfall wird eine Fehlermeldung mit entsprechenden Details zurückgegeben.</p>
3. Ergebnis anzeigen	
<i>Hinweis an den Versicherten</i>	<p>Die Rückgabedaten des Plattformbausteins enthalten Informationen über den Erfolg der Operation auf der eGK des Versicherten. Im Fehlerfall wird der Versicherte in verständlicher Form über den Fehler informiert. Im Erfolgsfall ist dem Versicherten eine Bestätigung zur Anzeige zu bringen.</p> <p>Falls eine Warnung aufgetreten ist, wird diese dem Versicherten in verständlicher Form angezeigt.</p>

[<=]

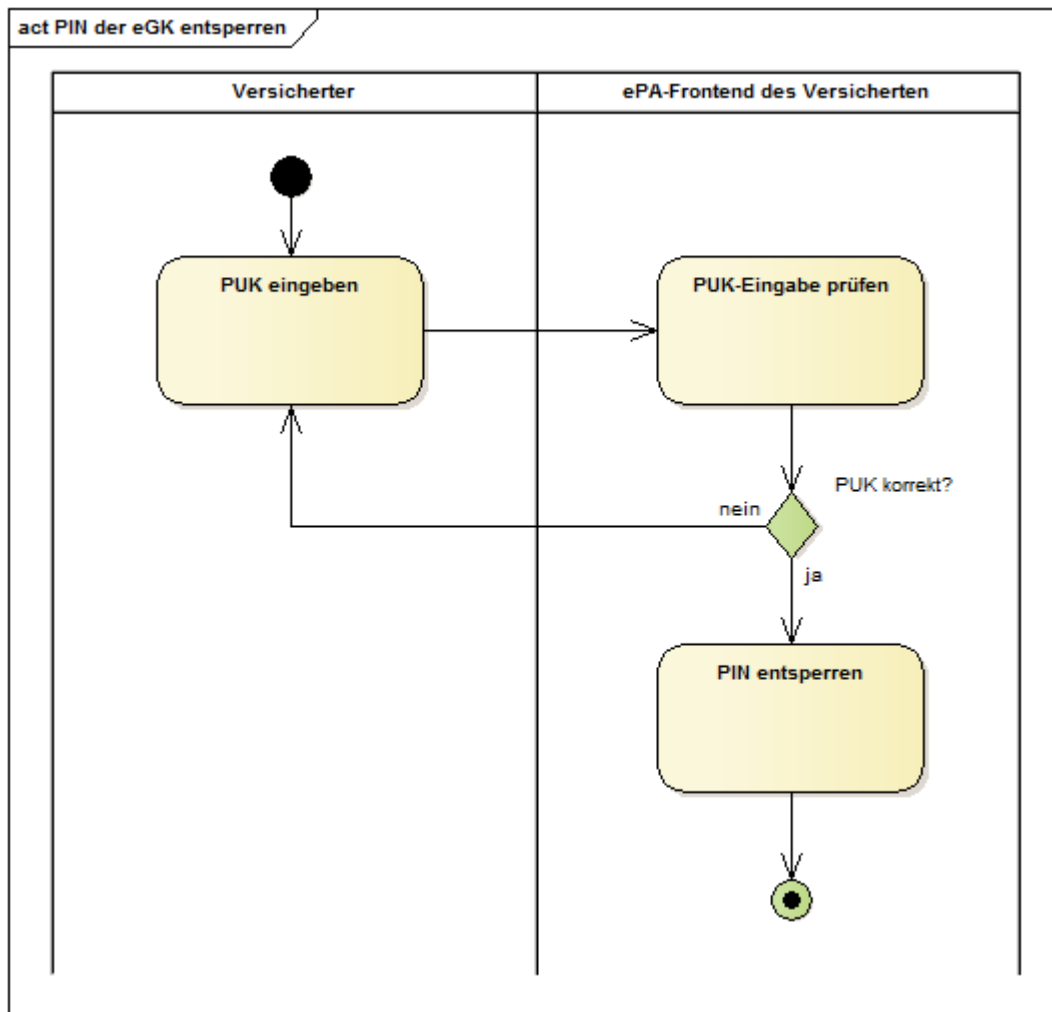


Abbildung 19: Aktivitätsdiagramm "PIN der eGK entsperren"

6.2.10 Geräteverwaltung

6.2.10.1 Benachrichtigungsadresse für Geräteautorisierung aktualisieren

Um ein Gerät mit dem FdV für den Zugriff auf ein Aktenkonto zu autorisieren, muss der Nutzer dieses über einen separaten Benachrichtigungskanal (E-Mail mit Freischalt-Link) bestätigen. Die E-Mail wird an die im Aktenkonto hinterlegte Benachrichtigungsadresse des Nutzers gesendet.

Für den Aktenkontoinhaber wird die Benachrichtigungsadresse initial im Rahmen der Kontoeröffnung hinterlegt. Für Vertreter erfolgt die initiale Hinterlegung der Benachrichtigungsadresse während der Vergabe der Zugriffsberechtigung.

Der Anwendungsfall "Benachrichtigungsadresse für Geräteautorisierung aktualisieren" gibt dem Nutzer die Möglichkeit eine neue Benachrichtigungsadresse im Aktenkonto zu hinterlegen.

A_15499 - ePA-Frontend des Versicherten: Benachrichtigungsadresse erfassen

Das ePA-Frontend des Versicherten MUSS es dem Nutzer ermöglichen, eine Benachrichtigungsadresse für die Geräteautorisierung einzugeben.[<=]

A_15500 - ePA-Frontend des Versicherten: Benachrichtigungsadresse aktualisieren

Das ePA-Frontend des Versicherten MUSS das Hinterlegen der Benachrichtigungsadresse im ePA-Aktensystem gemäß TAB_FdV_160 umsetzen.

Tabelle 62: TAB_FdV_160 – Benachrichtigungsadresse aktualisieren

I_Authorization_Management_Insurant:: putNotificationInfo Request erstellen	Eingangsparameter: <ul style="list-style-type: none"> • AuthenticationAssertion aus Session-Daten • RecordIdentifier aus Session-Daten • DeviceID aus Gerät-Daten • NewNotificationInfo = vom Nutzer eingegebene Benachrichtigungsadresse
I_Authorization_Management_Insurant:: putNotificationInfo Response verarbeiten	Http OK ohne SOAP-Response oder gematik Fehlermeldung

[<=]

6.3 Realisierung der Leistungen der TI-Plattform

Der Produkttyp FdV realisiert die von den Fachanwendungen benötigten Leistungen der TI-Plattform, die in den fachlichen Anwendungsfällen der ePA genutzt werden. Die durch die TI-Plattform bereitgestellten Leistungen umfassen einen für die Fachanwendungen einheitlichen Zugriff auf die eGK des Versicherten, Leistungen der PKI der Telematikinfrastruktur, kryptographische Operationen, etc. die in übergreifenden Spezifikationen der gematik festgelegt sind. Die Definition der Leistungen der TI-Plattform im FdV finden sich in [gemSpec_Systemprozesse_dezTI].

Das FdV verwendet u.a. die in der Tabelle TAB_FdV_177 dargestellten Plattformleistungen.

Tabelle 63 : TAB_FdV_177 – Verwendete Plattformleistungen

Kürzel	Bezeichnung
PL_TUC_CARD_CHANGE_PIN	PIN ändern
PL_TUC_CARD_INFORMATION	Gesammelte Statusinformationen zu einer Karte
PL_TUC_CARD_UNBLOCK_PIN	PIN mit PUK entsperren
PL_TUC_CARD_VERIFY_PIN	Benutzer verifizieren
PL_TUC_GET_CHALLENGE	Auslesen einer Zufallszahl
PL_TUC_SIGN_HASH_nonQES	mit Karten-Identität signieren

PL_TUC_SYMM_DECIPHER	Symmetrisch entschlüsseln
PL_TUC_SYMM_ENCIPHER	Symmetrisch verschlüsseln

In den folgenden Abschnitten wird festgelegt, wie umgebungsspezifische Operationen an der Schnittstelle zu den Leistungen der TI-Plattform umgesetzt werden sollen.

6.3.1 Transportschnittstelle für Kartenkommandos

Der hier beschriebene Produkttyp FdV ist als reines Softwareprodukt konzipiert. Als solches muss das FdV eine Schnittstelle zur eGK über ein Kartenterminal herstellen. Diese Schnittstelle muss die von den Plattformprozessen erzeugten, kartenverständlichen APDUs an die Karte übertragen und wird im Folgenden als ENV_TUC_CARD_APDU_TRANSPORT bezeichnet. Neben proprietären Schnittstellentreibern von Kartenterminalherstellern existieren eine Reihe standardisierter Schnittstellen, die auch von verschiedenen Betriebssystemen zur Anbindung handelsüblicher Kartenterminals unterstützt werden.

A_15501 - ePA-Frontend des Versicherten: Transportschnittstelle für Kartenkommandos

Das ePA-Frontend des Versicherten SOLL eine Transportschnittstelle für die Übertragung von SmartCard-APDUs gegen die Standards CT-API und PCSC implementieren.[<=]

Von der Anforderung A_15501 darf abgewichen werden, wenn die Umsetzung technisch nicht möglich ist (bspw. durch die fehlende Unterstützung der NFC-Schnittstelle bei Herstellern mobiler Endgeräte).

Das ePA-Frontend des Versicherten kann ergänzend eine Transportschnittstelle für die Übertragung von SmartCard-APDUs auf Basis des SICCT-Protokolls, gegen den Standard CCID oder gegen proprietäre Hardwaretreiber eines Kartenterminalherstellers implementieren.

A_15502 - ePA-Frontend des Versicherten: Handbuch: Liste unterstützter Kartenterminals

Der Hersteller des ePA-Frontend des Versicherten MUSS im Handbuch ausweisen, welche Standards und Schnittstellen zu Kartenterminals sein Produkt unterstützt und MUSS eine Liste mit handelsüblichen Kartenterminals angeben, die mit seinem Produkt funktionieren.[<=]

Es sollen Kartenterminalvarianten der Sicherheitsklassen 1 (reine Kontaktiereinheit) zum Einsatz kommen. Zusätzlich können auch Kartenterminalvarianten der Sicherheitsklassen 2 (Kartenterminal mit eigenem PIN-Pad) oder 3 (PIN-Pad plus Display) unterstützt werden. Zusätzlich ist die Ausstattung des eingesetzten Kartenterminals (Klasse 1, 2 oder 3) mit einer NFC-Schnittstelle möglich. Das FdV muss die von den Varianten gebotenen Features geeignet nutzen.

A_15503 - ePA-Frontend des Versicherten: PIN-Eingabe nicht speichern

Das ePA-Frontend des Versicherten DARF ein eingegebenes PIN-Geheimnis NICHT temporär und NICHT persistent speichern.[<=]

A_15504 - ePA-Frontend des Versicherten: PIN-Geheimnis ausschließlich an Karte übermitteln

Das ePA-Frontend des Versicherten MUSS sicherstellen, dass das eingegebene PIN-Geheimnis ausschließlich an die Karte und nicht an andere Adressaten übermittelt wird.[<=]

Das temporäre Speichern bezieht sich bei der Verwendung eines Kartenterminals der Sicherheitsklasse 1 auf das Verwenden der PIN über den Anwendungsfall hinaus, für den die PIN-Eingabe erfolgt ist, z.B. Caching während einer Sitzung. Gelangt das FdV bei der Verwendung eines Kartenterminals der Sicherheitsklassen 2 und 3 ggfs. durch Fehlkonfiguration in Kenntnis der PIN, darf es diese ebenfalls weder temporär noch persistent speichern.

6.3.1.1 Kartenterminals der Sicherheitsklasse 1

Kartenterminals der Sicherheitsklasse 1 verfügen über keine Sicherheitsmerkmale, sie sind eine reine Kontaktiereinheit einer SmartCard. Sämtliche Geheimnis-Eingaben und Hinweistext-Ausgaben müssen über das FdV mittels Bildschirm und Tastatur/Maus erfolgen.

A_15505 - ePA-Frontend des Versicherten: Kartenterminal der Sicherheitsklasse 1: PIN-Eingabe

Das ePA-Frontend des Versicherten MUSS, wenn ein Kartenterminal der Sicherheitsklasse 1 verwendet wird, die PIN-/PUK-Eingabe über ein angeschlossenes Eingabegerät entgegennehmen und in ein an die Karte adressiertes Kommando einbetten.[<=]

A_15506 - ePA-Frontend des Versicherten: Kartenterminal der Sicherheitsklasse 1: PIN-Eingabe Geheimnis

Das ePA-Frontend des Versicherten DARF, wenn ein Kartenterminal der Sicherheitsklasse 1 verwendet wird, die eingegebene PIN/PUK Ziffernfolge NICHT im Klartext auf dem Bildschirm darstellen.[<=]

A_15507 - ePA-Frontend des Versicherten: Kartenterminal der Sicherheitsklasse 1: PIN-Eingabe Eingabefeedback

Das ePA-Frontend des Versicherten MUSS, wenn ein Kartenterminal der Sicherheitsklasse 1 verwendet wird, ein eingegebenes Zeichen einer Geheimniseingabe mit dem Zeichen "*" (Wildcard) quittieren.
[<=]

A_15508 - ePA-Frontend des Versicherten: Kartenterminal der Sicherheitsklasse 1: PIN-Eingabe Validierung

Das ePA-Frontend des Versicherten MUSS, wenn das Geheimnis durch einen Anwendungsfall geändert werden soll und wenn ein Kartenterminal der Sicherheitsklasse 1 verwendet wird, ein eingegebenes, neues PIN-Geheimnis durch eine erneute Abfrage des neuen PIN-Geheimnisses verifizieren.[<=]

6.3.1.2 Kartenterminals der Sicherheitsklasse 2

Kartenterminals der Sicherheitsklasse 2 verfügen über eine Eingabeschnittstelle zur Eingabe eines Benutzergeheimnisses. Typischerweise werden Kartenterminals der Sicherheitsklasse 2 in Anwendungsfällen mit Eingabe einer PIN bzw. PUK so angesteuert, dass das vorbereitete Kartenkommando mit einem Platzhalter des PIN-Geheimnisses an das Kartenterminal geschickt wird. Das Kartenterminal nimmt die PIN über die Eingabeschnittstelle entgegen, ersetzt den Platzhalter durch das eingegebene Geheimnis und leitet das Kartenkommando anschließend weiter an die Karte.

A_15509 - ePA-Frontend des Versicherten: Kartenterminal der Sicherheitsklasse 2: PIN-Eingabe

Das ePA-Frontend des Versicherten MUSS ein angeschlossenes Kartenterminal der Sicherheitsklasse 2 so ansteuern, dass ein Kartenkommando, das eine PIN-/PUK-

Eingabe erfordert, an einem Kartenterminal um die Benutzereingabe ergänzt und anschließend direkt an die adressierte Karte weitergeleitet wird.[<=]

A_15510 - ePA-Frontend des Versicherten: Kartenterminal der Sicherheitsklasse 2: PIN-Eingabe Fehlkonfiguration

Das ePA-Frontend des Versicherten MUSS alle Operationen mit einer eindeutigen Fehlermeldung abbrechen, in denen es die Kenntnis eines PIN/PUK-Geheimnisses erlangt, nachdem dieses an einem PIN-Pad eines Kartenterminals der Sicherheitsklasse 2 eingegeben wurde.[<=]

A_15511 - ePA-Frontend des Versicherten: Kartenterminal der Sicherheitsklasse 2: PIN-Eingabe Eingabefeedback

Das ePA-Frontend des Versicherten MUSS während der Abfrage einer PIN/PUK an einem Kartenterminal der Sicherheitsklasse 2 einen Benutzerhinweis zur PIN-Eingabe am Kartenterminal an der Bildschirmausgabe ausgeben.[<=]

6.3.1.3 Kartenterminals der Sicherheitsklasse 3

Kartenterminals der Sicherheitsklasse 3 verfügen über eine Eingabeschnittstelle zur Eingabe eines Benutzergeheimnisses und Ausgabeschnittstelle zur Anzeige kurzer Textmeldungen. Typischerweise werden Kartenterminals der Sicherheitsklasse 3 in Anwendungsfällen mit Eingabe einer PIN bzw. PUK so angesteuert, dass das vorbereitete Kartenkommando mit einem Platzhalter des PIN-Geheimnisses an das Kartenterminal geschickt wird. Das Kartenterminal nimmt die PIN über die Eingabeschnittstelle entgegen, ersetzt den Platzhalter durch das eingegebene Geheimnis und leitet das Kartenkommando anschließend weiter an die Karte.

Während des Wartens auf eine Benutzereingabe kann ein an das Kartenterminal übergebener Text angezeigt werden. Einzelne Eingaben durch einen Benutzer werden in der Regel durch das Zeichen "*" quittiert. Ebenso besitzen Kartenterminals der Sicherheitsklasse 3 meist zusätzliche Logik, z.B. Eingaben zu verifizieren (siehe Anforderungen zum Ändern einer PIN mittels Klasse 1-Kartenterminal). Auf diese Logik soll hier nicht weiter eingegangen werden.

A_15512 - ePA-Frontend des Versicherten: Kartenterminal der Sicherheitsklasse 3: PIN-Eingabe

Das ePA-Frontend des Versicherten MUSS ein angeschlossenes Kartenterminal der Sicherheitsklasse 3 so ansteuern, dass ein Kartenkommando, das eine PIN-/PUK-Eingabe erfordert, an einem Kartenterminal um die Benutzereingabe ergänzt und anschließend direkt an die adressierte Karte weitergeleitet wird.[<=]

A_15513 - ePA-Frontend des Versicherten: Kartenterminal der Sicherheitsklasse 3: PIN-Eingabe Fehlkonfiguration

Das ePA-Frontend des Versicherten MUSS alle Operationen mit einer eindeutigen Fehlermeldung abbrechen, in denen es die Kenntnis eines PIN/PUK-Geheimnisses erlangt, nachdem dieses an einem PIN-Pad eines Kartenterminals der Sicherheitsklasse 3 eingegeben wurde.[<=]

A_15514 - ePA-Frontend des Versicherten: Kartenterminal der Sicherheitsklasse 3: PIN-Eingabe Eingabefeedback

Das ePA-Frontend des Versicherten MUSS während der Abfrage einer PIN/PUK an einem Kartenterminal der Sicherheitsklasse 3 einen Benutzerhinweis zur PIN-Eingabe am Display des Kartenterminals ausgeben.[<=]

Die Anzeige eines Benutzerhinweises soll den Nutzer informieren zu welchem Zweck eine Eingabe getätigt (z.B. alte PIN, neue PIN im Anwendungsfall PIN ändern) und welches konkretes Geheimnis abgefragt werden soll (PIN, PUK).

6.3.2 Schnittstelle für PIN-Operationen und Anbindung der eGK

Anwendungsfälle zur PIN-Verwaltung, das Login sowie weitere Anwendungsfälle können die Eingabe eines PIN- oder PUK-Geheimnisses durch den Versicherten erfordern. Der Zugriff auf die eGK erfolgt über die Systemprozesse `PL_TUC_CARD_*`. Das FdV als Realisierungsumgebung der Systemprozesse muss ihrerseits die von der Plattform geforderten Schnittstellen `ENV_TUC_CARD_SECRET_INPUT` implementieren, um die Kommunikation der Plattform mit dem Nutzer über die Außenschnittstelle des FdV zu ermöglichen. Die Außenschnittstelle ist in Kapitel "6.3.1 Transportschnittstelle für Kartenkommandos" beschrieben und umfasst das Kartenterminal, Eingabemedium und Hinweistexte an den Nutzer. Diese kann je nach Konfiguration an einem Gerät als Kartenterminal der Sicherheitsklasse 3 oder auch eine Kombination aus Bildschirmausgabe, Kartenterminal-PIN-Pad und/oder Tastatureingabe erfolgen.

A_15515 - ePA-Frontend des Versicherten: Übergabeschnittstelle PIN/PUK-Geheimnis

Das ePA-Frontend des Versicherten MUSS eine Operation `ENV_TUC_SECRET_INPUT` zur Eingabe eines PIN/PUK-Geheimnisses und Weiterleitung an eine SmartCard mit den Parametern

- Eingangsparameter:
 - `Identifikator`
 - `Aktion`
 - `minLength`
 - `maxLength`
 - `commandApduPart`
- Rückgabewerte:
 - `responseApdu`

implementieren.[<=]

A_15516 - ePA-Frontend des Versicherten: Umsetzung der Operation `ENV_TUC_SECRET_INPUT`

Das ePA-Frontend des Versicherten MUSS die Abbildung der Eingangsparameter auf die Rückgabewerte der Operation `ENV_TUC_SECRET_INPUT` derart umsetzen, dass

- die Eingangsparameter `Identifikator` und `Aktion` für einen Hinweistext an den Nutzer verwendet werden, welche Aktion auf welchem konkreten Kartenobjekt (z.B. Name einer PIN) durchgeführt wird
- wenn der Eingangsparameter `Aktion` die Eingabe eines Nutzerhinweises erfordert, der `commandApduPart` an der Eingabeschnittstelle um das Geheimnis des Nutzers ergänzt wird
- der `commandApduPart` über die Transportschnittstelle für Kartenkommandos an die Karte gesendet wird

und die Antwortnachricht der Karte als `responseApdu` an den Aufrufer zur Auswertung zurückgegeben wird.[<=]

A_15517 - ePA-Frontend des Versicherten: Minimalprinzip Karteninteraktion

Das ePA-Frontend des Versicherten DARF ein Kartenkommando NICHT an eine angebundene Karte weiterleiten, dass nicht explizit im Kontext eines Anwendungsfalls (intendierte Kartenoperationen und Erhöhen des Sicherheitszustands der Karte falls erforderlich) erforderlich ist.[<=]

7 Informationsmodell

Akte:

Datenfeld	Herkunft	Beschreibung
Akten-ID (RecordIdentifier)	Konfiguration	beinhaltet Versicherten-ID und Anbieter-ID (homeCommunityId)
Name des Aktenkontoinhabers	Konfiguration	
FQDN des ePA-Aktensystem	Konfiguration	

Geräte-Daten:

Datenfeld	Herkunft	Beschreibung
Geräteerkennung (DeviceID)	Konfiguration	beinhaltet Gerätenamen und Geräteidentität
Geräteidentität	Konfiguration	wird von der Autorisierung beim erstmaligen Aufruf zusammen mit dem DEVICE_UNKNOWN Fehler übermittelt
Gerätenamen	Konfiguration	durch Nutzer festgelegt

Session-Daten:

Datenfeld	Herkunft	Beschreibung
Akten-ID (RecordIdentifier)	Konfiguration	Kennung des Aktenkontos, auf das in der Aktensession zugegriffen wird, im Format von RecordIdentifier gemäß [gemSpec_DM_ePA#2.2] Die homeCommunityID muss bekannt sein.
Status Nutzer (Aktenkontoinhaber oder Vertreter)		Vergleich Versicherten-ID aus Akten-ID mit Versicherten-ID aus Authentisierungszertif

		ikat des Nutzers
Authentisierungstoken (AuthenticationAssertion)	Komponente Authentisierung (I_Authentication_Insurant::LoginCreateToken)	
Autorisierungstoken (AuthorizationAssertion)	Komponente Autorisierung (I_Authorization_Insurant::getAuthorizationKey)	
Aktenschlüssel (RecordKey)	AuthorizationKey	entschlüsselter Aktenschlüssel
Kontextschlüssel (ContextKey)	AuthorizationKey	entschlüsselter Kontextschlüssel
Zustand des Aktenkontos (RecordState)	Autorisierungstoken Attribut Assertion/AttributeStatement/Attribute mit dem Namen "Zustand des Kontos"	
Zeitpunkt der letzten Authentifizierung durch den Nutzer	Konfiguration	
Liste der vergebenen Berechtigungen	Aktivität "Vergebene Berechtigungen bestimmen"	Liste der für alle Berechtigungen ausgelesenen AuthorizationKeys und Policy Documents

Nutzer:

Datenfeld	Herkunft	Beschreibung
Authentisierungszertifikat des Nutzers	eGK für alternative Versichertenidentität: Signaturdienst	falls eGK: C.CH.AUT falls alternative Versichertenidentität: C.CH.AUT_ALT
Name des Nutzers	Authentisierungszertifikat des Nutzers	
Versicherten-ID des Nutzers	Authentisierungszertifikat des Nutzers	
Benachrichtigungskanal für Geräteverwaltung (E-Mail)		durch den Nutzer während des Eröffnens des Aktenkontos angegeben.

Berechtigungen:

Datenfeld	Herkunft	Beschreibung
Name des Berechtigten		
Kategorie		LEI , KTR oder Vertreter
ID		für LEI oder KTR: TelematikID für Vertreter: Versicherten-ID
Berechtigung ausgestellt am	Policy Document	nur LEI
Berechtigung gültig bis	Policy Document	nur LEI
Berechtigung für den Zugriff auf von LEI eingestellten Dokumenten	PolicyDocument mit "urn:gematik:policy-set-id:permissions-access-group-hcp"	nur LEI
Berechtigung für den Zugriff auf von Versicherten eingestellten Dokumenten	Policy Document mit "urn:gematik:policy-set-id:permissions-access-group-hcp-insurant-documents"	nur LEI
Berechtigung für den Zugriff auf von KTR eingestellten Dokumenten	Policy Document mit "urn:gematik:policy-set-id:permissions-access-group-hcp-insurance-documents"	nur LEI

8 Verteilungssicht

Eine Darstellung der hardwareseitigen Verteilung des Produkttyps bzw. seiner Teilsysteme und der Einbettung in die physikalische Umgebung wird nicht benötigt.

9 Anhang A – Verzeichnisse

9.1 Abkürzungen

Kürzel	Erläuterung
DSMLv2	Directory Services Markup Language v2.0
eGK	Elektronische Gesundheitskarte
ePA	Elektronische Patientenakte
FdV	ePA-Frontend des Versicherten
FQDN	Fully-Qualified Domain Name
GdV	Gerät des Versicherten
IHE	Integrating the Healthcare Enterprise
KTR	Kostenträger, d.h. die gesetzlichen Krankenkassen
KVNR	Krankenversichertennummer
LE	Leistungserbringer
LEI	Leistungserbringerinstitution
MTOM	Message Transmission Optimization Mechanism
NFC	Near Field Communication
OWASP	Open Web Application Security Project
PDF	Portable Document Format
PIN	Personal Identification Number
PUK	Personal Unblocking Key
SGD	Schlüsselgenerierungsdienst
SOAP	Simple Object Access Protocol
TI	Telematikinfrastruktur

TLS	Transport Layer Security
TSL	Trust-service Status List
VZD	Verzeichnisdienst der TI

9.2 Glossar

Begriff	Erläuterung
Funktionsmerkmal	Der Begriff beschreibt eine Funktion oder auch einzelne, eine logische Einheit bildende Teilfunktionen der TI im Rahmen der funktionalen Zerlegung des Systems.
leistungserbringeräquivalentes Dokument	Ist ein durch den Versicherten oder einen Kostenträger im Aktenkonto bereitgestelltes Dokument, welches von einem Leistungserbringer anderen Leistungserbringern, welche keinen Zugriff auf Dokumente mit erhöhter Vertraulichkeit haben, zugänglich gemacht wurde.
Patienteninformation	Ist ein durch eine Leistungserbringerinstitution im Aktenkonto bereitgestelltes Dokument, welches vorrangig der Information von Versicherten dient. Das Dokument wird durch den Leistungserbringer als Versicherteninformation gekennzeichnet.
Policy Document	Das Policy Document ist ein technisches Dokument. Es enthält die Zugriffsregeln eines Berechtigten im Aktenkonto des Versicherten in der Komponente "Dokumentenverwaltung". Berechtigte der Aktenkontoinhaber, Vertreter oder LEIs.
Versicherten-ID	Die Versicherten-ID ist der 10-stellige unveränderliche Teil der 30-stelligen Krankenversicherungsnummer (KVNR).
Versichertendokument	Ist ein durch einen Versicherten (Aktenkontoinhaber oder Vertreter) im Aktenkonto bereitgestelltes Dokument
Versicherteninformation	siehe Patienteninformation

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

9.3 Abbildungsverzeichnis

Abbildung 1: Komponenten des FdV.....	12
Abbildung 2: Aktivitätsdiagramm "Login Aktensession".....	65
Abbildung 3: Aktivitätsdiagramm "Logout Aktensession".....	70
Abbildung 4: Aktivitätsdiagramm "Aktenkonto aktivieren".....	73

Abbildung 5: Aktivitätsdiagramm "Anbieter wechseln".....	77
Abbildung 6: Aktivitätsdiagramm "Berechtigung an LEI für Aktenkonto vergeben"	83
Abbildung 7: Aktivitätsdiagramm "Vertretung einrichten".....	86
Abbildung 8 Berechtigung an Kostenträger für Aktenkonto vergeben	90
Abbildung 9: Aktivitätsdiagramm "Vergebene Berechtigungen anzeigen"	92
Abbildung 10: Aktivitätsdiagramm "Berechtigung für LEI ändern"	95
Abbildung 11: Aktivitätsdiagramm "Berechtigung für LEI löschen"	97
Abbildung 12: Berechtigung für Kostenträger löschen.....	100
Abbildung 13: Aktivitätsdiagramm "Dokumente einstellen".....	103
Abbildung 14: Aktivitätsdiagramm "Dokumente suchen"	107
Abbildung 15: Aktivitätsdiagramm "Dokumente herunterladen".....	109
Abbildung 16: Aktivitätsdiagramm "Dokumente löschen"	111
Abbildung 17: Aktivitätsdiagramm "Protokolldaten einsehen".....	113
Abbildung 18: Aktivitätsdiagramm "PIN der eGK ändern"	119
Abbildung 19: Aktivitätsdiagramm "PIN der eGK entsperren"	122

9.4 Tabellenverzeichnis

Tabelle 1: TAB_FdV_101 – Akteure und Rollen.....	9
Tabelle 2 : TAB_FdV_102 – Schnittstellen des ePA-Aktensystems	10
Tabelle 3 :TAB_FdV_167 – Komponenten des FdV.....	12
Tabelle 4: TAB_FdV_103 – IHE Akteure und Transaktionen.....	18
Tabelle 5 : TAB_FdV_125 – Metadatenattribute	24
Tabelle 6: TAB_FdV_104 – Parameter FdV.....	29
Tabelle 7: TAB_FdV_105 – Session-Daten.....	33
Tabelle 8: TAB_FdV_106 – DNS RR ePA-Aktensystem Komponenten	34
Tabelle 9 : TAB_FdV_110 – Zertifikatsnutzung	36
Tabelle 10: TAB_FdV_161 – Zulässigkeit von Anwendungsfällen.....	40
Tabelle 11: TAB_FdV_107 – Behandlung von Fehlercodes von Plattformbausteinen.....	42
Tabelle 12: TAB_FdV_108 – Behandlung von Fehlern des ePA-Aktensystems	43
Tabelle 13: TAB_FdV_109 – Authentisieren des Nutzers	44
Tabelle 14: TAB_FdV_173 – Logout - Authentisierungstoken abmelden.....	45
Tabelle 15: TAB_FdV_111 – Dokumentenset in Dokumentenverwaltung hochladen	46
Tabelle 16: TAB_FdV_112 – Dokumentenset aus Dokumentenverwaltung herunterladen	47
Tabelle 17: TAB_FdV_113 – Dokumentenset in Dokumentenverwaltung löschen	49

Tabelle 18: TAB_FdV_114 – Suche nach Dokumenten in Dokumentenverwaltung	49
Tabelle 19: TAB_FdV_115 – Vergebene Berechtigungen bestimmen.....	50
Tabelle 20 : TAB_FdV_179 – Akten- und Kontextschlüssel verschlüsseln	54
Tabelle 21 : TAB_FdV_180 – Akten- und Kontextschlüssel entschlüsseln	55
Tabelle 22: TAB_FdV_116 – Schlüsselmaterial aus ePA-Aktensystem laden	56
Tabelle 23: TAB_FdV_163 – Schlüsselmaterial aller Berechtigten aus ePA-Aktensystem laden.....	57
Tabelle 24: TAB_FdV_117 – Schlüsselmaterial im ePA-Aktensystem speichern	57
Tabelle 25 : TAB_FdV_118 – Schlüsselmaterial im ePA-Aktensystem ersetzen	58
Tabelle 26: TAB_FdV_119 – Schlüsselmaterial im ePA-Aktensystem löschen	59
Tabelle 27: TAB_FdV_120 – Suchkriterien LDAP Search.....	60
Tabelle 28: TAB_FdV_121 – Abfrage Verzeichnisdienst.....	61
Tabelle 29: TAB_FdV_122 – PIN-Eingabe durch Nutzer.....	63
Tabelle 30: TAB_FdV_123 – Login Aktensession	64
Tabelle 31: TAB_FdV_124 – Login - Einlesen der Karte	66
Tabelle 32: TAB_FdV_126 – Login - Aktenkontext öffnen - Operation OpenContext	68
Tabelle 33: TAB_FdV_127 – Logout Aktensession	69
Tabelle 34: TAB_FdV_128 – Logout - Aktenkontext schließen	71
Tabelle 35: TAB_FdV_172 – Logout - Authentisierungstoken abmelden.....	71
Tabelle 36: TAB_FdV_130 – Aktenkonto aktivieren	72
Tabelle 37: TAB_FdV_131 – Anbieter wechseln	75
Tabelle 38: TAB_FdV_132 – Anbieter wechseln - Aktenkonto in Exportzustand versetzen	78
Tabelle 39: TAB_FdV_133 – Anbieter wechseln - Aktenkonto fortführen	79
Tabelle 40: TAB_FdV_134 – Berechtigung an LEI für Aktenkonto vergeben	82
Tabelle 41: TAB_FdV_135 – Vertretung einrichten	85
Tabelle 42: TAB_FdV_171 – Berechtigung an Kostenträger für Aktenkonto vergeben....	88
Tabelle 43: TAB_FdV_137 – Vergebene Berechtigungen anzeigen.....	91
Tabelle 44: TAB_FdV_138 – Berechtigung für LEI ändern.....	93
Tabelle 45: TAB_FdV_139 – Berechtigung löschen.....	96
Tabelle 46: TAB_FdV_168 – Berechtigung Vertreter löschen	98
Tabelle 47: TAB_FdV_166 – Berechtigung für Kostenträger löschen.....	99
Tabelle 48: TAB_FdV_146 – Dokumente einstellen.....	101
Tabelle 49: TAB_FdV_147 – Dokumente einstellen - Dokument verschlüsseln	104
Tabelle 50: TAB_FdV_148 – Dokumente suchen	106
Tabelle 51: TAB_FdV_149 – Dokumente aus Aktenkonto herunterladen.....	108
Tabelle 52: TAB_FdV_150 – Dokumente löschen.....	110

Tabelle 53: TAB_FdV_151 – Protokolldaten einsehen	112
Tabelle 54: TAB_FdV_152 – Protokolldaten einsehen - Dokumentenverwaltung abfragen	114
Tabelle 55: TAB_FdV_153 – Protokolldaten einsehen - Autorisierung abfragen	114
Tabelle 56: TAB_FdV_154 – Protokolldaten einsehen - Zugangsgateway des Versicherten abfragen.....	114
Tabelle 57: TAB_FdV_155 – Felder im Protokolleintrag.....	115
Tabelle 58: TAB_FdV_156 – PIN der eGK ändern	117
Tabelle 59: TAB_FdV_157 – Ablaufaktivitäten – PIN der eGK ändern	117
Tabelle 60: TAB_FdV_158 – PIN der eGK entsperren	120
Tabelle 61: TAB_FdV_159 – Ablaufaktivitäten – PIN der eGK entsperren	120
Tabelle 62: TAB_FdV_160 – Benachrichtigungsadresse aktualisieren	123
Tabelle 63 : TAB_FdV_177 – Verwendete Plattformleistungen.....	123

9.5 Referenzierte Dokumente

9.5.1 Dokumente der gematik

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

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: 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_Dokumentenverwaltung]	gematik: Spezifikation Dokumentenverwaltung ePA
[gemSpec_Krypt]	gematik: Übergreifende Spezifikation

	Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_OM]	gematik: Übergreifende Spezifikation Operations und Maintenance
[gemSpec_PKI]	gematik: Übergreifende Spezifikation Spezifikation PKI
[gemSpec_SGD_ePA]	gematik: Spezifikation Schlüsselgenerierungsdienst ePA
[gemSpec_Signaturdienst]	gematik: Spezifikation Signaturdienst
[gemSpec_Systemprozesse_dezTI]	gematik: Spezifikation Systemprozesse der dezentralen TI
[gemSpec_TSL]	gematik: Spezifikation TSL-Dienst
[gemSpec_X_509_TSP]	gematik: Spezifikation Trust Service Provider X.509
[gemSpec_Zugangsgateway_Vers]	gematik: Spezifikation Zugangsgateway des Versicherten ePA
[gemSysL_ePA]	gematik: Systemspezifisches Konzept ePA

9.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[DSML2.0]	OASIS: Directory Services Markup Language v2.0 December 18, 2001 https://www.oasis-open.org/standards http://www.oasis-open.org/committees/dsml/docs/DSMLv2.doc http://oasis-open.org/committees/dsml/errata https://www.oasis-open.org/committees/dsml/docs/DSMLv2.xsd
[ETSI_TS_102_231_V3.1.2]	ETSI TS 102 231 V3.1.2 (2009-12) Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust-service status information
[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-TF]	IHE International (2018): IHE IT Infrastructure (ITI) Technical Framework, Revision 15.0

[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-2x) – Volume 2 Appendices, Revision 15.1, http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2x.pdf
[MTOM]	W3C (2005): SOAP Message Transmission Optimization Mechanism, https://www.w3.org/TR/soap12-mtom/
[OWASP Proactive Control]	OWASP Top Ten Proactive Controls Project OWASP Proactive Controls For Developers v3.0 https://www.owasp.org/images/b/bc/OWASP_Top_10_Proactive_Controls_V3.pdf
[OWASP SAMM Project]	OWASP SAMM Project https://www.owasp.org/index.php/OWASP_SAMM_Project#tab=Browse_Online
	https://www.owasp.org/index.php/Projects/OWASP_Mobile_Security_Project_-_Top_Ten_Mobile_Controls
[OWASPMobileTop10]	https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf OWASP Mobile Security Project: Top 10 Mobile Risks https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=Top_10_Mobile_Risks
[RFC6960]	RFC 6960 (Juni 2013): X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP https://tools.ietf.org/html/rfc6960
[vesta]	Zentrales Interoperabilitätsverzeichnis des deutschen Gesundheitswesens https://www.vesta-gematik.de/
[WSIBP]	Web-Services Interoperability Consortium (2010): WS-I Basic Profile V2.0 (final material), http://ws-i.org/Profiles/BasicProfile-2.0-2010-11-09.html
[XMLEnc-1.1]	XML Encryption Syntax and Processing, W3C Recommendation 11 April 2013, http://www.w3.org/TR/xmlenc-core1/